LI, XIAOYU, Ph.D. An Investigation of Commitment to Information Security and Information Sharing on Social Media. (2020)
Directed by Dr. Gurpreet Dhillon. 153pp.

Information sharing has been growing hugely and globally. Research has shown that collecting and utilizing information results in a more effective way to develop business. However, the ubiquitous data collection on the Internet has raised concerns about invasion of privacy and abuse of personal data widely. A data breach could cause serious consequences such as monetary loss, social embarrassment, psychological violation of private space, and so on (Bansal et al. 2016). Therefore, more and more people have become unwilling to share their personal information on the Internet. However, the younger cohort of Internet users and the internet/technology natives, iGeneration (iGen) share information across several online platforms without a second thought, largely because they prioritize personalization over privacy. Online communication is not something they need to learn, but social media and screens encompass them as a norm, making them the most technologically centered generation (McCrindle and Wolfinger, 2010). Based on the Generational Cohort Theory, different generations have specific habits, beliefs, and values. It is generally agreed that iGen has a unique perspective of the digital world from its predecessors (WP Engine, 2017; WP Engine and The CGK, 2017). Therefore, using the Theory of Commitment, this dissertation seeks to provide a deeper understanding of information security in the context of the iGen by focusing on their commitment to information security and the motivators of their intention to share information online.

Based on the survey of 431 iGen participants, the findings indicate that iGen's trust in social media and compensation offered by social media directly and positively affect iGen's intention to share information on social media. Additionally, iGen with strong continuance commitment has less trust in social media, but their perceived privacy controls on social media boost social media confidence. Moreover, strong normative commitment and affective commitment of iGen promote their continuance commitment. The findings contribute to the literature of information security in the following ways. Firstly, it extends the application of the commitment theory into the field of information sharing. Secondly, it expands the literature of information sharing and the commitment theory to the youngest generation of internet users, iGen. They are the internet and technology natives. Thirdly, it demonstrates how iGen commits to their privacy and information security. Fourthly, this study explores relationships between the three forms of commitments, which contribute to a deeper understanding of individuals' commitment to information security.

AN INVESTIGATION OF COMMITMENT TO INFORMATION SECURITY AND INFORMATION SHARING ON SOCIAL MEDIA

by

Xiaoyu Li

A Dissertation Submitted to
the Faculty of The Graduate School at
The University of North Carolina at Greensboro
in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

Greensboro
2020

Approved by

_____
Committee Chair

To my mom, my dad, my husband, my daughter, and my son for their infinite love and support.

APPROVAL PAGE

This dissertation written by XIAOYU LI has been approved by the following committee of the Faculty of The Graduate School at The University of North Carolina at Greensboro.

Committee Chair _____
Dr. Gurpreet Dhillon

Committee Members _____
Dr. A.F. Salam

_____
Dr. Kane Smith

_____
Dr. Haimeng Zhang

_____
Date of Acceptance by Committee

_____
Date of Final Oral Examination

ACKNOWLEDGEMENTS

I would like to express my whole-heart gratitude to Dr. Dhillion, my committee chair, my advisor and the best mentor, who has supported me in various forms - time, ideas, patience, motivation and knowledge. Next, I would like to thank Dr. Zhang, who helped me build the theoretical foundation of Statistics which is more than useful in my research and future career. Then, I would like to thank Dr. Smith who gives me guide on my thesis writing and answer all my questions; and thank Dr. A.F. Salem for his invaluable support and advice.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

CHAPTER I

INTRODUCTION

1.1 Overview

The Internet Generation (iGen) are individuals born between 1995 and 2012. Not only is this generation highly attached to the Internet, but they have also "individualized" the way they choose to use Internet-based technologies (Levin, 2017). The iGen are important as they represent a growing economic power, constituting roughly 24% of the population in 2020 with an estimated $44 billion in annual purchasing power (Sparks and Honey, 2018). iGen was 61 million individuals in the US alone in 2015 (Weinswig, 2016) and are estimated to reach 1.3 million entering labor force by 2030 (Brown, 2020). According to Kevin Thorpe (2019), global chief economist and head of research with Cushman and Wakefield, iGen is the largest generation in the world with close to two billion people, and it accounts for 26% of the global population (Brown, 2020).

The iGen hence represents an important and unique generation that possesses characteristics that are distinct from other generations, such as their “expectations, experiences, lifestyles, values, and demographics”, which all serve to influence their attitudes and behaviors (Williams and Page, 2011). It is widely accepted that iGen is the most technologically centered generation (McCrindle and Wolfinger, 2010), having a very distinguishable perspective of the digital world (WP Engine, 2017).

However, prior research has found that members of the iGen are less aware and knowledgeable about the nature of information security than older generations, which can potentially lead to various cyber risks to themselves and others (Schiola, 2017). For example, iGens have the highest usage of social media and data sharing (Harrison, 2018); they value authenticity (Schiola, 2017), expect a predictive Internet (Kreamer, 2018), and prioritize personalization over privacy (WP Engine, 2017). For these reasons, iGens easily share personal information across a number of online platforms without a second thought, exposing themselves and their social networks to potential security risks (Security News Desk, 2016).

Therefore, in order to combat the potential risks of iGens sharing information via social media, this research argues that we must first begin by understanding the antecedents to iGens' intention to share personal information via social media. Furthermore, we must also understand their commitments to personal privacy and how this influences the iGen's use of social media. By developing this understanding of iGens' social media with respect to the sharing of personal information, we lay the foundation for developing information security measures for protecting the personal data of iGen social media users.

When considering the importance of commitment for effectiveness of information security, it is critical and necessary to understand the role of the iGen's commitment to information security and their intention to share information online. This facilitates the understanding of the complex interaction between the iGen's desired social media experience and the security of their personal information.

1.2 Information Sharing

Information sharing refers to the data transfer and exchange between people, organizations, and technologies (Techopedia, 2018). There are two types of information sharing: personal information sharing and cybersecurity information sharing. Although this study will focus on personal information, both types of information sharing will be introduced in this section to provide a wider understanding of the topic.

1.2.1 Personal Information

According to U.S. Department of Labor (2020) Personal information describes personal information that are used for identification, which is defined by the US Government Accountably Office as:

> (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (Mccallister et al., 2010; Gao, 2008).

Personal information sharing refers to personal information being transmitted to others. It includes initiatively and passively sharing information by the owners or non-owners. Initiative sharing denotes that an Internet user discloses their information on their own volition, such as sharing personal picture posts on social media. Passively sharing indicates that a person is requested to share information through the Internet, such as the submission of necessary information to obtain a loan approval.

Social media platforms not only provided the technology to enable personal information sharing on the Internet, but also encouraged the information sharing, which

made information sharing online become pervasive (Techopedia, 2018). According to Techopedia (2018), Social networking platforms have built a sharing network consisting of more than a billion people, and almost 10% of the global population exchanges information and shares themselves through their mutual networks daily (Techopedia, 2018). Alongside social networking, a variety of information systems, such as e-commerce, online banking, web-based registration or appointment making systems, and mobile healthcare apps, have been continuously creating, sharing, and asking to share personal information (Hajli and Lin, 2016).

1.2.2 Cybersecurity Information Sharing

Cybersecurity information refers to cyberattack- and cybersecurity-related information or experience. Correspondingly, cybersecurity information sharing denotes the conveyance of cyberattack- and cybersecurity-related information or experience from one trusted party to another (Nolan, 2015).

After the terrorist attacks of September 11, 2001, United States governments aimed to build an information collection systems in other to prevent similar events in the future, and hence government agencies and departments was mandated to design and implement the approach to regularly collect and share relevant security information (Techopedia, 2018). The US government expected this information widely and quickly shared, because the reactions to terroristic activities were always in a timely manner, and the purpose of information sharing was to improve the effectiveness of responses to various threats in US (Techopedia, 2018).

It is complex for sharing the right information, because it is the automation of sharing by technology and machine to counter increasing and complicated threats (Goodwin and Nicholas, 2015). Gain of the valuable information at the right time can enable businesses or organizations to detect and defense security attackers, reduce cybersecurity risks, and improve their elasticity (Goodwin and Nicholas, 2015). Industry practitioners and academic researchers agreed that collaboration through information sharing was able to reduce cybersecurity risks (Skopik, 2016).

> Information sharing is a concept supported by most corporate executives and government officials responsible for reducing and responding to cybersecurity breaches related to their organizations (Gordon et al. 2015).

Moreover, legislators and other stakeholders have recognized that the importance of reducing cybersecurity risks to government information systems and boosting critical infrastructures, hence they encourage the sharing or exchanging of information, and consequently enterprises have increasingly depended on the collaboration of information sharing (Goodwin and Nicholas, 2015). The following is what executive order of President Obama states about improving critical infrastructure cybersecurity through cybersecurity information sharing:

> It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats (Obama, 2013).

1.3 Issues of Information Sharing

Firms are currently eager to acquire useful data to identify their business trend analysis and develop business strategies. Therefore, increasingly more businesses and organizations are collecting their customers' shared data to generate valuable information and insights for conception and improvement of their commercial decision making and operation management (Hajli and Lin, 2016). Due to more and more personal information sharing in public, such as on social media, unauthorized information collection raises both security and ethical issues (Hajli and Lin, 2016). It is not known that what information can be collected and used, who are allowed to collect personal information, who can access to and use personal information, how and where personal information can be used and so on (Hajli and Lin, 2016).

Private information might be protected from been abused based on assumption that the applying of penalty for breaking trust, hence people shared sensitive information with their intimate familiarity in traditional markets (Bansal et al., 2016). For example, patients shared their sensitive and private health information with their health providers, and believed their physicians would keep that health information confidential due to the restrains of law and professional ethics; Also, banks would be punished if they abuse their customers' financial information (Bansal et al., 2016). On the contrary, it is not easy to apply these penalties for punishing or preventing unauthorized information sharing online (Bansal et al., 2016).

Furthermore, marketers also face challenges of information sharing online. According to the survey of 292 marketing executives, the security of business transactions was the most often mentioned ethical concerns regarding online marketing,

and illegal activities such as Internet fraud and hacking, customers' privacy, and the honesty or truthfulness of the information shared by their customers were ranked as the next three most often mentioned concerns (Bush et al., 2000).

Existing literature found that the predominant ethical issues of information sharing on the Internet are privacy, identity theft, and phishing (Schlegelmilch and Öberseder, 2010). Additionally, extant literature identified the critical issues of e-commerce as the authority of data access, privacy and informed consent, information security, and intellectual property (Kracher and Corritore, 2004).

Data collection and data analysis have achieved huge improvement of human's life convenience and life quality (Floridi and Taddeo, 2016). An example of this is the development of smart cities, which apply data collection and data analysis to serve and ease citizens' daily life and support city admonition and operation (Kitchin and Dodge, 2019). Unfortunately, such opportunities also face significant ethical issues and challenges (Elbeltagi and Agag, 2016). The increased use of customers' data, especially private data, and the extensive reliance on algorithms to analyze the collected data using machine learning, artificial intelligence, and robotics aims to predict consumers' choices of products and services, hence to support businesses' decision making and revenue promotion (Hajli and Lin, 2016). All those activities potentially pose pressing issues of privacy invasion, the disrespect of human rights, abuse of data, data attack, data theft, and all other data security threats (Floridi and Taddeo, 2016).

1.3.1 Issues of Information Sharing on Social Media

Nowadays, social media platforms or apps are embedded with more functions for users to disclose their information (Sarang, 2018). Apps such as Snapchat and Facebook can constantly collect the location information of their users through default settings, geotagging photos or videos (Sarang, 2018). Previously, people merely exhibit their latest experiences, but now they share their location through the function of "checking in" on social media to reap commercial rewards, which encourages more people to share more information on social media and could expose personal location and important life information to malicious audiences (Sarang, 2018).

When people take or post a picture at home, the snapshots with GPS location can potentially reveal detailed home address and internal house information to the stalkers or cybercriminals (Sarang, 2018). Moreover, the metadata within their photos can also be used by cybercriminals to track where the users live, thus leaving cyber-devices and home with a slew of cybersecurity threats (Sarang, 2018). Additionally, although the geotagging function provided by social media can be enjoyable and useful, the unauthorized spread of customer data created by geotagging with no regulations can cause serious cybersecurity issues (Sarang, 2018).

It is essential to comprehend that once information has been put on the Internet, it is nearly impossible to revoke or reverse this (Sarang, 2018). However, the iGeneration, the youngest generation of Internet users, have gotten into the habit of oversharing their life on the Internet (Sarang, 2018). They share text information of their demographic and photos of friends, family, parties, works, locations, hobbies, and experiences (Sarang, 2018). Cybercriminals can utilize and combine all the information being shared on social

media websites and mobile apps to decipher passwords as keys to users' digital worlds (Sarang, 2018).

1.3.2 Issues of Illegal Data Collection

Alongside users' oversharing of personal information and marketers' unethical collection of user information, breach issues caused by the malicious disclosure of private information is another problem of information sharing (Fischer, 2016). The inadequate knowledge of web technology and impersonal nature of online environment could lead to all kinds of data breaches and privacy invasion (Bansal et al., 2016).

The public disclosure of private information can harm individuals financially and socially (Mothersbaugh et al., 2012). For example, the exposure of an individual's identity or financial information could lead to cybercriminals using victims' identity to fraud or stealing money from victims' accounts (Bansal et al., 2016).

According to a Symantec study, the costs of data breaches have been increasing all over the world, and the US has the highest per capita cost of data breaches (Ponemon, 2013). The advent of technology enables data collection, data mining, and data analysis, which makes the demand for information become ubiquitous and pervasive on the Internet (Bansal et al., 2016).

More and more Internet users became reluctant to share their private information on the internet and even fabricated such data to mitigate the potential abuse of their personal information online (Li and Santhanam, 2008). However, they may share their private information to their trustees, which can also be taken by cybercriminals, who phish victims to obtain their personal or identity information (Fischer, 2016). Such

information sharing can cause “monetary loss, social embarrassment, and psychological violations of private space” (Bansal et al. 2016).

1.4 Information Sharing among iGeneration

According to the WP engine (2020), iGens will represent 40% of the population with a buying power of $150 billion and an influence of $600 billion in spending globally by 2025 (WP Engine, 2020; WP Engine and The CGK, 2017). Currently, the iGeneration is at 91 million strong. They are the largest generation in the US and account for 40% of global consumers (WP engine, 2020).

These statistics imply that the iGen is a growing economic power and will soon be key to the majority of organizations (Hoxha and Zeqiraj, 2019). The iGen is not just a generation segmented by age but also by “a new set of behaviors and attitudes about how the world will work and how we will need to respond to stay current, competitive and relevant” (Koulopoulos and Keldsen, 2014).

1.4.1 Who is the iGeneration

For the past decade, there has been considerable discussion about how to understand and reach Millennials or Generation Y, but the new generation called iGens are the latest focus (Hoxha and Zeqiraj, 2019). The literature provides a great variety of names for those who were born in 1995 through 2012. The most popular term referring to this generation is “Generation Z”, which was first proposed and applied by Tari (2011), following the pattern of Generation X and Generation Y. Other researchers and practitioners have used the terms digital native (Prensky, 2001); App Generation, where “App” refers to mobile applications; Net Generation, where “Net” denotes the Internet; D

Generation; where “D” signifies “digital”; C Generation, where “C” denotes connection; Facebook Generation; Selfie Generation; Trans Generation; Post-Millennials, and Dotcom Children (Hoxha and Zeqiraj, 2019).

Arguably, the term "iGeneration" is the most suitable name for this generation. Not only they were raised alongside the Internet and are highly attached to the Internet, but also the "i" represents both that these technologies are mostly "individualized" in the way they are used and the types of mobile technologies, such as iPhone, iPod, Wii, and iTunes, being heralded by iGens (Levin, 2017). Born predominantly in the new millennium, the iGen is defined by their Internet and technology use. Their habit of digital usage or online communication is not something they need to learn, but they are electronic natives who accept social media and screens as the norm (Geiger, 2018). Extant study found that iGens assume that everyone has a social media presence, website, or smart device (Levin, 2017).

In the US, researchers have categorized the current population into five groups based on the year in which they were born (Zhang et al., 2006). In general, those who were born before 1946 are often called the “Traditional” or “Silent” generation; Those born between 1946 and 1964 belongs to the Baby Boomer generation; People born between 1965 and 1979 are called Generation X (XGen) (Zhang et al., 2006; Coupland, 1991). The label “X” is somewhat vague, signifying that in comparison with the Baby Boomers, Generation X is not as easily categorized (Rosen, 2010). Those born between 1980 and 1994 are named Generation Y (Ygen) or “Millennials” (Zhang et al., 2006). At this time, computers were starting to be more pervasively used, and the Internet came to

the world. Finally, those who were between 1995 and 2012 are called Generation Z or the iGeneration (Levin, 2017). This generation are the real technology and Internet natives because they have never experienced a time without the Internet (Schröder, 2019).

1.4.2 The Digital Natives

In 2017, the Center for Generational Kinetics for WP Engine conducted a study of more than 1,200 people between the ages of 14 and 59 in the US. This study explores the mindsets, preferences, and expectations of four generations of Americans (namely iGen, YGen, XGen, and Baby Boomers) for their Internet experiences and digital lives. The study, named "The Future of Digital Experiences," found that the digital experience is the iGen's human experience (WP Engine, 2017; WP Engine and The CGK, 2017). Although YGen has long been described as digital natives, they grew up in a world that relied on landlines and dial-up Internet (Beck and Wright, 2019).

In contrast, iGens are true digital natives, because they have lived in a world of smartphones and internet for as long as they can remember, and online communication is not something that they have had to learn because it has always surrounded them (Beck and Wright, 2019). As digital natives, iGens expect to have constant access to the Internet and expect their online experiences to be free, personalized, authentic, entertaining and secure (WP Engine, 2017; WP Engine and The CGK, 2017).

Literature emphasized that iGens are real digital natives because they were born after the invention and the pervasion of the Internet, which made them experience digital applications at a young age, while other generations started to utilize technology either at their adolescent stage or at their adulthood (Turner, 2015). According to a Pearson survey

of students in grades 4 –12 in 2015, 78% of students in elementary school use tablets every day, and 72% of them believed that they were more comfortable and proficient in using computers or tablets for learning purpose than their teachers (Beck and Wright, 2019). The extant study concluded that iGen is the most likely generation to start a business and the only generation whose first business would be implemented by or related to technology (WP Engine, 2020; WP Engine and The CGK, 2017).

Literature showed that the predominant characteristics of iGens are being technology savvy and having an attachment to the Internet (Turner, 2015), because the Internet has implemented global society online (Toronto, 2009). Since the wave of technological advancements in the 1990s, the Internet has played a critical and irreplaceable role in the lives of iGens (Turner, 2015). Compared with older generations, the daily lives of the iGen have inherently bonded to the Internet (Harrison, 2018).

They have the world in their hands through mobile smartphones, almost literally (Geiger, 2018). Via the Internet and smartphones, the iGen has been grown up in the real mobile time and make smartphones as the center of "everything" for entertainment (Palley, 2012). In total, 55% of iGens use their smartphones for more than five hours every day, and 26% of iGens use their smartphones over 10 hours every day (Boucher, 2018). On average, iGens total around eight hours of total electronic multimedia usage daily for a variety of tasks for both life and work (Beck and Wright, 2019).

According to WP Engine (2020), 58% of iGens cannot remove themselves from the Internet for more than four hours and 27% for more than one hour. On the other hand, 27% of Baby Boomers state that they can live without the Internet for more than two days

(WP Engine, 2020; WP Engine and The CGK, 2017). iGens have established a digital connection to the Internet so that they developed an emotional attachment to it, with more than 90% respondents indicating that they felt frustrated and like being punished when disconnecting to Internet connection (Palley, 2012).

A survey of 2,000 iGens indicates that the media use of those aged between 8 and 18 has reached epic proportions (Rideout et al., 2018). With advancement of multimedia technology, such as social media, mobile tablets, and smartphones, which combine the capabilities of mobile phones, Internet, cameras, and media players into one device, the iGen has become accustomed to online aspects of life, such as social communications, shopping, and even education (Turner, 2015).

A recent survey illustrates that 56% of iGens build digital relationships (WP Engine, 2020), which means that they have friends that they only know and have social interactions with online. This extant study also revealed that in comparison to older generations, who use the Internet primarily to source information, the iGen use the Internet mainly for social media and entertainment (WP Engine, 2020; WP Engine and The CGK, 2017). In other words, iGens use the Internet for much more complicated purposes, from social connections to income sources (e.g., being a YouTuber or social media influencers). In contrast, their predecessors utilize the Internet as a tool for gaining information (WP Engine, 2017).

The youngest generation of internet users does not distinguish if they are online or offline and are able to seamlessly connect the digital world to the real (WP Engine, 2017;

WP Engine and The CGK, 2017). In study of Twenge (2017), a thirteen-year-old interviewee shared her life:

> We didn't have a choice to know any life without iPads or iPhones. I think we like our phones more than we like actual people (Twenge, 2017).

Prior Literature also showed that traditional entertainments and activities, such as watch movies in theaters, attending sports events, or eating in the restaurants, were ranked much lower than tablets and social media usage for the choice of entertainment (Turner, 2015).

1.5 Issues of Cybersecurity and Information Sharing among iGen

1.5.1 Cybersecurity Issues for iGen

Although iGens are considered as digital natives, confidence in their technological savvy tends to make them careless to cybersecurity risks (Lunarline, 2018). To this end, recent research by Microsoft examined iGens' susceptibility to online tech support scams and found that iGen is the generation most vulnerable to cybersecurity risks (Lunarline, 2018).

Although the iGen are considered as a tech-savvy generation, their attitude to cybersecurity are much more relaxed than older generations (Huffman, 2017). This can present as poor password protection, reusing passwords, a careless connection to the Internet, and oversharing. Among all generations, iGen was most concerned about losing personal photos in a cyber-attack and are most likely to forward emails from unknown senders (Abel, 2018).

Furthermore, extant research indicates that iGen lacks cybersecurity awareness and are the least ransomware-savvy generation, because iGens often fail to identify ransomware and phishing threats as accurately as older generations (Abel, 2018). It has been well documented that iGens are overconfident in that they would not fall for phishing scams, yet they are the generation most likely to forward emails from unknown senders, click on malware links, and spread malware as other cyber threats (Grothaus, 2019).

Prior studies have also shown that iGen has fewer concerns about privacy and security when using mobile pay applications than when using credit and debit cards online (Mastroianni, 2016). To emphasis this lack of concern, a recent McAfee survey illustrated that iGen tends to reuse the same password for multiple online accounts (Sarang, 2018). Notably, research shows that most iGens turn on two-factor authentication for their online accounts to prevent unauthorized access (Grothaus, 2019). However, most iGens also frequently authorize login access to third-party applications through social media platforms (Grothaus, 2019).

Moreover, iGen is also more likely to connect to a free but unsecured public Wi-Fi network than older generations (Abel, 2018). They are also more likely to use crowd-sourced knowledge online to solve tech problems, which may prompt significant cyber risk (Abel, 2018). ObserveIT reported:

> Generation posed the highest cybersecurity risk to organizations, as 34% of the 18-24-year olds said that they don't know or understand what is included in their company's cybersecurity policy. This group was also the most likely generation to

> reportedly not follow their company's security policies, even when they do understand it (Harrison, 2018).

However, this generation find it appealing to work in an innovative environment that is comprised of new technology; they also intend to use social media to enable highly personal interactions and immediate-response data access (Schiola, 2017). In the meanwhile, the new apps and devices that support innovative workplaces may compromise cybersecurity, because there may be no adequate security measures or security standard (Schiola, 2017). Additionally, they use technology, such as social media and crowd-sourced, and online knowledge to deal with their work tasks and problems. Their cybersecurity habits regarding the use of those technologies and crowd-sourced knowledge are highly varied and are often far from the best practices (Harrison, 2018).

1.5.2 Information Sharing Issues for iGen

A recent study has shown that iGen is generally less concerned about protecting personal information than their older peers and thus overshare information online (Security News desk, 2016; Schiola, 2017). Another study provides the similar view that iGen shares sensitive information across a number of online platforms without a second thought due to their use of mobile and social media by default, rather than adopting these technologies through trend or necessity (Security News desk, 2016).

The existing research shows that 70% of iGen believe in personalization, 45% of iGen expect personalization, and 25% of iGen more possibly disclose personal information for a more predictive and personalized digital experience (WP Engine, 2020; WP Engine and The CGK, 2017). This signifies that iGen want websites to predict what

they want, like, or need; if this is not the case, they are likely to leave the websites (WP Engine, 2020).

In brief, the iGen do not show the same level of security knowledge or experience as previous generations (Schiola, 2017). Most iGens do not know a time and life without social media and are spend most of their spare time online via mobile devices (Boucher, 2018). Consequently, they are much more attached and even addicted to their virtual world due to the gratifications of the entertainment on the Internet and social media uses with their personal information sharing than Millennials and other previous generations (Kircaburun et al., 2018). However, iGens also seem less aware and knowledgeable about the nature of cybersecurity than older generations (Schiola, 2017). It seems they neither know about the various threats and implications of cybercriminals, privacy breaches, and data exploits nor have the proper education to be using their devices and the Internet safely (Sarang, 2018). Even if there is a broad awareness of cybersecurity, iGen has a lack of deep knowledge of what constitutes good security practice (**Bourne, 2018**) such as stopping of oversharing their personal information online, following cybersecurity policies, protecting passwords, not clicking through unknown links, not connecting to unknown public WiFi or networks, and so on.

1.6 Commitment to Information Security

Information systems security researchers believe that commitment to information systems security is required for effectiveness of information system security (Patnayakuni and Patnayakuni, 2014; Holgate and Hardy, 2012). Many studies have demonstrated that

commitment is critical to reducing security risk to data, cyber, and information systems (Barton et al 2016).

Commitment alone cannot absolutely guarantee successful security controls, but it is a prior condition for achievement of cybersecurity defense (Boss et al., 2009). An appropriate individual commitment to cybersecurity or information security can enable cybersecurity professionals to effectively develop and implement security controls (Oltsik, 2019). Emerging technologies necessitate a commitment to cybersecurity, along with information technology governance and countermeasures for an organization's sustainability and survivability (Curtis 2012). The level of practical commitment to cybersecurity dictates how secure an organization will be (Shoemaker, 2019).

The theory of commitment will be the theoretical foundation to guide the study of the iGen's commitment to information security and information sharing on social media. The theory of commitment developed by Meyer and Allen (1997) has arguably become the distinguished and predominant model for studies of commitment through its widespread application and enhanced measurement of commitment constructs (Jaros, 2007).

Literature proposed that commitment is:

> a force that binds an individual to a course of action of relevance to one or more targets (Meyer and Herscovitch, 2001).

Prior literature has also theorized that individuals

> experience this force in the form of three mindsets: affective commitment, normative commitment, and continuance commitment (Jaros, 2007).

These reflect:

> emotional ties, perceived obligation, and perceived loss or negative costs concerning a target, respectively" (Allen and Meyer, 1990).

Therefore, an individual's commitment to information security is the critical element to complete the field of information security. This study focuses on a featured cohort, namely iGen, and investigates their commitment to privacy and information security.

1.7 Motivation and Research Questions

1.7.1 Information Sharing

In the current age, online information sharing, communication, and collaboration are quick, easy, and convenient. Social media have demonstrated the importance of the investment and gain of the virtual social capital of individuals (Nardi et al., 2002) and the capabilities to achieve organizational benefits (Boyd and Ellison, 2007) and personal benefits (Carboni-Brito, 2011). Obtaining the data is no longer an insurmountable challenge. Coordination between datasets and human-designed algorithms or machine-learning analysis to comprehend data and produce insights from data have become much more demanding (James, 2018).

However, this causes ethical debates about information security online (Hajli and Lin, 2016). If we examine a recent scandal of the Cambridge Analytica over its

interference in the 2016 U.S. presidential election from a social engineering perspective, their social network data sharing practice leads to the question of data usage for analytical purposes (Bourne, 2018). Our privacy and information security may be threatened. The analytical purposes should be based on the willingness of users or customers, but the analyses are often derived from the intentions and benefits of marketers or businesses. The information security field is challenging to examine, with many unsolved questions and unclear ground (Bourne, 2018).

Security is always of the utmost importance. The study of online information sharing facilities a deeper comprehension of information security and provides critical insights and implications for both theoretical researchers and practitioners (Hajli and Lin, 2016). Companies operating in industries that use sensitive information cannot be left vulnerable. Data hacks on transport firms that hold identity data or healthcare companies that hold medical records can inflict their customers' social embarrassments and financial losses by explosion and abuse of their customers' confidential information, hence data breaches and cyberattack attempts are not likely to decrease as more iGens enter the workplace (Schiola, 2017).

1.7.2 The iGeneration

Generations are not alike (Hoxha and Zeqiraj, 2019), and the way that people view information sharing changes with age. "generation has unique expectations, experiences, generational history, lifestyles, values, and demographics" that impact their attitudes and behaviors (Williams and Page, 2011). These uniqueness lead to a significant impact on the overall evolution of industry and business, which represents the new

segment of a generation (Inglehart,1997). The importance of generations and their traits should not be ignored, and the differences and changes are more notable in different fields (Hoxha and Zeqiraj, 2019).

According to the WP Engine, iGen as the largest generation in the US; it represents $150 billion in buying power globally and accounts for 40% of global consumers in 2020 (EW Engine, 2020; WP Engine and The CGK, 2017). The prior literature indicated that it was notable that when one generation becomes the primary of the society, their values predominate the main culture, hence considering and study on generation is very important (Inglehart, 1977; Inglehart, 1997). Moreover, they have experienced very important technological innovations, such as the development of the personal computer, the appearance of the Internet, the pervasion of social media, and new careers of social media influencer or social media content creators. This generations prefers following others on social media and being followed, creating content, and learning about the world through social media online as opposed to visiting physical entertainment places and hang-outs (Halliday and Astafyeva, 2014). In order to better engage with this cohort, who are growing up in an increasingly different world, it is essential to understanding how iGen inhabits the digital world, shapes technology, collects and shares information online, and uses social media.

The most Internet-dependent generation have blended their physical and digital worlds in a way that their previous generations have never envisioned (WP Engine, 2020). This can cause iGen to hold different beliefs and values to previous generations, and they have already made noteworthy changes (Hoxha and Zeqiraj, 2019). For

example, nowadays, the newest career is content creators on social media, or called "YouTuber". It not only can be a high-income job, but also impacts people's use of social media and internet. Moreover, it is notable that most social media content creators or social media influencers are iGens. Therefore, the faster that marketers familiarize themselves with iGen, the sooner they can create competitive advantages (Hoxha and Zeqiraj, 2019). iGen repsents a new set of beliefs, values and behaviors about how the world works (Koulopoulos and Keldsen, 2014). iGens undergo technical education earlier than their predecessors and are exposed to marketing at a young age (McCrindle and Wolfinger, 2010). Some iGens have already entered the workforce, either working for employers or running their own social media influencer business. In this way, iGens are dissimilar to their predecessors in terms of what they expect from and value in an employer (Castellano, 2019).

While it is challenging to assert whether the predominant differences between iGen and older generations are truly superior or inferior, these differences nevertheless reflect the societal changes in work, business, and culture. It is essential to appreciate how iGen experiences the world and views life. As future leaders, iGens tend to display ambition, open-mindedness, and commitment (Levin, 2017). However, they also seem less aware and knowledgeable about the nature of cybersecurity than older generations, which can potentially lead to various digital risks that they or their employers will face (Schiola, 2017).

If we expect to conquer these seemingly endless privacy invasions and data breaches and build a professional environment where cybersecurity is more than a

guarantee, it is crucial to examine the major Internet surfers, namely the iGen, to create new defenses. When iGens join companies, they have new rules regarding the Internet and Internet safety. Dismissing or glossing over iGen can therefore be highly damaging to business productivity, corporate profile, and social stability.

1.7.3 Commitment to Information Security

The literature has demonstrated that commitment is necessary for maximum benefits from information security awareness and training, the development of an information system security culture, the implementation of security controls, the reduction of security risks, and an effective security defense (McFadzean et al., 2006; Hu et al., 2007; Chai et al., 2011; Bulgurcu et al., 2010; Boss et al., 2009). Therefore, in this research, we propose the concept of iGen's commitment to information security as the research of interest and a tool to deeper understand the determinates of iGen's intention to share information online.

1.7.4 Research Questions

In order to combat the potential risks of iGen's interaction with cybersecurity, specifically in terms of their information sharing via social media, this research argues that we must first begin by understanding the antecedents to the iGen's intention to share personal information via social media. Furthermore, we must comprehend iGen's commitments to personal privacy and information security and how this influences their use of social media. By developing this understanding of iGen's social media use with respect to the sharing of personal information, we lay the foundation for developing information security measures for protecting the personal data of iGen social media users.

To accomplish this goal, we explore the concept of individual commitment to information security. Prior literature has demonstrated that commitment to information security is a prerequisite and is necessary for effective information security achievement (e.g., see Oltsik, 2019). In this research, we hence develop the concept of iGen's commitment to information security as a means of providing a deeper understanding of the determinants of the iGen's intention to share personal information on social media.

As shown by prior literature, when considering the importance of commitment for effectiveness of information security (Johnson, 2009), it is critical and necessary to comprehend the role of iGen's commitment to information security for their intention to share information online. This facilitates the understanding of the complex interaction between iGen's desired social media experience and the security of their personal information.

Our research is guided by the two following research questions. First, **what are the determinants of iGen's intentions to share personal information on social media?** Second, **how does iGen commit to information security on social media?**

Identifying the role of iGen's commitment will enable the relevant perception of iGen's social media use to be more complete. Online fraudsters are using increasingly complex schemes. To better prevent potential data breaches and defend against incoming cyberattacks, iGen's information sharing on social media and their commitments to information security are worthy of study to ensure all ages employing best practices. This paper aims to provide a deeper and complete understanding of information security by

concentrating on the impacts of iGen's commitment to information security on their information sharing behaviors.

CHAPTER II

LITERATURE REVIEW AND THEORETICAL FOUNDATION

2.1 Overview

To accomplish our goal, this study uses the generational cohort theory and the theory of commitment, which are explicated in the following sections. Additionally, we draw upon the prior literature to form the basis for a theoretical understanding of iGen's intention to share information on social media and their commitment to information security. We do so by exploring the emphasis on social media for iGens as well as their cybersecurity-related habits in regard to their use of social media and the sharing of personal information.

2.2 Generational Cohort Theory

Inglehart (1977) first proposed the generational cohort theory for the explanation of the concept and the characteristics of generations. The theory suggests that a "generation" can be distinguished by the sharing of similar values and personalities; these are often based on the specific periods in which they were born and the social locations in which they were raised that are distinct from other generations (Inglehart, 1977). "The term cohort refers to a group of individuals who have a common experience of an event within the same time" (Ryder, 1965). Generational cohort theory is founded on the principle that an individual's philosophy is shaped by their formative years (Ryder, 1965)

as a generation experiences a mutual historical, social, political, economic, and technological environment (Lantos, 2011).

During the formative years of each cohort, these environments, together with accompanying significant events, shape and establish a generation's core values and beliefs; this thus differentiates between and characterizes generational cohorts (Inglehart, 1977). The distinctive attitudes and beliefs form a generational identity, which may remain relatively unchanged throughout the lifetime of the generation and can significantly impact their behaviors (Parment, 2013). Therefore, when seeking to understand and solve problems related to a particular generational cohort, it is essential to understand their particular and unique motivations (Lissitsa and Kol, 2016).

Researchers note that generational cohort theory is based on two assumptions (Dou, 2006). One is a socialization assumptions, and the other is a scarcity assumptions (Dou, 2006). The socialization assumption proposes that an individual's core values were built on the socio-economic conditions before their adulthoods. This assumption asserts that it does not matter whether societal conditions change later in a person's life; their generational attributes and personal values will remain relatively stable throughout their lifetime (Inglehart 1977). In comparison, the scarcity hypothesis proposes that adults tend to subjectively extend the value of the lack of socioeconomic resources in their childhood and adolescence into adulthood (Dou, 2006).

Therefore, generations whose childhood is socioeconomic insecure are more conservative, but generations whose childhood is socioeconomic secure are more liberal (Dou, 2006). Consequently, individuals' values and preferences change across

generational cohorts (Conger, 1997; Rogler, 2002). In particular, core value changes across generations tend towards be greater in countries with higher rates of economic growth (Abramson and Inglehart, 1995).

The generational cohort theory may contradict some traditional beliefs that people change or mature over time and that beliefs and behaviors are the consequence of aging (Costa and McCrae, 1999). In particular, around one third of studies include age as a linear variable, which considers the effect of age is maturational, instead of a categorical variable, which considers the effect of age is cohort (Jackson et al., 2003). In reality, generational cohort theory and maturational theory are not absolutely inconsistent but do offer competitive explanations (Sessa et al., 2007).

Generational cohort theory emphasizes the consistent or unchanged characteristics of a generation cohort, while maturational theory emphasizes the development of human beings. A generation is a social creation, and slow change is associated with rare significant events; in a traditional tribal community, for example, there may even be no appearance of distinct generations (Mannheim, 1952). Only when significant events occur and influence or change beliefs and behaviors is a new generation cohort demarcated (Sessa et al., 2007).

Therefore, Sessa et al. (2007) suggested that six characteristics to determine the scope of a generation in their study:

> (a) a traumatic or formative event such as a war, (b) a dramatic shift in demography that influences the distribution of resources in society, (c) an interval that connects a generation to success or failure (e.g., the Great Depression), (d) the creation of a "sacred space" that sustains a collective memory (e.g.,

> Woodstock), (e) mentors or heroes that give impetus and voice by their work (e.g., Martin Luther King), and (f) the work of people who know and support each other (e.g., Bill Gates, Steven Jobs) (Sessa et al., 2007).

For U.S. citizens, the invention and the growth of the Internet is the most recent significant event (following, for example, "the Great Depression, World War II, the Vietnam War, the Iraqi War, and September 11, 2001") that has impacted how iGen form their core values, beliefs, and lifestyles (Deborah et al., 2012). In actuality, many current labels can be applied over the world due to the assimilations of the world (McCrindle, 2014).

Prior research has found that older generations use technology passively, while younger cohorts use technology, such as social media, as an intimate aspect of their lives (McHenry and Ash, 2010). To this end, generational cohort theory, based on the extant literature, suggests that generational attributes should be considered to develop theories of technology adoption, such as the utilization of social media (Shirish et al., 2016).

Moreover, Padayachee (2017) illustrates that technological applications, such as social media, are enhanced by the study of generational cohorts. In other words, generation cohorts provide a unique perspective compared to other societal factors for studying human intention or behavior towards technology adoption and/or use (Padayachee, 2017). This study hence applies the generational cohort theory as the theoretical mechanism to demonstrate the need to further study the iGen's intention to share personal information on social media.

Generational cohort theory as an approach has been widely used in diverse fields of study, customizing the generational cohort's object of research. It is applied to understand the customers decision making in the business field such as iGen's decision making of their online shopping (Thangavel et al., 2019) and characteristics of YGen's attitude to spots business (Bennett and Lachowetz, 2004), to identify different generations' preferences and purchase patterns in the field of retailing (Carpenter and Moore, 2005), to maintain and boost productivity of workplace in the field of management (Martin, 2005), and to conceive marketing strategies in the field of tourism (Niemczyk et al., 2019) and so on.

In addition, in the social sciences field, the theory has been applied to understand people's attitudes and values (Davis, 2004), political partisanship (Greenberg, 2003) and political activity (Soule, 2001). For example, it was employed to examine participation in peaceful demonstrations in the US during the Vietnam War era (Dunham, 1998).

In the field of education, the theory has been used to investigate the integration of information communication technology in education (Padayachee, 2017), to explain the impact of YGens in higher education (Haynie et al., 2006), to identify the pattern of information-seeking (Weiler, 2004), to understand and evaluate the utilization of library services (Gardner and Eng, 2005), and to develop students' learning formats (Oblinger, 2003).

Finally, in the field of healthcare, the theory has been used to investigate and improve patients experience in digital era (Alkire et al., 2020), to understand both patients and heath care providers (Berkowitz and Schewe, 2011), to explore and improve

nurses' commitment to organizations (Jones, 2011), to develop effective health recruitment approaches (Schoo et al., 2005), to develop primary solutions to the challenges for nurses at care-frontings (Kupperschmidt, 2006), to understand and respond to changes in healthcare education (Schmoll and Moses, 2002), to understand, adapt to and improve the work environments of healthcare (Schofield and Fletcher, 2007), and to identify and improve generic abilities of physicians (Stumbo et al., 2007).

2.3 iGeneration

The literature proposed a diversity of names for people who were born after 1995. IGen is defined by its media, technology, and Internet use. Their habit of digital or online communication is not something they need to learn because they are electronic natives (Geiger, 2018). They assume that everyone has a social media presence, website, or smart device (Twenge, 2017).

2.3.1 iGen and Technology

The undeniable and most significant influence on iGen is technology (Wright, 2019). The iGen has demonstrated its proficiency and comfort with technology at a much earlier age than previous generations (Palley, 2012). The generation "grew up in a sophisticated technological environment", which enables iGen to be more proficient in technology than their predecessors (Salleh et al., 2017). The extant study found that 71% of iGens' typical entertainment consumption is online videos, and around one third of the videos are viewed from their mobile devices (Velasco, 2017). The iGen has never experienced life before the Internet, hence why they are called iGens or digital natives (Prensky, 2001).

Moreover, prior research found that 52% of iGens were more confident with the tech skills that employers needed than previous generations, and iGen believed that technology change the work and jobs in a positive way; In total, 80% of them believe technology will create a more equitable and innovative work environment (Dell, 2018). It is evident that the majority of iGens believe that technology is positive and is engrained into both the workforce and daily life; they aspire to work for companies that apply cutting-edge technology and are able to mirror their personal attributes (Levin, 2017). The iGen expect highly personal interactions and immediate-response data access at an innovative workplace (Twenge, 2017). Based on a recent study, 50% of iGens believes that virtual reality will be implemented within no more than three years; Moreover, 92% of iGens believe that the way they behavior on the Internet will significantly affect the world from all aspects (CSM Newsdesk, 2019).

2.3.2 iGen and the Internet

The Internet as a human experience is an integral part of iGen's identity (Mobile ID World, 2017). The iGen switches seamlessly their daily life to the digital world (WP Engine, 2017; WP Engine and The CGK, 2017). They cannot imagine living without the Internet and mobile device, because it is like oxygen to them, which results in iGen's savvy in technology and the Internet (Herosmyth, 2020; Bilderlings, 2018). iGens connect to the world through the Internet for daily life by default (Törőcsik et al., 2014). According to a survey by Anderson and Jiang, 45% of the iGen were online almost constantly in 2018; this figure is nearly double what it was three years previously, at only 24% in 2015 (Anderson and Jiang, 2018). Additionally, 44% of iGen reported themselves

to be online several times a day. Combining this number with the 45% of iGen online almost constantly, the study concluded that 89% of iGen are online multiple times a day (Anderson and Jiang, 2018).

Furthermore, a recent study by Brown asserts that 55% of iGen feel uncomfortable going more than four hours without the Internet, and the Internet determines their daily activities (Brown, 2019). Correspondingly, a total of 59% of iGen believe that online shopping is more convenient and will become dominant over offline stores; they also expect all shopping to be online in the 10 years (WP Engine, 2020).

According to a study conducted by WP Engine (2020), 86% of iGen use the Internet mainly for social media and entertainment, whereas older generations use the Internet primarily as an information source. In other words, iGen find more fun, connection, and emotion on the Internet. This demonstrates a change from their predecessors' utilization of the Internet as an information tool to iGens' utilization of the Internet as an entertainment tool. Moreover, 64% of iGen believe that their decisions will be driven by the Internet, which will become a daily norm in five years; specifically, 57% of iGen believe that what they do daily will be determined by the Internet. A total of 60% of iGen believe that their online reputation will affect their lives, such as their dating options, and 71% of iGen believe that online activities, such as social media posts and purchase histories, can affect their job offers. These figures demonstrate the likelihood that the Internet will become and is already becoming an integral part iGen's life (WP Engine, 2020).

Notably, Anderson and Jiang's recent study illustrated that the frequency of iGen's Internet usage is different by gender, race, and ethnicity. In the iGen cohort, females are more likely to be constantly online than males, and Hispanics are more likely to almost constantly use the Internet than their white counterparts (Anderson and Jiang, 2018). More specifically, 50% of female iGens are more likely constantly online, whereas 39% of male iGens are more likely constantly online; moreover, 54% of Hispanic iGens are more likely to almost constantly use the Internet, whereas 41% of white iGens are more likely to almost constantly use the Internet (Anderson and Jiang, 2018).

2.3.3 Personalization

According to Criteo's report, iGens state that they are personally independent and want to be different from others. In total, 49% of iGens think that unique products are vital and attractive (Pruett, 2018). With their willingness to challenge and evolve the formed concepts, uses, functions, and forms of all things, iGens therefore expect each product to be customizable to their style own. Similarly, they strongly value their individuality and tend to embrace the differences of other people (Pruett, 2018). Inclusion and individuality are hence the two principles that most impact iGen and give the digital natives a singular sense of style (Pruett, 2018). Alongside personalized products, iGens expect personalized interactions and conversations (Schneider, 2015). According to an extant study that was conducted in the larger U.S. cities, iGens dislike and are less likely to respond to generic emails, such as those that start with universal regards (e.g., "Dear Student/Customer"; Schneider, 2015).

The youngest generation of the Internet users pursues "hyper-customization" or personalization and believes that online experiences should to be personalized across websites and apps (WP Engine, 2017; WP Engine and The CGK, 2017). With the abundant personalization in their real world, they are looking for the same in their digital world (Geiger, 2018). As Kearney asserts, iGens' motto is "Unique is the new cool," in comparison to Millennials' major trends being merely "cool" (Hoxha and Zeqiraj, 2019).

With countless information and products, the iGen is able to seek out exactly what attracts and relates to them. A Google study stated that:

> for iGen, what's cool is also a representation of their values, their expectations of themselves, their peers, and the brands they hold in the highest regard (Smithson, 2018).

The iGen use products that can "express their individuality and unique sense of identity"; they prefer products and services that are seen as creative, unique, and cool (Hoxha and Zeqiraj, 2019).

A recent study conducted by WP Engine (2020) revealed the following findings: 70% of iGen believe in personalization, and 45% of iGen expect personalization. In total, 62% of iGen believe websites should know what they like, want, or need before they tell the Internet; if they do not, iGens are more likely to stop visiting those websites. Moreover, 55% of iGen believe that the Internet will soon interact with them like a human by exhibiting personalized emotion. Finally, the study revealed that 52% of iGen believe that Internet can calculate their online reputation and accurately predict if a

person can be approved for a loan; that is, they believe that the Internet can act as credit scores do (WP Engine, 2020; WP Engine and The CGK, 2017).

Additionally, the iGen has grown up in a hyper-targeted marketing environment. Over half (56%) of the iGen want to write their own job descriptions, and 62% want to customize their career path (Levin, 2017). These figures reinforce that the iGen is accustomed to personalizing everything for themselves, from newsfeeds to product features (Fisher, 2014).

2.3.4 iGen and Visual Content

Although the technology revolution is affecting all generations, iGen are impacted the most uniquely by visual contents as a primary means of entertainment, communication, sharing, and learning (Chamberlain, 2017). A study conducted by Chamberlain found that iGen could watch 68 videos in a day across five social media platforms (Chamberlain, 2017), which indicates that they are able to sort visual contents faster than older generations (Velasco, 2017), and they can quickly determine the value of those visual contents (Manifest, 2019; Bradley, 2018).

Similarly, Criteo's report of 2018 showed that iGen spent more time on mobile devices and watched more videos than older generations (Pruett, 2018). They spent an average of 11 hours per week on a mobile device and watched an average of 23 hours of videos a week, which is almost one full day spent watching content (Pruett, 2018). Criteo's study also indicated that iGen's favorite social network was the most visual one such as YouTube (Pruett, 2018) or TikTok, where they could stream more content. The study results recommend that businesses and marketers learn how to use visually driven

platforms and optimize both their photos of the brand and product and their social media presence online (Pruett, 2018).

According to a study by Manifest (2019), iGens stream online videos for learning something new, browsing new products, and various other entertainments that help them escape from their daily stresses (Manifest, 2019). A similar study reported that 52% of iGens are more likely to watch a video that makes them laugh (Velasco, 2017). Visual contents on social media enable iGens to reduce stress and free their minds from the required work and activities that can cause stress (Manifest, 2019; Bradley, 2018).

The way that the iGen uses the platforms of visual content is different from the generations before them (Manifest, 2019; Bradley, 2018). Another study illustrated a similar finding that the iGen use YouTube in their daily lives in a different way to older generations (Velasco, 2017). Around 60% of iGens enjoy learning on visual content platforms rather than learning through textbooks or group activities, either for their school subjects or beyond (Pearson, 2018). Similarly, according to a study by Ipsos, 80% of iGens said that video platforms facilitate them improving their knowledge, and nearly 70% of iGens said that video platforms help them acquire skills that will help them achieve their future wealth (Anderson, 2018).

Unlike other generations, who generally avoid advertising, iGens do not reject advertisings but expect authentic content in advertisements (WP Engine, 2017; WP Engine and The CGK, 2017). In particular, they prefer videos that are trustworthy, informative, entertaining, and tell stories; they favor branded content and adverts that simply leave them with positive feelings, as opposed to visual content that aggravate their

insecurities and negative emotions (Manifest, 2019; Bradley, 2018). For example, one of the iGen's favorite types of branded content advertisement are unboxing videos, which shows people opening product packages in front of the camera. Moreover, iGens welcome authentic reviews from real customers based on their real experiences (Manifest, 2019; Bradley, 2018).

2.3.5 Social Ability

According to the study, nearly one third of iGens state that everyone is and should be treated as equal (Pruett, 2018). Currently, 80% of iGens are largely in favor of the Black Lives Matter movement, 74% of iGens support transgender rights, and 63% of iGens endorse feminism and believe that these movements should be acceptable in society today (Velasco, 2017). Those social perspectives of iGen ensure that social media is iGens' favorite place to connect to other people, communities, and societies; they are able to quickly and easily find the people and communities who hold the same views as them, and they are able to connect with worlds that they may not have been able to reach in the physical world (Velasco, 2017).

Social media impacts how iGens interact with the world. Nearly 60% of the iGen start their social life online; 50% feel more comfortable and 70% feel more convenient to communicate with people on the web than in person (Palley, 2012). Nearly 97% of iGens use at least one social media app or website, and About 50% were online "almost constantly" (Anderson and Jiang, 2018; Dimock, 2019).

However, the iGen has mixed views regarding the impact of social media on their lives, with half perceiving a majorly negative versus half perceiving a majorly positive

impact (Beck and Wright, 2019). Some iGens shared concerns about their social ability. For example, someone commented that social media made it harder when people socialized in real life because they had used to not interacting and communicating with people in real life; and someone complained that social media

> provide fake images of someone's life, and it makes me feel that their life is perfect when it is not (Beck and Wright, 2019).

Researchers believe that people who stare at their phones excessively during their formative years will struggle to interact relationally with others (Turkle, 2011).

2.3.6 Multiple Tasks

As the first generation that explore endless information on the Internet (Turner, 2015), the iGen can quickly adapt to multiple information sources, and they can process information more quickly than their previous generations due to the use of apps such as Snapchat (McCullough, 2018). iGen has the skills to filter and distill limitless amounts of information exactly to their preferences and interests (Brown, 2019). Moreover, the iGen prefers graphics before text (i.e., the "less is more" approach). They also believe in simplification and quickly reaching the point of a message because a short attention span is a typical characteristic of the iGen (Törőcsik et al., 2014).

Technology and the Internet have shaped iGens to process and multitask in parallel, allowing them to transit fast from one task to another (McCrindle and Wolfinger, 2010). In school, they are able to do research on their smartphone, take notes on their

notebook, edit files and finish their work on their laptop in front of the TV, all while facetiming a friend (McCullough, 2018; Beall, 2017).

2.3.7 Moving Fast

iGens are always connected to their devices, which allows them to feel instant emotions, such as gratification or hurt, and they expect to find what they need immediately (Turkle, 2011). They still conduct face-to-face communication, but they want it quick, concentrated, and actionable; they expect others around them to move as fast as they do (Levin, 2017). The current way of communication does not give iGens sufficient time to deeply consider complicated issues and questions, which has reduced the time they can spend to think (Turkle, 2011). The instantaneous online communication and edge-technology applications do not give iGen downtime and daydreams any more (Turkle, 2011).

2.3.8 Mixed Views of Money

The iGen is ambitious, but in a survey conducted by LinkedIn, only 1% list salary as a priority, and 84% of respondents view career progression and growth as their most important priority for evaluating future employers. However, 56% of iGen believe that salary is important in the long term, and 59% of them would learn professional skills in order to make more money (Poague, 2018). iGen appreciates other valued benefits provided by their potential employers, including opportunities for schedule flexibility and global travel (Levin, 2017). Interestingly, iGen is motivated by financial incentives (Abramovich, 2019).

To advance our understanding of iGen in the information and cybersecurity environment, the following sections will present the results of the extant literature on the cybersecurity and information sharing behaviors of iGen.

2.4 iGen and Social Media

In total, 53% of iGen think social media has the biggest impact on their generation (Velasco, 2017). As evidence of this, 69% of users of TikTok, the most popular social media in the world in 2020, belong to iGen (Kapoor, 2020). iGen like to voice their opinions across social media (Pruett, 2018). As a digital native generation, iGen is the biggest group of content makers on social media such as YouTube and TikTok among all generations (Maguire, 2020).

An existing marketing study has indicated that businesses or brands targeting iGen should engage in social media such as TikTok to gain iGen customers (Maguire, 2020). Many brands have successfully demonstrated that their engagements with iGens on social media boosted as much as 90% of their revenue. Their techniques included interacting with their customers across social media channels and merging online activates with offline activities (Pruett, 2018).

Internet-enabled social interaction as part of the human experience is an integral part of iGen's identity (Stover, 2017). Roughly 97% of iGen are active on one or more social media platforms, and almost half of them connect to social media constantly (Anderson and Jiang, 2018; Dimock, 2019). They use mobiles and social media by default in their daily life for communication and entertainment (Törőcsik et al., 2014).

Through the frequent use of social media at a young age, iGen's social norms have been significantly modified compared to prior generations. They seamlessly switch between online and offline activities and do not differentiate between what is public and what is private (Beck and Wright, 2019). Besides the impact on how they interact with the world, 42% of iGens feel social media directly affects how they perceive themselves (Seymour, 2019). Additionally, social media has prompted iGen to consume information differently to the generations before them (Schneider, 2015).

iGen predominantly uses social media to view interesting content, whereas the older generation may use social media to keep in touch with friends (WP Engine, 2017; WP Engine and The CGK, 2017). However, iGen can still conduct an emotional investment in developing a friendship by closely following a friend over social media (Beck and Wright, 2019). According to a survey, 60% of iGens prefer using social media to contact and interact their school friends (Schneider, 2015). Although previous studies have shown the impact of social media on how iGens interact with the world, most iGens feel more comfortable socializing with people on the Internet rather than in person (Palley, 2012). Conclusively, iGens are more motivated to communicate on social media (Seymour, 2019). Additionally, according to the survey of 2014, 81% of iGens take advantage of social media as information resource besides using it to keep in touch and interact with friends (Schneider, 2015).

The Most Memorable New Product Launch survey found that iGen uses social media to get known about new products to make their purchase decision (Schneider, 2015). iGens screen brands, follow the brands that represent their ideas, and

communicate with their peers who like the same brands and products through social media; this is likely to cause brands that are not fully engaged with social media lose the entire cohort of iGen (Schneider, 2015). iGen expects two-way communication with brands on social media and prefer the brands that make direct communication easy and seamless (Pruett, 2018).

Other significant social media uses by iGen include selfies, photo uploads, and content created (Kim and Chock, 2017), and personal information sharing (Misoch 2015). Consequently, iGen is much more attached to and gratified by social media usage than XGen or Millennials (Kircaburun et al., 2018). Although iGen is more involved in social media in most ways, they rarely use social media for or as a management tool or educational and informational gratification, which are predominant ways that Millennials use social media (Kircaburun et al., 2018).

Despite the ubiquity of social media in iGen's lives, they do not have a consistent consensus about the ultimate impact of social media on their generation cohort. Significantly, 45% of iGen does not believe the impact of social media is either negative or positive; 31% of iGen believe the impact of social media is positive; and 24% of iGen believe the impact of social media is negative (Anderson and Jiang, 2018).

According to a study, iGen believes that the impact of social media is positive through its implementation of connectivity with the world. Respondents emphasized that social media enabled them to connect and interact with people who have similar interests, communicate with family, friends, and new people more easily, and access news and information more conveniently (Anderson and Jiang, 2018). iGen also believes that social

media is a place for entertainment, self-expression, getting support, and learning new things (Anderson and Jiang, 2018).

In contrast, iGens who believe that social media has a negative impact on them perceive that social media misrepresents reality, gives an unrealistic reflection of someone's lives, spreads too much misinformation and rumors, harms relationships between humans, and leads to bullying and less meaningful human interactions (Anderson and Jiang, 2018). Moreover, these iGens believe that their peers spend too much time on social media, which influences them to give way to social pressure and results in psychological issues due to social comparison and cyberbullying (Anderson and Jiang, 2018). Although the constant presence of social media in iGen's lives allows them to stay connected with their community and the world, it can also make them feel depressed, have low self-esteem or anxiety; moreover, constantly staying on social media can leaves iGens exhausted (Manifest, 2019; Bradley, 2018).

2.5 iGen and Cybersecurity

Although iGens are digital natives, false confidence in their technological savvy can make them careless when facing cyber threats (Lunarline, 2018). Surveys have shown that iGen is the generation with the least concern about cybersecurity. As the generation that is most confident in the law enforcement of cybersecurity, iGens expect the authorities to combat cybercrime more than they expect real-world crime among all generations (Consultancy.uk, 2015).

Recent research from Microsoft found that iGen is the generation most vulnerable to cybercrime. Through examining online tech support scams, the research indicates that

males particularly within this generation are most at risk (Lunarline, 2018). Cybersecurity strategist Adenike Cosgrove stated that iGen lacks cybersecurity awareness, which brings a great, unexpected threat to organizations (Cosgrove, 2018). The newest research illustrates that iGen cannot identify threats such as ransomware and phishing as accurately as older generations (Beckingham, 2019).

Studies show that iGen expect the same secured Internet environment that is valued by their predecessors, such as effective detection of fraud or ID theft, effective blocking from malware, and trustworthiness and authenticity of websites (WP Engine, 2017; WP Engine and The CGK, 2017). However, they actually step away from Internet security and privacy because more iGen share their personal information with predictive websites and apps that can forecast what they want or need, whereas anonymous web visiting costs more of their manipulations to discover what they want or need (WP Engine, 2017; WP Engine and The CGK, 2017).

2.5.1 Ransomware and Phishing

Of all generations, iGen has the least knowledge of ransomware and phishing; they are less likely to accurately perceive ransomware and phishing area (Abel, 2018). A recent Webroot survey found that only 23.7% of iGen were able to accurately define ransomware compared to 47.6% of Baby Boomers (Abel, 2018). Similarly, various surveys have shown that only a few percent of iGen were able to clearly define what ransomware and phishing are (Beckingham, 2019; Grothaus, 2019). They were also confident that they would not fall for phishing scams (Grothaus, 2019), despite being the generation that is most likely to forward emails from unknown senders, click on malware

links, and spread malware and other cyber threats (Beckingham, 2019; Grothaus, 2019; Abel, 2018).

2.5.2 Digital Payments

Almost everybody in the iGen is conducting online shopping or online payments. This generation is likely to comfortably pay online using their debit or credit cards without awareness of the risks of cyber threats associated with online payments (Duma and Gligor, 2018). iGen had fewer concerns about privacy and security when using mobile payment apps, such as Venmo, in comparison to directly paying online with credit and debit cards (Mastroianni, 2016).

In regard to cryptocurrencies, research has found that iGen can be divided into two categories(Duma and Gligor, 2018). The first category knows the definition of the bitcoin, the blockchain technology and the mining process, the names of other cryptocurrencies, and the main advantages and disadvantages of bitcoin; This category trusts cryptocurrencies for online payments and assumes them to be safer than conventional online payment methods; The second category may not know about the blockchain technology, names of other cryptocurrencies, and the advantages or disadvantages of the bitcoin, but they still show potential interest in investment in and use of the bitcoin in the future (Duma and Gligor, 2018).

2.5.3 Passwords

Passwords are the first security defense to deter cybercrimes. However, a recent McAfee survey indicated that many iGens reused the same password for several online accounts and authorize login access to third-party applications through networking

websites or apps (Sarang, 2018; Grothaus, 2019). The entire digital life of a cybercrime, iGen victim could thus be exposed by a cybercriminal cracking only one password. iGen rarely differentiates passwords across various accounts or uses a password manager with proper precautions in place (Sarang, 2018). However, different research has reported that 76% of iGen have turned on two-factor authentication for their online accounts for effective defense against unexpected access (Grothaus, 2019).

2.5.4 Public Wi-Fi

Many iGens expect authentic, free, and secure Internet at all times (WP Engine, 2017; WP Engine and The CGK, 2017). They are more likely than other generations to connects to public or unsecured Wi-Fi networks without security concerns (Abel, 2018). Internet service providers (ISPs) track and communicate with each device using its unique Internet protocol (IP) address. Connecting to unsecured public WiFi could provide cybercriminals a pass to eavesdrop on computer processes, steal confidential information, and attack devices by spreading malware such as Trojan horses (Sarang, 2018).

2.5.5 Cybersecurity Training

iGen anticipates an innovative workplace made of new technology (Twenge, 2017), but the new technical applications forming innovational workplaces may compromise data and cybersecurity (Levin, 2017). When new apps come with no adequate security measures as standard, iGen is accustomed to seeking an online solution to technological problems through crowd-sourced knowledge, and this may post significant cybersecurity risks (Security News Desk, 2016). The iGen views the traditional lecture-based trainings negatively due to their ineffectiveness, but a "values-

based approach" better engages iGen in good cybersecurity behaviors, such as emphasizing "values of shared responsibility in protecting our community" (Skill, 2019).

2.6 iGen's Information Sharing

iGens tends to share information on peer-to-peer social media sites and messaging apps, such as Snapchat, Vine, and Instagram, because they expect to access, retrieve, share, exchange, and store various types of information quickly and easily (Jones and Hosein, 2010). This generation are continuously involved in the online activities and interactions (Kitchen and Proctor, 2015), especially over social media (Turner, 2015). Additionally, iGens are sharing increasingly more of their personal lives online (Taylor and Keeter, 2010). They thus expect brands to use their shared information, such as their interests, hobbies, music, and sports, to have personalized communication with them (Schneider, 2015).

In sharp contrast to older generations, who are generally more concerned about anonymity online and keeping personal information private, iGen is comfortable sharing personal information in order to personalize their experience (WP Engine, 2017). More iGens than members of other generations choose a predictive Internet, and 50% of iGen would not return to a website that cannot anticipate what they liked or needed (Kreamer, 2018).

This indicated the desired "hyper-customization" of iGens' online world (Geiger, 2018). They seek to use products that can express their individuality, thus preferring products and services featuring creativity, customization, and uniqueness (Hoxha and

Zeqiraj, 2019). iGen has grown up in a hyper-targeted marketing environment, enabling them to personalize everything from news feeds to product features (Fisher, 2014).

With a wealth of information at their fingertips, iGen expects a more predictive and personalized service to filter endless information. This leads to iGen's priority of personalization over privacy by trading personal information across a number of mobile apps and Internet platforms without hesitation (Schiola, 2017). For gaining a tailored experience that efficiently fits their needs and interests, iGens rarely hesitate to share sensitive information online instead of keeping their information private (Schiola, 2017). As Sarang asserts, the more iGens share data sharing and use social media, the more they are unknowingly exposing themselves and their networks to security risks (Sarang, 2018).

Authenticity is the characteristics of iGen from offline to onine. A total of 50% of iGen believe that Internet are as authentic as what they expected (WP Engine, 2017). Extant research indicates that iGen values authenticity overwhelmingly more than other generations; iGen prefers that products have reviews from real customers who are not incentivized for their compliments (Schiola, 2017). This does not only apply for online shopping; iGens also expect every online share and interaction to be authentic because the generation genuinely shares so much of themselves and expects the same in return (WP Engine, 2017).

However, this kind of authenticity in online sharing, primarily via social media, leaves iGen exposed to an incredible number of cyber risks and threats related to their

personal information. The golden rules of cybersecurity may hence be difficult to apply for iGens (Schiola, 2017).

2.7 Theory of Commitment

The theory of commitment was developed by Meyer and Allen in 1997. It has demonstrably become the predominant model for studying the concept of commitment through its widely adoption and enhanced measurement of commitment constructs (Jaros, 2007).

The theory of commitment firstly described employees' commitment to their organizations, which has been defined by the many organizational scientists. The concept of employee's commitment emerged in the research in the early 1970s. The breakthrough occurred when Porter et al. (1974) defined commitment as

> (a) strong belief in and acceptance of the organizational goals; (b) willingness to exert effort on the part of organization; and (c) a definite desire to maintain organizational membership" (Kaur and Sharma, 2015).

However, the most frequently cited definition of employee's commitment was developed by Meyer and Allen (1991), who state that commitment is

> a psychological state that (a) characterizes the employee's relationship with the organization, and (b) has implications for the decision to continue or discontinue membership in the organization (Meyer and Allen, 1991).

This widely proliferated definition attempts to integrate numerous definitions of employee's commitment in the literature and create consensus between them (Jaros, 2007).

Later, the theory of commitment was adopted in much wider fields. Researchers describe commitment as a stabilizing or obliging force that determines an individual's attitudes and behaviors (Meyer and Herscovitch, 2001). This commitment model proposes that a person commits three simultaneous yet distinct mindsets that are labeled as the following: affective, continuance, and normative commitment (Meyer and Allen, 1991).

2.7.1 Affective Commitment

Affective commitment originally means a sense of belonging or being tied to organizations by identification and involvement, primarily through work experiences (Jaros, 2007). It is a form of psychological attachment to groups that people like and choose to identify with (Allen and Meyer, 1990). With affective commitment, a person is not only happy but is engaged in a proactive manner to make contributions to their organization (Gautam et al. 2004).

Affective commitment is led by social identity being formed by their relationships and connection to certain social groups (Tajfel and Turner, 1986). To affectively commit to the organizations is demonstrated by characteristics such as acceptation of values, support of goals, and a strong desire to associate with the organizations (Perry, 2004).

According to extant studies, there are certain organizational variables are influenced by affective commitment. In particular, affective commitment can influence characteristics such as advancement career opportunities, job security and development, leadership behaviors, organizational structures, organizational environment, organizational/supervisory support, fair treatment, satisfaction with compensation,

acceptance of innovation, and working hours (Lee and Corbett 2006; Demirtas and Akdogan, 2015).

In a broader context, affective commitment refers to the emotional and affective link to an individual's target (Meyer and Herscovitch, 2001; Allen and Meyer, 1990). It is a psychological tie to an individual's desired goal (Allen and Meyer, 1990). A person who is happy and engages proactively to contribute to their targets characterizes affective commitment (Gautam et al. 2004). It is rooted in emotion such as enjoyment, feelings, and desires, and hence guides individuals' attitudes and behaviors (González and Guillén, 2008). Affective commitment also suggests that an individual's previous positive experience is affectively related to their target (Jaros, 2007).

More specifically, the affection or pleasure that a target produces can be induced by an individual's involvement in a set of active behaviors, or the recognition of the value relevance of the set of behaviors (Meyer and Herscovitch, 2001). In brief, affective commitment is an individual's psychological state in which they like to conduct certain behaviors derived from their emotions and willingness (Allen and Meyer, 1990).

2.7.2 Continuance Commitment

Continuance commitment originally refers to commitment based on necessity, which denotes the perceived economic and social costs associated with leaving an organization (Jaros, 2007). With continuance commitment, individuals feel they must stay in the organization for a longer period of time because they have already invested energy and effort in that organization (Jacob, 2007).

In a broader context, it is the psychological state in which individuals are invested in a decision that they have made and maintain continuance in their behaviors regarding to this decision (Meyer and Herscovitch, 2001). Continuance commitment hence is the product of an individual's perceptions of investments such as time, effort, and money (Jaros, 2007).

Continuance commitment is characterized by an individual's recognition of the rewards and benefits associated with a continuance related to a decision or the costs or negative consequences associated with a termination of a course of action (Allen and Meyer, 1990). Allen and Meyer's define continuance commitment as

> a tendency to engage in consistent lines of activity based on the individual's recognition of the costs (or lost side-bets) associated with discontinuing an activity (Allen and Meyer, 1990).

In brief, continuance commitment is an individuals' psychological state that is necessary to conduct certain behaviors to prevent negative consequences (Allen and Meyer, 1990).

2.7.3 Normative Commitment

Normative commitment refers to commitment based on a feeling of obligation towards an object or a target (Allen and Meyer, 1990; Tandon and Ahmed, 2015). This third form of commitment was proposed more recently than affective and continuance commitments (Meyer et al., 2002). With normative commitment, individuals expend effort and perform actions due to customariness or obligation (Beck and Wilson, 2000). For example, normative commitment makes employees feel obligated to stay in the

organization, often because employees feel that it is the "right thing to do" (Jha, 2011). Normative commitment can cause an individual to expend effort and perform actions due to obligation (Beck and Wilson, 2000). In some cases, a reciprocal exchange with a given target can induce an individual's affective commitment (Jaros, 2007). Extant research indicated that normative commitment occurs when an individual receives benefits and perceives the need to reciprocate (Meyer and Herscovitch, 2001).

Normative commitment is derived from moral norms, which are connected to one's desirable traits and moral virtues (Jaros, 2007). It is beyond a feeling and is the conscience about what is right (González and Guillén, 2008). Normative commitment is derived from the sense of moral accountability and responsibility, and it is guided by a person's willingness to account for their behaviors (González and Guillén, 2008). Therefore, normative commitment is characterized by individual's guilty feelings when they fail to conduct behaviors that comply with moral norms or virtues (Jaros, 2007). In brief, normative commitment is a psychological state in which individuals feel that they should conduct certain behaviors to fulfill obligations and responsibilities. Extant literatures showed a diversity of factors of normative commitments. For example, stronger normative commitment of employees was produced by job satisfaction, job involvement, and occupational commitment (Lee, et al., 2000; Meyer et al., 2002; Jaros, 2007).

The impacts on affective, continuance, and normative commitments are not always unified (Chen et al., 2015). For example, job satisfaction, job involvement, and occupational commitment positively influence employee's affective commitment

stronger than normative commitment, but negatively influence continuance commitment (Lumley et al., 2011; Rathi, 2009). The work experience variables, such as organizational support and interactional justice, positively impact affective commitment stronger than normative commitment, but negatively impact continuance commitment (Lumley et al., 2011; Rathi, 2009). However, existing literature demonstrated that "personal characteristics such as age, gender, education, marital status, and position tenure" do not affect any of commitments (Meyer et al., 2002).

2.7.4 Application of Commitment Theory

The commitment theory has also been applied as the foundation to understand critical individual behaviors at workplace, "including turnover and citizenship behaviors, job performance, absenteeism, and tardiness" (Meyer et al., 2002). Withdrawal cognitions have negative relationships with turnover within all the three commitments and influence affective commitment the most (Meyer et al., 2002; Moynihan et al., 2000; Jenkins, 1993; Somers,1999).

Affective commitment negatively affects absenteeism, while normative and continuance commitment positively impact or have near-zero impact on this factor (Somers,1995; Gellatly, 1995; Meyer et al., 2002). Affective and normative commitment positively impact "job performance and organizational citizenship behavior", whereas continuance commitment negatively and barely influences them, respectively (Meyer et al., 2002). Finally, affective commitment negatively impacts of "self-reported stress and work-family conflict", while continuance commitment positively and normative commitment ineffectually impacts these (Meyer et al., 2002).

2.7.5 Commitment to Cybersecurity and Information System Security

Cybersecurity researchers have theorized that a commitment to cybersecurity can directly boost cybersecurity assimilation (Liang et al., 2007; McFadzean et al., 2006) and IS security achievement and can effectively reduce organizational risk (Johnson, 2009; Lee and Larsen, 2009). Although commitment alone cannot guarantee successful security defense, it is necessary for effectiveness of design and compliance with cybersecurity policies (Bulgurcu et al., 2010). After organizational security issues are identified, the commitment of executive or board level management can ensure the allocation of organizational resources to initiate security programs (Dutton et al., 2001).

The commitment to information system protection provides the blueprint for effective security design, the enhancement of the evolutionary strategies for security policies (Curtis, 2012), and the defense of potential countermeasures (Alam and Bokhari, 2007). An organizational commitment to private and public inter-organizational partnerships facilitates governance and compliance with cybersecurity (Curtis, 2012).

The commitment to cybersecurity can be presented by leaders or top management teams' thoughtfulness and adherence to a developed and practical framework (Shoemaker, 2019). Literatures demonstrated that an organization's commitment to cybersecurity are organizational committing resources to IS security (Johnson, 2009), organization's adoption of IS security (Hsu, 2009), top management teams developing and assigning roles and responsibilities for IS security (Backhouse and Dhillon, 1996), communicating the IS security vision cross organization (Patnayakuni and Patnayakuni, 2014), and effectively monitoring employee compliance (Herath and Rao, 2009).

Cybersecurity strategy implementation needs stakeholders' commitments and responsibilities at all organizational levels, external commitment through cooperative partnerships, and internal commitment to support the network infrastructure (Curtis, 2012). Consistently, research shows that a lack of commitment to cybersecurity is associated with poor security practice, high-security threats, and more vulnerabilities (Hsu, 2009). Motivating top management and employee's commitment is one of the critical approaches to promote cybersecurity in organizations (Curtis, 2012).

Moreover, extant research indicates leadership's commitment to cybersecurity are dominated and motivated by various drivers, such as

> pressures from business partners and ability to compete with other companies (Johnson, 2009), regulatory and mandates pressures, normative pressures through professional organizations, mimetic mechanisms of perceived best practices, and employees' compliance with regulations (Barton et al., 2016).

Empirical evidence demonstrated that external factors, such as energy, water, health, and finances, are also identified as the key drivers behind top management commitment in critical sectors of organizations (Holgate and Hardy, 2012). Coercive forces and mechanisms influence leadership's commitment (Teo et al., 2003) and directly influence leadership's involvement in information system assimilation (Liang et al., 2007). However, the curriculums to evaluate leadership's commitment are not clear (Johnson, 2009).

2.8 Research Gap in Information Security

In recent years, increasingly more academic and empirical literature appear to study iGen because characteristics of different age groups must be understood (Moschis et al., 2000). It is also true that information security researchers and defenders must develop a solid understanding of iGen in order to assert how to work with them. However, contrary to other generational cohorts or fields of study, not much is known about iGen in the cybersecurity context. Based on our literature review, there is a gap in the literature that can be identified as the role of commitment to information security on iGen's intention to share information online.

Additionally, there has been no research exploring the role of iGen's commitment to information security in affecting iGen's intention to share information online. To advance comprehension of iGen in the information and cybersecurity environment, the purpose of this study is to explore the concept iGen and its implications for cybersecurity through determining a model for the analysis of their information sharing intent. Specifically, this study aims to fill the research gap in the role of commitment to information security on information sharing and the factors of commitment to information security among iGen.

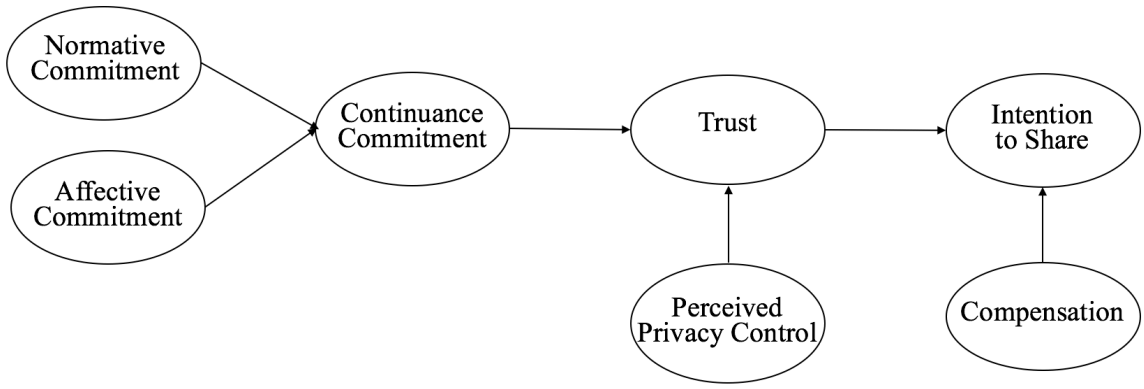
To advance comprehension of iGen in the information security environment, this research applies the generational cohort theory and theory of commitment to study iGens and their commitment to information security through determining a model for analysis of their intention to share information online. Therefore, this study aims to fill the research gap of what motivates iGen's intentions to share information online and how they commit to information security.

CHAPTER III

RESEARCH MODEL

This study focuses on the potential motivators of iGen's intention to share personal information on social media and their respective antecedents. Two factors that have been theoretically shown to motivate an individual's intention to share information in the information security literature are trust, an intrinsic factor, and compensation, an extrinsic factor. In the context of this study, trust refers to iGen's trust in social media, while compensation refers to the various kinds of incentives offered by social media for the disclosure of iGen's personal information. Additionally, two antecedents of trust are also identified for use in this model: continuance commitment and perceived privacy control. There are also two constructs affecting the continuance commitment: normative commitment and affective commitment. The research model is presented in Figure 1.

Figure 1: Research Model



3.1 iGen's Intention to Share Information Online

Customers sharing information has become a novel channel that enables businesses to attain valuable data for analyzing customer trends and improving organizational decision-making (Hajli and Lin, 2016). Research has shown that by leveraging customer data, businesses can better enhance strategic opportunities, which can then lead to the improvement of customer loyalty (Miranda and Saunders, 2003; Hajli et al., 2014). Therefore, businesses should utilize numerous methods of customer engagement to enhance customers' information sharing.

To this end, the iGen is more comfortable with the digital exchange of information and thus shares more information online than previous generations due to their expectations of customized products and technical knowledge (Schiola, 2017). However, at this time, little research has explored the antecedents to the iGen's intention to share information based on these unique expectations for social media; nor has the impact of security on the information being exchanged been examined. Hence, for the purposes of our study, the iGen's intention to share information via social media acts is proposed as the dependent variable.

3.2 iGen's Trust and the Intention to Share

Within the literature, trust has been commonly defined as "a faith or confidence that the other party will fulfill obligations set forth in an exchange" (Gundlach and Murphy, 1993). This denotes that trust is the degree to which people willingly depend on others, and it thus significantly impacts human behavior across numerous and varied situations (Mayer et al., 1995). Research on traditional and online businesses has showed

the important role of trust in business interactions (Kim et al., 2008; Chen and Dhillon, 2003); trust is the foundation for" building long-term relationships with consumers" (Doney and Cannon, 1997) and is a mechanism for improving relationship quality (Campbell, 1997). Therefore, establishing trust can reduce consumer privacy concerns and promote continued relationships with consumers (Milne and Boza, 1999).

Traditionally, private information is shared only with trusted entities (i.e., people or organizations) based on the protection of the application of a penalty for breaking the trust. For example, patients shared their health information with their health providers, and believed their private information will be kept confidential due to the restrains of law and professional ethics; Also, banks would be punished if they abuse their customers' financial information (Bansal et al., 2016). In this way, the penalties can prevent the abuse of private information to some degree.

However, due to the nature of social media applications, the ease of interpersonal digital exchanges of information, and people's varied concerns for a variety of cybersecurity breaches, these penalties are not wholly effective in preventing online information abuse; Therefore, trust plays a critical role in determining online activities, such as sharing personal information via social media (Bansal et al., 2016).

Correspondingly, in this study, trust refers to iGen's trust in social media, based on the reliability and integrity of the social media platforms (de Ruyter et al, 2001). In the context of social media, trust is iGen's willingness to depend on the belief in the integrity, ability, dependence, and un-opportunism of social media platforms. Additionally, prior research has found that trust significantly influences an individual's

information sharing (Dinev and Hart, 2006), and it is an antecedent of intention to share personal information online (Bansal et al., 2016). This leads to our first hypothesis:

H1: Trust in social media platforms positively impacts iGen's intention to share information.

3.3 Compensation and iGen's Intention to Share Information Online

As the collection and use of consumer information have numerous benefits for businesses, many business or marketers attempt to do so offer some certain forms of compensation as a means of enticing consumers to share; social media is no different. For this reason, the use of compensation has become more widespread, and its impact on consumer's intention to share information online may have important implications for marketers and policymakers when conceiving data collection strategies and privacy policies and regulations (Gabisch and Milne, 2014), particularly for iGen social media users.

It is important to note that compensation includes both monetary rewards and non-monetary rewards (Lee et al., 2013). Monetary rewards are physical gifts, such as cash, whereas non-monetary rewards are intangible gifts, such as customized services (Taylor et al., 2009) or free app use with no advertising.

One reason that it is important to explore the use of compensation in the context of the iGen is that prior research indicated that iGen is motivated by financial incentives (Abramovich, 2018). Moreover, extant literature has proven the effectiveness of the monetary rewards on an increase in the participation rate in surveys (Cobanoglu and Cobanoglu, 2003). Additionally, previous studies have also shown that compensation can

stimulate consumers' purchase intention as well as other behavioral intentions online (Hui et al., 2007).

Of particular importance to this study, prior literature has illustrated that adequate compensation can offset customers' privacy concerns, thus enabling them to compromise certain levels of privacy protection to trade their personal information or conduct more online transactions (Yang and Wang, 2009). Moreover, monetary rewards may not only stimulate information sharing but also alleviate misrepresentation intentions (Bentley and Thacker, 2004). Additionally, scholars have demonstrated that online users can tolerate improper access, unauthorized review, and use of their information for the gain of monetary rewards and utilization convenience, such as customized services (Hann et al., 2007).

Within the context of risk-benefit and utility theory, it is posited that monetary reward or compensation is the key factor for individual information disclosures (Xie et al., 2006). This is consistent with prior studies that shows that individuals possess a clear preference towards adequate compensation for access to their personal information (Gabisch and Milne, 2014).

In this study, we postulate that when monetary compensation is used as a reward, iGen will be more inclined to share their personal information. We posit that they are willing gain desired benefits in exchange for certain personal information. In contrast, when iGens are not rewarded in any form of compensation, they will be less likely to share their information. Thus, in this research, we hypothesize that the presence of compensation will lead to iGen's higher intention to share information on social media.

H2: Compensation increases iGen's intention to share information on social media.

3.4 Perceived Privacy Control and Trust

Within the literature, perceived privacy control has been identified as a potential factor that may influence individual's attitude and perceptions in an online environment (Keith et al., 2014). Perceived control refers to "a person's belief to significantly alter and predict a situation" (Perry et al., 2001). It stems from the belief of the amount of power that people can control over the objective (Skinner, 1996), "such as a situation or another person" (Bugental et al., 1989).

Personal information is created by the user; the social media platform then links an identifier to the personal information of that person, which creates an inherent controversy over ownership of personal information, hence users believe they own this information. However, these platforms may also believe that they own users' personal information, especially when data are created through users' behaviors or activities on the businesses' platforms (Jarvenpaa and Staples, 2001). Unfortunately, there has not been clear regulation that defines the ownership of users' activity information on the platforms. Therefore, in IS research, perceived control over personal information has been a critical topic within privacy and security studies (Belanger et al., 2002; Dhillon et. al. 2018).

Although national and international legal regulations are limited regarding to Internet users' control over their information access and usage (Corbett, 2013), studies on customers' privacy control as an important criterion of security evaluation are necessary.

The reason for this is that in online environments, when users perceive themselves as having less control of their information, their perceived risks of online sharing are increased and vice-versa (Weber, 2009). For example, Borchers (2001) illustrates that perceived privacy control is positively related to trust in online shopping. Similarly, Olivero and Lunt (2004) indicate that there is a direct effect between an individual's perception of control over information and their trust in trustees. Furthermore, Liu et al. (2005) and Joinson et al. (2010) found that the loss of perceived control mitigates customers' trust in an organization, and other previous studies have also demonstrated that the perception of privacy control promotes a level of general trust (Taddei and Contena, 2013). Likewise, Chang et al. (2018) demonstrate that the level of perceived privacy control can determine whether to trust other online activities, such as online banking.

It is notable that Trust is an individual's willingness to take risks (Mayer et al., 1995), and individuals have various propensities to trust due to their distinct personalities, ages, cultural backgrounds, and developmental experiences (Hofstede, 1984). In regard to social media, perceived privacy control is considered as a cognitive construct and the degree to which a customer perceives that they are allowed control over who and how their personal information is accessed, edited, and used through various privacy settings (Rohm and Milne, 2004).

Therefore, losing such control over personal information causes users to distrust those websites (Govani and Pashley, 2005). Hence, based on prior studies, it is postulated that the perceived privacy control provided by social media platforms is likely to

influence iGen's trust of a social media platform and therefore influence their intention to share information using that platform. With less privacy control, customers may perceive more possible opportunistic behavior by the trustee (Chang et al., 2018), which leads to the following hypothesis:

H3: Higher levels of perceived privacy control will increase iGen's trust in the social media platform.

3.5 iGen's Continuance Commitment to Information Security and Trust

Commitment plays a critical role with respect to information security (AlHogail, 2015). The most adopted and enhanced model to study on commitment is Meyer and Allen's three-component model of commitment, which describes an individual's commit through three simultaneous but distinct mindsets as continuance commitment, affective commitment, and normative commitment (Jaros, 2007). They are perceived distinct, because continuance commitment serves the theory from the behavior aspect, while affective commitment and normative commitment serve the theory from the perceptional aspect.

Continuance commitment refers to commitment based on the perceived economic and social costs due to terminating a behavior (Jaros, 2007). The literature has also conceptualized continuance commitment as the enduring motivation to maintain a valued relationship with a trustee (Moorman et al., 1992). Hence, based on prior studies' use of continuance commitment, this study proposes to use this construct to explore iGen's continuance commitment to information security in the context of their trust towards a social media platform. In this study, iGen's continuance commitment refers to iGen's

continuance desires to protect their personal information in an online environment. In other words, it is the degree to which iGen perceive that they need to protect their personal information from the trustee (i.e., social media platforms) and believe that an information breach or invasion of privacy by a social media platform would be economically and socially costly for them.

iGen's continuance commitment acts as a driver that ensures the safety of online activities and prevents information breaches and privacy invasions. iGens who have strong continuance commitment believe that protecting personal information in an online environment is a matter of necessity as much as desire and that the consequences of an information breach are serious. Strong continuance commitment to information security may also make iGen worry about the cost or disruption to life caused by an invasion of privacy.

Within the literature, prior studies have reported a negative relationship between continuance commitment and trust (Geyskens et al., 1996). To this point, in considering the serious consequences of an information breach, iGen with strong continuance commitment may be less likely to trust social media platforms. As trust is the confidence that iGens believe that the social media platform will act in their best interest to prevent an invasion of privacy and continuance commitment is iGen's commitment to preventing such an invasion, it can be argued that a high level of continuance commitment leads to a lower level of trust in social media platforms. This leads to the following hypothesis:

H4: iGen's continuance commitment to information security negatively impacts iGen's trust in social media platforms.

3.6 iGen's Affective Commitment to Information Security

Although Meyer and Allen's three-component model of commitment has been the most predominant approach applied in commitment-related research (Meyer et al., 2002), the relations between the three commitments have rarely been studied. This study will investigate the potential relations between them.

We discuss the role of iGen's affective commitment to information security in this study. Affective commitment refers to the degree to which iGen likes to protect their personal information in an online environment. In the context of social media, iGen's affective commitment is based on a general emotional attachment towards their privacy, thus it is a reflection of how much iGen likes or wants to protect their personal information and ensure information security. Affective commitment hence causes people to protect their personal information in exchange for security, confidence, enjoyment, or any other satisfaction that is derived from the privatization of their personal information (González and Guillén, 2008; Allen and Meyer, 1990).

To this end, if iGen are effectively committed to their privacy, they typically identify with the goals of personal information protection, such as preventing the potential privacy invasion, and usually perceive that they need to protect their information. Since continuance commitment reflects iGen's perceived sunk costs, such as privacy invasion, it can be argued that iGen with strong affective commitment may have strong continuance commitment. In other words, iGen's affective commitment may positively impact their continuance commitment, which leads to the following hypothesis:

H5: iGen's affective commitment to information security increases iGen's continuance commitment to information security.

3.7 iGen's Normative Commitment to Information Security

Differing from continuance commitment reflecting a "need" feeling and affective commitment reflecting a "like" feeling, normative commitment reflects a "should" feeling. It originally refers to the sense of obligation that employees should stay in their organizations, meaning that normative commitment represents a form of implied obligation that an individual feel towards others (Allen and Meyer, 1990) or the reciprocation of an obligation.

Normative commitment motivates an individual to expend effort and improve performance because it complies with social norms or customary, typically in the social sense (Beck and Wilson, 2000). In this study, we explore iGen's normative commitment to information security when sharing information on social media. iGen's normative commitment hence is the degree to which iGen feel they are obligated to protect and ensure the security of their information or the degree to which iGen believe that this is expected of them.

Individuals with strong normative commitment will feel obligated to protect their privacy, and, for the iGen who complete most of their tasks online, they should perceive a greater obligation to protect their personal information. Therefore, if iGen feels a normative commitment (i.e., an obligation) to protect their personal information, then they may be more likely to privatize their personal information, leading to continuance commitment as they perceive the great cost of a potential loss of personal information. In

other words, iGen with strong normative commitment have strong continuance commitment, which leads to the following hypothesis:

H6: iGen's normative commitment to information security increases iGen's continuance commitment to information security.

CHAPTER IV

RESEARCH METHOD

4.1 Scale Development

The constructs of this study were measured by multi-item scales that have been validated in prior literature and were modified to suit the context of social media as the focus of this study. The multi-item measurement was subjected to various validation procedures including but not limited to content validity, construct validity, and reliability (Straub, 1989).

Prior to the actual data collection, content validity of the survey questions was developed through a pre-test with three faculty members who specialize in information security and five information system major Ph.D. students. Feedback from participants of the pretest showed an overall 87% agreement of initial construct validity, which demonstrated that the survey questions are meaningful and valid (Lu and Ramamurthy, 2011). The ambiguous indicators were identified and modified based on the agreement of pretest participants. Certain relevant variables (e.g., demographic variable and response cost) that may potentially influence users' intention of online information sharing were controlled to avoid any potential bias.

The refined scale items were further pilot tested with 55 college students aged 18–25 to ensure clarity and structure of the questionnaire. Additionally, interviews were

conducted to assess the reasonability and comprehensiveness of survey questions, and feedback was collected for further improvement of the scale.

After careful revisions and editing based on results and feedback from the pretest and pilot test, we finalized the survey questionnaires based on the agreements and approval of two professors of information systems.

4.2 Data Collection

The final survey was developed and launched through Qualtrics, and 431 survey invitations were distributed by email among college students across 20 days in May 2019. A total of 392 responses were initially received. After careful screening and removing incomplete responses, 362 valid survey responses were used for further data analysis, forming a response rate of 84%. A test for nonresponse bias showed no significant differences between responding and nonresponding students.

All responses are from participants whose are aged between 18 and 25, which indicates the respondents are all iGen. The percentage of male respondents is 43%, and the percentage of female respondents is 57%. The majority of survey participants are college students, which accounts for 94% of the total participants, and the remaining participants are graduate students. Only 21% of the survey respondents are IT-related majors, studying subjects such as computer science, IT, and information systems. A total of 79% of survey respondents reported themselves to be non-IT-related majors. Only 14% of the survey participants have participated in information security-related courses or training. The remaining 86% of survey participants have not received any information security training. Table 1 shows the demographic characterization of the final sample.

Table 1. Respondent Profile

Demographic features	Frequency (N=392)	Percentages
Gender		
Male	169	43.1
Female	223	56.9
Age		
Under 18	0	0
18-25	392	100
26-39	0	0
40-49	0	0
50-59	0	0
Above 60	0	0
Level of education		
Middle School	0	0
High School	0	0
College	369	94.1
Graduate School	23	5.9
IT Major		
Yes	82	20.9
No	310	79.1
Participation in Courses or Training of Information Security		
Yes	56	14.3
No	336	85.7

4.3 Operationalization of the Constructs

The constructs used to explore and answer the research questions in this study were adapted from previously validated studies. The measurements of the constructs were also adapted from validated studies. The measurements were multi-item scales using a 7-point Likert scale with anchors ranging from 1 (strongly disagree) to 7 (strongly agree) except demographic variables (e.g. age, gender, and education).

Firstly, we used three items from Venkatesh et al. (2012) to measure iGen's intention to share information on social media. For example, respondents were asked how much they agreed or disagreed with statements such as: "I intend to share my information on Social Media in the future," "I plan to share my information on Social Media frequently," and "I will always try to share my information on Social Media in my daily life." This measure revealed a high level of reliability ($\alpha = 0.89$).

Secondly, the construct of trust was measured using three items from Bansal et al. (2010), such as: "I believe that Social Media I often use is honest," "I believe that Social Media I often use cares about their customers all the time," and "I believe that Social Media I often use is dependable, not opportunistic." The scale demonstrated an acceptable level of reliability ($\alpha = 0.75$).

Thirdly, we used three items adopted from Lee et al (2013), Gabisch and Milne (2014), and Prince (2018) to measure the construct of compensation, which were offered by social media platforms or mobile apps. Participants were asked to what degree they agree or disagree with the following statements: "Immediately receiving monetary rewards will make me share personal information on Social Media," "Receiving customized e-services such as customized web/app contents or customized advertisings will make me share personal information on Social Media," and "Getting rid of unwanted advertisings will make me share personal information on Social Media." The scale also had an acceptable level of reliability ($\alpha = 0.79$).

Fourthly, the construct of iGen's Perceived Privacy Control on social media platforms was measured using three items adopted from Krasnova et al (2010). These

items included: “I feel in control over who can view my information on Social Media platforms,” “I feel in control over how Social Media Companies use my information,” and “I feel in control over the access to my information that is collected by Social Media Companies.” The reliability of this scale was acceptable ($\alpha = 0.75$).

Finally, three constructs served to define iGen’s commitment to their privacy and information security: Continuance Commitment, Normative commitment and affective commitment.

First, we adapted three items from Allen and Meyer (1990) and Kaur and Sharma (2015) to measuring Continuance Commitment, including: “I am afraid of what might happen if I share my personal info on Social Media,” “Protecting my personal information on Social Media is a matter of necessity as much as desire,” and “One of the few serious consequences of sharing personal information on Social Media would be privacy invasion.” The reliability of this scale was acceptable ($\alpha = 0.74$).

Next, normative commitment was also adopted from Allen and Meyer (1990) and Kaur and Sharma (2015) and measured by three items, which included: “A person needs to always protect their personal information on Social Media,” “I feel protecting my personal information on Social Media as a sense of moral obligation to remain,” and “I was taught to believe in the value of protecting my personal information on Social Media.” This scale was also reliable ($\alpha = 0.75$).

At last, three items were adopted from Allen and Meyer (1990) and Kaur and Sharma (2015) to measure affective commitment. For instance, participants were asked to specify the degree to which they agreed or disagreed with following statements: “I do not

feel comfortable when I disclose my personal information to Social Media Companies," "My personal information has a great deal of personal meaning for me," and "It concerns me to discuss my personal information on Social Media." The reliability of this scale was also acceptable ($\alpha = 0.74$).

CHAPTER V

RESULTS

This study consists of two approaches to test the model: the measurement model and the structural model. Partial least squares (PLS) structural equation modeling (SEM) was selected to implement this the measurement model and the structural model. It is recommended to use PLS-SEM when the goal is to identify key determining constructs, when testing is in the early stage of theoretical development, or when the structural model is complex (Hair et al., 2011). PLS-SEM utilizes a principle component/composite-based, or variance-based estimation method.

Unlike covariance-based SEM, which fits a common factor model to the data, PLS-SEM maximizes the amount of explained variance to fit a composite model (Henseler et al, 2015). The software used for applying this method was PLS Smart 3.0. Nunnally (1978) suggests that SEM estimation should have at least 10 times as many respondents as measurement items. In our tested model, 31 measurement items were present, implying that a minimum sample size of 310 was needed. Therefore, our sample size of 362 was adequate for modeling.

5.1 Measurement Model

The measurement model estimates the relationships between the measurement items and the latent constructs they represent (Dhillon et al., 2020). To estimates this relationship, constructs reliability, including individual item reliability and internal

consistency, and construct validity, including convergent and discriminant validities of the measurement model are calculated and assessed. Table 2 illustrates the mean, variance, and loadings for individual measurement items, Cronbach's alpha, and the composite reliability for each construct.

For individual item reliability, each item must load significantly with their respective construct statistically (Hair et al., 1998), with the factor loadings being greater than 0.7. In our measurement model, all item loadings are significant ($p < 0.05$, two-tailed) and above 0.7, with the exception of four items, which were eliminated. The eliminated items include one item measuring trust, one item measuring normative commitment, one item measuring continuance commitment, and one item measuring affective commitment.

In order to evaluate internal consistency, we verify whether the Cronbach's alpha (CA) of all constructs is above 0.7. As shown in table 2, all Cronbach's alphas range between 0.736 and 0.885, indicating an acceptable level of internal consistency for the measurement items of this study.

In addition to Cronbach's alpha, the composite reliability of a construct should be at least 0.7 to demonstrate adequate reliability (Fornell and Larcker, 1981). As shown in Table 2, the composite reliability for each construct ranges from 0.744 to 0.921, thus demonstrating adequate composite reliability for the purpose of this study.

Table 2. Measurement Model Quality Criteria

Latent Variable	Mean	Variance	Loadings
Intention to Information Sharing (α=0.885, CR=0.921)			
ISHI1	4.71	1.47	0.875
ISHI2	4.80	1.56	0.884
ISHI3	5.18	1.53	0.805
Compensation (α=0.786; CR=0.8791)			
Compen1	3.67	1.73	0.815
Compen2	3.38	1.54	0.865
Compen3	3.51	1.62	0.829
Trust (α=0.751; CR=0.756)			
Trust1	3.17	1.41	0.812
Trust2	3.07	1.56	0.866
Trust3	3.60	1.53	0.770
Perceived Privacy Control (α=0.754; CR=0.776)			
PPC1	3.42	1.61	0.796
PPC2	3.26	1.52	0.796
PPC3	3.38	1.31	0.857
Continuance Commitment (α=0.737; CR=0.744)			
CCom1	5.50	1.37	0.817
CCom2	5.20	1.27	0.835
CCom3	5.44	1.29	0.774
Normative commitment (α=0.748; CR=0.747)			
NCom1	5.91	1.21	0.819
NCom2	5.52	1.27	0.855
NCom3	5.29	1.30	0.771
Affective Commitment (α=0.736; CR=0.794)			
ACom1	5.06	1.37	0.716
ACom2	5.54	1.27	0.886
ACom3	5.28	1.35	0.848
Notes: α = Cronbach's alpha, CR = composite reliability			

In addition to Cronbach's alpha, the composite reliability of a construct should be at least 0.7 to demonstrate adequate reliability (Fornell and Larcker, 1981). As shown in Table 2, the composite reliability for each construct ranges from 0.744 to 0.921, thus demonstrating adequate composite reliability for the purpose of this study.

Table 3. Convergent and Discriminant Validities

	Constructs	**AVE**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	Info Share Intention	0.744	0.773						
2	Compensation	0.700	0.537	0.837					
3	Trust	0.667	0.496	0.376	0.746				
4	Perceived Privacy Control	0.667	0.630	0.432	0.523	0.817			
5	Continuous Commitment	0.655	-0.447	-0.301	-0.313	-0.299	0.809		
6	Normative Commitment	0.665	-0.417	-0.262	-0.169	-0.232	0.629	0.815	
7	Affective Commitment	0.653	-0.407	-0.242	-0.319	-0.305	0.620	0.591	0.808

Convergent validity is the degree to which items measuring the same construct are related to each other. The assessment measure and threshold of convergent validity are average variance extracted (AVE) of the construct and should be above 0.5, indicating that a latent variable can explain more than half of the variance of its indicators on

average (Fornell and Larcker, 1981). The AVEs of our measurement model shown in Table 3 range from 0.653 to 0.744, which provides evidence of adequate convergent validity.

Discriminant validity is the degree to which the items for a respective construct do not reflect other constructs; discriminant validity is thus demonstrated by low correlations between the measure items of interest and the measure items of other constructs (Fornell and Larcker, 1981). To assess discriminant validity, it is necessary to verify that the squared root of the AVE for each construct is higher than the correlations between this construct and all other constructs. In our measurement model, the square roots of the AVEs for all constructs are reported in the diagonal of the correlation matrix in Table 3. They are all larger than the corresponding off-diagonal correlations, which demonstrates adequate discriminant validity.

Although Fornell-Larcker is the most common method used for testing discriminant validity, concerns around its effectiveness have been expressed (Henseler et al., 2015). The reason for this is that the Fornell-Larcker criteria may suffer from uncertainty in an examination of the discriminant validity for variance-based (VB)-SEM or PLS-SEM (Yusoff et al., 2019), which is used in this study.

To address these concerns, there is an alternative approach named heterotrait-monotrait (HTMT), which uses a ratio of correlations to assess discriminant validity. Prior studies have shown that the HTMT criterion is able to achieve higher specificity

Table 4. Heterotrait-Monotrait (HTMT) Ratio

	Constructs	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	Info Share Intention							
2	Compensation	0.641						
3	Trust	0.595	0.485					
4	Perceived Privacy Control	0.789	0.565	0.675				
5	Continuous Commitment	0.551	0.407	0.415	0.411			
6	Normative Commitment	0.512	0.344	0.228	0.315	0.834		
7	Affective Commitment	0.517	0.398	0.448	0.447	0.812	0.777	

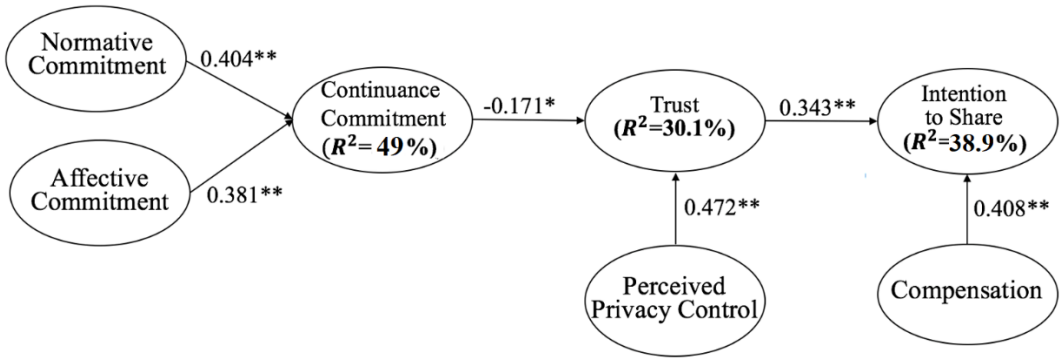
and sensitivity rates (97% to 99%) to detect a lack of discriminant validity than the Fornell-Larcker (20.82%) criterion, including the cross-loadings (0.00%; Henseler et al., 2015). Therefore, HTMT achieves a superior performance when assessing discriminant validity (Ab Hamid et al., 2017) in VB-SEM. This is important as failure to demonstrate discriminant validity can cause biased estimates in the discriminating criteria of the structural parameters that disprove the hypothesized relationship between constructs (Henseler et al., 2015). This study thus also tested the HTMT to assess discriminant validity. The method used is based on the matrix multitrait-multimethod (Yusoff et al., 2019). Using HTMT to assess discriminant validity requires the value of HTMT to be lower than the predefined threshold of 0.85 (Kline, 2011); it otherwise indicates the existence of a discriminant validity problem or the multicollinearity among the

constructs. Table 4 illustrates that the results of HTMT are all lower than the threshold of 0.85, which demonstrates discriminant validity.

As the above results indicate, the measurement model satisfies all the requirements for internal consistency, convergent validity, and discriminant validity to demonstrate construct reliability and construct validity.

5.2 Structural Model

Figure 2. Research Model with Results



To test the research model, bootstrapping with 5000 resamples was used to estimate the path coefficients and significance levels, based on t-statistic values. The results are presented in Table 3 and figure 2. Based on our model inputs, 38.9% of the variation in iGen's intention to share information is explained by the research model. The hypotheses for trust (0.343; $p < 0.01$) and compensation (0.408; $p < 0.01$) are also both statistically significant for impacting iGen's intention to share information online. Therefore, hypotheses H1 and H2 are supported. Furthermore, the research model

explains 30.1% of the variation in trust. The hypotheses of perceived privacy control (0.472; $p < 0.01$) and continuance commitment (-0.171; $p < 0.05$) are both statistically significant with respect to trust. Hypotheses H3 and H4 are thus supported. Lastly, the research model explains 49.0% of the variation in continuance commitment. The hypotheses of normative commitment (0.404; $p < 0.01$) and affective commitment (0.381; $p < 0.01$) are statistically significant in relation to continuance commitment. Hypotheses H5 and H6 are therefore supported.

5.3 iGen's Commitment to their Privacy and Information Sharing

iGen's commitment to their privacy and information sharing are measured by their continuance commitment, normative commitment, and affective commitment based on the theory of commitment, which has arguably been the predominant model for measurement of commitment constructs (Jaros, 2007).

As shown in Table 5, for the average continuance of all survey respondents, normative and formative commitments are 5.39, 5.58, and 5.3 respectively, which demonstrates that iGen has stronger continuance commitments than normative and affective commitments to their privacy and information security. Moreover, these results indicate that iGen's normative commitment is slightly stronger than their affective commitment. The value 4 is the threshold to determine if iGens are committed to their privacy and information security because in the survey questionnaires, the value 4 represents "neither agree nor disagree." The value 4 thus signifies a neutral attitude, and values larger than 4 denote that iGen is committed at those levels, whereas values smaller than 4 indicate that iGen is not committed at those levels.

Based on our results, female respondents were slightly more committed to their privacy and information security than male respondents (values of 5.44 vs 5.40). The values of female iGens' continuance, normative and formative commitments (5.43, 5.60, and 5.32) were all higher than the values of male iGens' continuance, normative and formative commitments (5.36, 5.57, and 5.28), respectively.

Significantly, iGens in college were more committed to their privacy and information security than iGens in graduate school (5.47 vs 5.22). The values of the three commitments (5.43, 5.67, and 5.32) of college respondents were also all larger than the values of the three commitments (5.20, 5.19, and 5.26) of respondents in graduate school, respectively.

Table 5. iGen's Commitment to Information Sharing

	Continuance Commitment	Normative Commitment	Affective Commitment	Overall Commitment
Gender				
Female	5.43	5.60	5.32	5.44
Male	5.36	5.57	5.28	5.40
Level of Education				
College	5.43	5.67	5.32	5.47
Graduate School	5.20	5.19	5.26	5.22
IT Major				
Yes	5.38	5.59	5.28	5.41
No	5.40	5.58	5.31	5.43
Participation in Courses or Training of Information Security				
Yes	5.44	5.62	5.32	5.46
No	5.37	5.56	5.30	5.41
Total	5.39	5.58	5.30	5.42

iGens who were not IT majors were more committed to their privacy and information security than iGens who were IT majors (5.41 vs 5.43). However, only the values of continuance and affective commitments (5.40 and 5.31) of non-IT-major respondents were higher than those (5.38 and 5.28) of IT major respondents, respectively. The normative commitment (5.58) of non-IT-major respondents was slightly lower than that (5.59) of IT major respondents.

iGens who had participated in courses or training of information security were more committed to their privacy and information security than iGens who had not participated in security training (5.46 vs 5.41). All values of continuance, normative and formative commitments (5.44, 5.62, and 5.32) of respondents with information security training were higher than the three commitments (5.37, 5.56, and 5.30) of respondents without information security training, respectively.

5.3.1 Male vs Female Respondents

In particular, the continuance commitment of female respondents is 5.43. Firstly, 67% of female respondents were afraid of what might happen if they shared their personal info on social media, whereas 11% of them were not afraid. Secondly, 65% of female respondents agreed that protecting personal information on social media is a matter of necessity as much as desire, whereas 15% disagreed. Thirdly, 71% of female respondents perceived that one of the few serious consequences of sharing personal information on social media would be privacy invasion, whereas 12% did not perceive this.

The normative commitment of female respondents is 5.60. Firstly, 68% of female respondents believed that they needed to always protect their information on Social Media, whereas 12% did not. Secondly, 66% of female respondents felt protecting personal information on Social Media as a sense of moral obligation to maintain, whereas 10% did not feel this. Thirdly, 73% of female respondents were taught to believe in the value of protecting personal information on Social Media, whereas 9% were not taught this.

The affective commitment of female respondents is 5.32. Firstly, 59% of female respondents did not feel comfortable when they disclosed their information to social media companies, whereas 9% feel comfortable. Secondly, 68% of female respondents agreed that their personal information had a great deal of personal meaning for them, whereas 6% did not. Thirdly, 62% of female respondents believed that discussion of personal information on Social Media concerned them, whereas 11% did not believe this.

The continuance commitment of male respondents is 5.36. Firstly, 65% of male respondents were afraid of what might happen if they share their information on social media, whereas 14% were not afraid. Secondly, 62% of male respondents agreed that protecting personal information on Social Media is a matter of necessity as much as desire, whereas 17% disagreed. Thirdly, 69% of male respondents perceived that one of the few serious consequences of sharing personal information on Social Media would be privacy invasion, whereas 14% did not perceive this.

The normative commitment of male respondents is 5.57. Firstly, 67% of male respondents believed that they needed to always protect their personal information on

Social Media, whereas 12% did not believe this. Secondly, 64% of male respondents felt protecting personal information on social media as a sense of moral obligation to maintain, whereas 9% did not feel that. Thirdly, 68% of male respondents were taught to believe in the value of protecting personal information on social media, whereas 8% were not taught this.

The affective commitment of male respondents is 5.28. Firstly, 56% of male respondents did not feel comfortable when they disclosed personal information to Social media companies, whereas 9% felt comfortable. Secondly, 63% of male respondents agreed that their personal information had a great deal of personal meaning for them, whereas 5% did not agree with this. Thirdly, 59% of male respondents believed that discussion of personal information on Social Media concerned them, whereas 10% did not believe this.

5.3.2 College Students vs Graduate Students

The continuance commitment of college student respondents is 5.43. Firstly, 68% of college student respondents were afraid of what might happen if they shared their personal info on social media, whereas 13% of them were not afraid. Secondly, 63% of college student respondents agreed that protecting personal information on social media was a matter of necessity as much as desire, whereas 15% disagreed. Thirdly, 69% of college student respondents perceived that one of the few serious consequences of sharing personal information on social media would be privacy invasion, whereas 11% did not perceive this.

The normative commitment of college student respondents is 5.67. Firstly, 68% of college student respondents believed that they needed to always protect their personal information on social media, whereas 11% did not. Secondly, 66% of college student respondents felt protecting personal information on social media as a sense of moral obligation to maintain, whereas 9% did not feel this. Thirdly, 68% of college student respondents were taught to believe in the value of protecting personal information on social media, whereas 6% were not taught this.

The affective commitment of college student respondents is 5.32. Firstly, 59% of college student respondents did not feel comfortable when they disclosed personal information to social media, whereas 9% felt comfortable. Secondly, 68% of college respondents agreed that their personal information had a great deal of personal meaning for them, whereas 6% did not. Thirdly, 62% of college respondents believed that discussion of personal information on social media concerned them, whereas 11% did not believe this.

The continuance commitment of graduate student respondents is 5.20. Firstly, 60% of graduate student respondents were afraid of what might happen if they shared personal info on Social Media, whereas 17% were not afraid. Secondly, 59% of graduate student respondents agreed that protecting personal information on social media is a matter of necessity as much as desire, whereas 18% disagreed. Thirdly, 67% of graduate student respondents perceived that one of the few serious consequences of sharing personal information on social media would be privacy invasion, whereas 10% did not perceive this.

The normative commitment of graduate student respondents is 5.57. Firstly, 67% of graduate student respondents believed that people needed to always protect their personal information on Social Media, whereas 12% did not. Secondly, 64% of graduate student respondents felt protecting personal information on social media as a sense of moral obligation to maintain, whereas 9% did not feel this. Thirdly, 68% of graduate student respondents were taught to believe in the value of protecting personal information on Social Media, whereas 8% were not taught this.

The affective commitment of graduate student respondents is 5.26. Firstly, 55% of graduate respondents did not feel comfortable when they disclosed personal information to social media companies, whereas 9% felt comfortable. Secondly, 62% of graduate student respondents agreed that their personal information had a great deal of personal meaning for them, whereas 6% disagreed. Thirdly, 59% of graduate respondents believed that discussion of personal information on social media concerned them, whereas 12% did not believe this.

5.3.3 IT Majors vs Non-IT Majors

Non-IT respondents have slightly stronger continuance commitment (5.4) than IT respondents (5.38). Firstly, 66% of IT vs 68% of non-IT respondents were afraid of what might happen if they share personal info on social media, whereas 15% of IT vs 13% of non-IT respondents were not afraid. Secondly, 62% of IT vs 63% of non-IT respondents agreed that protecting personal information on social media was a matter of necessity as much as desire, whereas 13% of IT vs 11% of non-IT respondents disagreed. Thirdly, 68% of IT vs 69% of non-IT respondents perceived that one of the few serious

consequences of sharing personal information on social media would be privacy invasion, whereas 9% of IT vs 7% of non-IT respondents did not perceive this.

However, IT respondents have slightly stronger normative commitment (5.59) than non-IT respondents (5.58). Firstly, 68% of IT vs 67% non-IT respondents believed that people needed to always protect their personal information on Social Media, whereas 11% of IT vs 11% non-IT respondents did not believe this. Secondly, 65% of IT vs 65% non-IT respondents felt protecting personal information on Social Media as a sense of moral obligation to maintain, whereas 9% of IT vs 8% non-IT respondents did not feel this. Thirdly, 69% of IT vs 67% non-IT respondents were taught to believe in the value of protecting personal information on Social Media, whereas 7% of IT vs 10% non-IT respondents were not taught this.

Non-IT respondents have slightly stronger affective commitment (5.31) than IT respondents (5.28). Firstly, 56% of IT vs 58% non-IT respondents did not feel comfortable when they disclosed personal information to Social Media Companies, whereas 10% of IT vs 11% non-IT respondents felt comfortable. Secondly, 65% of IT vs 68% non-IT respondents agreed that their personal information had a great deal of personal meaning for them, whereas 9% of IT vs 8% non-IT respondents disagreed. Thirdly, 61% of IT vs 59% non-IT respondents believed that discussion of personal information on Social Media concerned them, whereas 7% of IT vs 10% non-IT respondents did not believe this.

5.3.4 Participation in Courses or Training of Information Security

Respondents with security training have stronger continuance commitment (5.44) than respondents without security training (5.37). Firstly, 71% of respondents with training vs 65% of respondents without training were afraid of what might happen if they share personal info on social media, whereas 9% of respondents with training vs 12% of respondents without training were not afraid of this. Secondly, 70% of respondents with training vs 65% of respondents without training agreed that protecting personal information on social media is a matter of necessity as much as desire, whereas 9% of respondents with training vs 13% of respondents without training disagree with this. Thirdly, 79% of respondents with training vs 67% of respondents without training perceived that one of the few serious consequences of sharing personal information on Social Media would be privacy invasion, whereas 5% of respondents with training vs 8% of respondents without training did not perceive this.

However, Respondents with security training have slightly stronger normative commitment (5.59) than respondents without security training (5.58). Firstly, 73% of respondents with training vs 68% of respondents without training believed that people needed to always protect their personal information on social media, whereas 6% of respondents with training vs 11% of respondents without training did not. Secondly, 74% of respondents with training vs 68% of respondents without training felt protecting personal information on social media as a sense of moral obligation to maintain, whereas 7% of respondents with training vs 9% of respondents without training did not feel this. Thirdly, 73% of respondents with training vs 69% of respondents without training were taught to believe in the value of protecting personal information on Social Media,

whereas 6% of respondents with training vs 8% of respondents without training were not taught this.

Respondents with security training have slightly stronger affective commitment (5.32) than respondents without security training (5.30). Firstly, 67% of respondents with training vs 63% of respondents without training did not feel comfortable when they disclosed personal information to social media, whereas 10% of respondents with training vs 14% of respondents without training felt comfortable. Secondly, 65% of respondents with training vs 62% of respondents without training agreed that their personal information has a great deal of personal meaning for them, whereas 10% of respondents with training vs 11% of respondents without training did not. Thirdly, 66% of respondents with training vs 62% of respondents without training believed that discussion of personal information on social media concerned them, whereas 7% of respondents with training vs 9% of respondents without training were not concerned.

5.4 iGen's Intention to Share Information on Social Media

The results showed that iGen intended to share their hobbies and interests, demographic information, and email addresses on social media. Among all types of information that they would like to share, more iGen intended to share their hobbies and interests on social media. The results also illustrated that iGen had a neutral attitude about sharing their family information. However, they generally declined to share their purchase, health information, financial information, and identity information. Notably, among all types of information that they declined to share, number of iGens who declined to share their purchase history on social media was the most.

Table 6. iGen's Intention to Share Information on Social Media

	Gender		Education		IT Major		Training of Information Security		Overall
	F	M	College	Graduate School	Yes	No	Yes	No	
Hobbies and Interests	5.0	5.3	5.3	5.5	5.4	5.5	5.3	5.4	5.4
Demography	4.9	5.1	4.9	4.7	5	4.6	4.3	5.1	4.9
Email	4.8	4.9	4.7	4.2	4.8	4.4	4.4	5.0	4.7
Family	3.9	4.2	4.2	4.0	3.7	4.1	3.9	4.1	4.0
Purchase History	3.1	3.6	3.0	3.6	3.4	3.3	2.9	3.5	3.3
Health	3.4	3.7	3.4	3.5	3.3	3.5	3.2	3.8	3.4
Finance	2.9	3.2	3.0	3.0	3.6	3.2	3.2	3.5	3.4
Identity	3.6	4.0	3.9	3.0	3.5	3.9	3.5	4.0	3.8

Hobbies and Interests

At first, the results indicated that more male respondents than female respondents intended to share their hobbies and interests on social media. A total of 75% of male respondents vs 70% of female respondents intended to accurately share their hobbies and interests at various levels. In contrast, 12% of female respondents vs 12% of male respondents declined to accurately share their hobbies and interests on social media at various levels.

Then, the results showed that more graduate respondents than college respondents intended to share their hobbies and interests on social media. 65% of college respondents vs 72% of graduate respondents intended to accurately share their hobbies and interests at

various levels. Whereas, 15% of college respondents vs 19% of graduate respondents declined to accurately share their hobbies and interests on Social Media at various levels.

Next, the results showed that more non-IT major respondents than IT major respondents intended to share their hobbies and interests on social media. 66% of IT major respondents vs 71% of non-IT major respondents intended to accurately share their hobbies and interests at various levels. Whereas, 17% of IT respondents vs 16% of non-IT respondents declined to accurately share their hobbies and interests on Social Media at various levels.

At last, the results showed that more respondents without security training than respondents with security training intended to share their hobbies and interests on social media. 60% of respondents with IT security training vs 79% of respondents without IT security training intend to accurately share their hobbies and interests at various levels. Whereas, 26% of respondents with IT security training vs 15% of respondents without IT security training declined to accurately share their hobbies and interests on Social Media at various levels.

Demography

At first, the results showed that more male respondents than female respondents intended to share their demographic information on social media. 51% of male respondents vs 48% of female respondents intended to accurately share their demographic information at various levels. In contrast, 21% of male respondents vs 25% female respondents declined to accurately share their demographic information on Social Media at various levels.

Then, the results showed that more college respondents than graduate respondents intended to share their demographic information on social media. 50% of college respondents vs 47% of graduate respondents intended to accurately share their demographic information at various levels. Whereas, 26% of college respondents vs 29% of graduate respondents declined to accurately share their demographic information on Social Media at various levels.

Next, the results showed that more IT major respondents than non-IT major respondents intended to share their demographic information on social media. 51% of IT major respondents vs 45% of non-IT major respondents intended to accurately share their demographic information at various levels. In contrast, 21% of IT respondents vs 25% of non-IT respondents declined to accurately share their demographic information on Social Media at various levels.

At last, the results showed that more respondents without security training than respondents with security training intended to share their demographic information on social media. 39% of respondents with IT security training vs 60% of respondents without IT security training intended to accurately share their demographic information at various levels. Whereas, 29% of respondents with IT security training vs 19% of respondents without IT security training declined to accurately share their demographic information on Social Media at various levels.

Email Address

At first, the results showed that more male respondents than female respondents intended to share their email addresses on social media. 49% of male respondents vs

45% of female respondents intended to accurately share their email addresses at various levels. In contrast, 29% of male respondents vs 40% female respondents declined to accurately share their email addresses on Social Media at various levels.

Then, the results showed that more college respondents than graduate respondents intended to share their email addresses on social media. 52% of college respondents vs 47% of graduate respondents intended to accurately share their email addresses at various levels. In contrast, 30% of college respondents vs 38% of graduate respondents declined to accurately share their email addresses on Social Media at various levels.

Next, the results showed that more IT major respondents than non-IT major respondents intended to share their email addresses on social media. 55% of IT major respondents vs 46% of non-IT major respondents intended to accurately share their email addresses at various levels. In contrast, 22% of IT respondents vs 26% of non-IT respondents declined to accurately share their email addresses on Social Media at various levels.

At last, the results showed that more respondents without security training than respondents with security training intended to share their email addresses on social media. 45% of respondents with IT security training vs 52% of respondents without IT security training intended to accurately share their email addresses at various levels. In contrast, 27% of respondents with IT security training vs 18% of respondents without IT security training declined to accurately share their email addresses on Social Media at various levels.

Family Information

At first, the results showed that more male respondents than female respondents intended to share their family information on social media. 35% of female respondents vs 39% of male respondents intended to accurately share their family information at various levels. In contrast, 30% of male respondents vs 43% female respondents declined to accurately share their family information on Social Media at various levels.

Then, the results showed that more graduate respondents than college respondents intended to share their family information on social media. 35% of college respondents vs 37% of graduate respondents intended to accurately share their family information at various levels. In contrast, 36% of college respondents vs 35% of graduate respondents declined to accurately share their family information on Social Media at various levels.

Next, the results showed that more non-IT major respondents than IT major respondents intended to share their family information on social media. 34% of IT major respondents vs 41% of non-IT major respondents intended to accurately share their family information at various levels. In contrast, 37% of IT respondents vs 34% of non-IT respondents declined to accurately share their family information on Social Media at various levels.

At last, the results showed that more respondents without security training than respondents with security training intended to share their family information on social media. 30% of respondents with IT security training vs 36% of respondents without IT security training intended to accurately share their family information at various levels. In contrast, 40% of respondents with IT security training vs 29% of respondents without IT

security training declined to accurately share their family information on Social Media at various levels.

Purchase History

At first, the results showed that more male respondents than female respondents intended to share their purchase history on social media. 18% of female respondents vs 22% of male respondents intended to accurately share their purchase history at various levels. In contrast, 56% of male respondents vs 60% female respondents declined to accurately share their purchase history on Social Media at various levels.

Then, the results showed that more college respondents than graduate respondents intended to share their purchase history on social media. 23% of college respondents vs 20% of graduate respondents intended to accurately share their purchase history at various levels. In contrast, 56% of college respondents vs 65% of graduate respondents declined to accurately share their purchase history on Social Media at various levels.

Next, the results showed that more IT major respondents than non-IT major respondents intended to share their purchase history on social media. 27% of IT major respondents vs 23% of non-IT major respondents intended to accurately share their purchase history at various levels. In contrast, 55% of IT respondents vs 54% of non-IT respondents declined to accurately share their purchase history on Social Media at various levels.

At last, the results showed that more respondents without security training than respondents with security training intended to share their purchase history on social media. 20% of respondents with IT security training vs 29% of respondents without IT

security training intended to accurately share their purchase history at various levels. In contrast, 60% of respondents with IT security training vs 54% of respondents without IT security training declined to accurately share their purchase history on Social Media at various levels.

Health Information

At first, the results showed that more male respondents than female respondents intended to share their health information on social media. 23% of female respondents vs 27% of male respondents intended to accurately share their health information at various levels. In contrast, 54% of male respondents vs 55% female respondents declined to accurately share their health information on Social Media at various levels.

Then, the results showed that more college respondents than graduate respondents intended to share their health information on social media. 28% of college respondents vs 50% of graduate respondents intended to accurately share their health information at various levels. In contrast, 21% of college respondents vs 41% of graduate respondents declined to accurately share their health information on Social Media at various levels.

Next, the results showed that more non-IT major respondents than IT major respondents intended to share their health information on social media. 24% of IT major respondents vs 27% of non-IT major respondents intended to accurately share their health information at various levels. In contrast, 54% of IT respondents vs 51% of non-IT respondents declined to accurately share their health information on Social Media at various levels.

At last, the results showed that more respondents without security training than respondents with security training intended to share their health information on social media. 18% of respondents with IT security training vs 26% of respondents without IT security training intended to accurately share their health information at various levels. In contrast, 52% of respondents with IT security training vs 55% of respondents without IT security training declined to accurately share their health information on Social Media at various levels.

Financial Information

At first, the results showed that more male respondents than female respondents intended to share their financial information on social media. 18% of female respondents vs 24% of male respondents intended to accurately share their financial information at various levels. In contrast, 57% of male respondents vs 66% female respondents declined to accurately share their financial information on Social Media at various levels.

Then, the results showed that more graduate respondents than college respondents intended to share their financial information on social media. 20% of college respondents vs 11% of graduate respondents intended to accurately share their financial information at various levels. In contrast, 60% of college respondents vs 70% of graduate respondents declined to accurately share their financial information on Social Media at various levels.

Next, the results showed that more IT major respondents than non-IT major respondents intended to share their financial information on social media. 27% of IT major respondents vs 23% of non-IT major respondents intended to accurately share their financial information at various levels. Whereas, 55% of IT respondents vs 54% of non-

IT respondents declined to accurately share their financial information on Social Media at various levels.

At last, the results showed that more respondents without security training than respondents with security training intended to share their financial information on social media. 20% of respondents with IT security training vs 29% of respondents without IT security training intended to accurately share their financial information at various levels. In contrast, 60% of respondents with IT security training vs 54% of respondents without IT security training declined to accurately share their financial information on Social Media at various levels.

Identity Information

At first, the results showed that more male respondents than female respondents intended to share their identity information on social media. 33% of female respondents vs 36% of male respondents intended to accurately share their identity information at various levels. In contrast, 37% of male respondents vs 53% female respondents declined to accurately share their identity information on Social Media at various levels.

Then, the results showed that more college respondents than graduate respondents intended to share their identity information on social media. 33% of college respondents vs 15% of graduate respondents intended to accurately share their identity information at various levels. In contrast, 50% of college respondents vs 52% of graduate respondents declined to accurately share their identity information on Social Media at various levels.

Next, the results showed that more non-IT major respondents than IT major respondents intended to share their identity information on social media. 24% of IT

major respondents vs 27% of non-IT major respondents intended to accurately share their identity information at various levels. In contrast, 56% of IT respondents vs 50% of non-IT respondents declined to accurately share their identity information on Social Media at various levels.

At last, the results showed that more respondents without security training than respondents with security training intended to share their identity information on social media. 18% of respondents with IT security training vs 26% of respondents without IT security training intended to accurately share their identity information at various levels. In contrast, 52% of respondents with IT security training vs 55% of respondents without IT security training declined to accurately share their identity information on Social Media at various levels.

CHAPTER VI

DISCUSSION AND CONTRIBUTION

6.1. Overview

In this study, we investigated the iGen's intention to share information online in the context of their commitment to information security as well as the impact of trust, compensation, and perceived privacy control. We found that iGen's commitment to information security impacts their intention to share on social media and is mediated by their trust in social media. Moreover, iGen's continuance commitment to information sharing can be boosted by their affective and normative commitment. In addition, compensation and perceived privacy control can positively affect iGen's intention to share and their trust in social media, respectively. In this section, we discuss how these findings theoretically contribute to information security literature.

6.2 iGen's Intention to Share, Commitment to Information Security, and Trust

This is the first study of information security that is unique to the group of iGen and extends generational cohort theory into the field of online sharing intention. The results of this research provide strong theoretical implications regarding the iGen's intention to share personal information on social media. The relationship between trust and intention to share online is well established. However, we have now illustrated that trust not only strengthens the older generation's intention to share information online, as

shown in prior literature, but likewise increases the younger generation's intention to share. This finding is important in the domain of information security as researchers can now explore additional antecedents for motivating trust that are unique to the iGen and provide implication for trust theory at large.

Additionally, our study finds continuance commitment to information security to be a key factor that vitiates iGen's trust in social media. This not only provides trust theory with a new intrinsic antecedent but is also the first time a study on continuance commitment in the field of information security has been conducted in this context. The major extant literature has concentrated on what online vendors should build and develop to boost customers' trust. However, there is limited research on the intrinsic factors that could influence the extent of trust in social media from the Internet users' point of view (Bansal et al., 2016). Prior studies have demonstrated that trust can be impacted by website contexts (Bansal et al., 2016) and previous positive website experience (Pavlou and Gefen, 2005). Moreover, some prior studies have shown that factors such as privacy concerns (Bansal et al., 2010) and customer personalities (Bansal et al., 2016) can affect customers' trust. Therefore, continuance commitment is a new and important factor that has been shown to have a direct impact on iGen's trust in social media.

The major contribution of this study is thus that it is the first study to apply the theory of commitment in the domain of information security among iGen. In addition, it expands the research to a broader domain, specifically the intention to share information on social media. The results reveal that trust plays a mediating role between iGen's intention to share on social media and their commitment to information security. In other

words, it shows the indirect impact of iGen's continuance commitment on their intention to share personal information on social media, as mediated by trust. Therefore, to prevent iGen's oversharing online, enhancement of their continuance commitment to information security can be an effective mechanism.

6.3 iGen's Continuance Commitment, Affective Commitment, and Normative Commitment

The three-component model of commitment has arguably been the most adopted model for the research of commitment (Shoemaker, 2019). However, to the best of our knowledge, this is the first study that explores the relations between the three commitments in the field of information security and the intention to share online. The impacts of the three commitments are not always unified (see, e.g., Chen et al., 2015), but the results of our study illustrate that iGen's affective and normative commitments are positively related to iGen's continuance commitment to information security. The findings of this study indicate that iGens with strong affective commitment, namely an emotional willingness to ensure information security, and strong normative commitment, namely a perceived obligation to ensure information security, have strong continuance commitment, which makes them feel a need to protect personal information. In other words, continuance commitment as a behavioral intention is motivated by iGen's inherent perceptions and affective and normative commitments. This study therefore contributes to and complements the research of commitment and provides new insights into the literature of iGen's perspective on information security by identifying iGen's affective,

normative, and continuance commitments and their positive relations in the context of social media.

6.4 Compensation

Although a prior study elucidated that iGen does not work for money (Poague, 2018), our study found that iGen's intention to share information online was positively affected by monetary compensation. This is consistent with previous literature that states that iGen are motivated by financial incentives (Abramovich, 2018) and that compensation reduces a consumer's intention to protect their privacy (Gabisch and Milne, 2014). Specifically, the results of this study indicate that iGen perceive compensation in the formats of money, free e-service, and customized products, thus providing a different view of the iGen regarding incentives than older generations. Previous studies have shown that customers prior to the iGen are more concerned with privacy risks and thus more frequently decline to trade personal information when compensation is provided for incentivizing self-disclosure (Lee et al., 2013). The results of this study contribute to the literature on iGen by providing a broader understanding of the economic perspectives of iGen and their information disclosure in the social media context. From a theoretical viewpoint, this study contributes to the literature of privacy exchange by identifying compensation as an extrinsic factor for understanding the underlying process by which iGen compares the costs and benefits for information tradeoffs as applying a privacy calculus (Gabisch and Milne, 2014).

6.5 Perceived Privacy Control

In this study, we demonstrated that iGen's perceived privacy control is positively associated with their trust in social media. Although existing studies have shown similar results, this study tested the relation between perceived privacy control and trust in the context of iGen, which expands the research of trust on a broader scale. Moreover, these results extend the research with the findings of iGen's perceived privacy control on social media as this area of research is currently underdeveloped (e.g. see Coss and Dhillon, 2020; Dhillon et al. 2020). These results may imply that iGen, as a tech-savvy generation, are proficient in online technology and applications, and, as such, they are able to handle and expect more privacy controls.

6.6 Gender

The results of this research illustrate that female iGen's commitment to information security on average is stronger than male iGen's commitment, and females had a lower intention to share information on social media. These results are consistent with extant literature as follows.

Previous studies have demonstrated that women have different perceptions of risk from men (Gustafsod 1998) in a variety of domains, such as finance (Dwyer et al., 2002), eCommerce (Lin et al., 2019), and newly invented technology (Hajli and Lin, 2016). Extant studies have also shown that women and men differ in their use of social media due to different motivations and different weightings of the same motivations (Lin et al., 2013). Specifically, women are more goal-oriented and share less information about themselves when they use social media because they are more concerned about online

security than men (Horzum 2016). For example, female bloggers were more worried about privacy issues when they were creating blogs online (Chai et al., 2011). Literature demonstrated that women are more concerned about risks and are consistently more sensitive to potential information invasions, while men more enjoy running risks (Dwyer et al., 2002).

6.7 Level of Education

Our results demonstrate that iGens in college were more committed to their privacy and information security than iGen in graduate school. Therefore, a higher level of education does not guarantee a stronger commitment to online security. One explanation of this could be that a higher level of education could cause iGen's overconfidence in their information security. However, the sample size of graduate iGen in this study was too small to be representative. The impact of the level of education on commitment to online security can be proposed as the interest of research for further study.

Additionally, college iGen and graduate iGen have different intentions to share different types of information on social media.

6.8 IT Major and Security Training

Our results show that IT-major iGens and non-IT-major iGens had a very close values of commitment to their privacy and information security. It is therefore evident that adequate IT knowledge does not cause a strong commitment.

On the other hand, the results of this study revealed that iGen who have security training experience were more committed to their privacy and information security and

have less intention to share all types of information on social media. This result indicates that security training was effective for iGen just as it works well for other generations, though iGen may become overconfident in their cyber skill and be less concerned with cybersecurity.

6.9 Practical Contributions

The findings of this study contribute to practical insights. The results suggest a promotion of iGen's commitments to their information security to prevent their information oversharing online through the decrease of their trust on social media, because stronger commitment to information security can increase iGen's standards of trust in social media. With higher standards and more requirements, iGen will not easily trust social media, hence they will intend to share less online, thus preventing oversharing.

For social media platforms that collect users' data in order to provide better services and products, this study recommends that they offer compensation and more privacy control for iGen within the platform. When iGen perceives that they have privacy control, they increase their trust in social media and increase their intention to share information on social media.

CHAPTER VII

LIMITATION AND FURTHER RESEARCH

7.1 Limitations

As with all research, this study has some limitations. Firstly, we collected data from college students. More diverse groups of iGen, such as those who have entered industries, teenagers, freelancers, and social media content creators, can also be studied. Secondly, this study focused on the context of social media, but this is not the only place that iGen share their information. Literature had demonstrated that individuals have different information share intentions in different contexts. iGen's commitments to their privacy and information security may hence vary in different contexts. Thirdly, this study did not differentiate between sensitive information and non-sensitive information.

Literature has shown that individuals have different intentions to share personal information based on the sensitivity of the information. In the same way, iGen may commit differently to their sensitive information protection and non-sensitive information protection. Moreover, this study investigates iGen, but it does not explore other age groups. The comparison of iGen and other generations may show unique insights into iGen's commitment to information security and their intention to share information on social media. Finally, this study only investigated perceived privacy control as users' perception of their privacy control rather than real privacy control provided by social

media platforms. The perceived and real privacy control could differ due to iGen's tech efficacy.

7.2 Future Research

Since this study focuses on iGen, further research can extend our study to other generations for exploration of common ground and the differences of various generations' commitment to their information security and their intention of information sharing on social media.

Moreover, the role of commitment to information security in the field of information security could be investigated more widely. For example, the direct relationship between an individual's commitment to information security and their intention to share information on social media is a topic that would be interesting to examine further. Additionally, the antecedents of individuals' commitment could be a new research direction for the promotion of an individual's commitment to information security.

In addition, this study focuses on the context of social media, but, as asserted above, this is not the only place that iGen share their information. Differing contexts may affect iGen's commitment to information security and their intention to share online. Therefore, iGen's commitment could be investigated in other contexts, such as shopping, finance, and healthcare websites and apps.

Furthermore, the sensitivity of information may influence iGen's commitment to information security and their intention to share on the Internet. New research could study iGen's information sharing and their commitment based on highly sensitive

information, such as phone number, address, and income, and less sensitive information, such as gender, hobbies, and interest.

Additionally, the impact of culture and personality on the information sharing intentions and commitment of iGen and other generations would be a suitable topic for further research. Culture and personality have been shown to significantly affect individuals' online attitude and behaviors. iGen with different cultures and personalities may commit differently to their privacy and information security.

Finally, online tracking as a means of information sharing should be studied. Diverse online tracking methods based on various technologies and algorithms has become the most pervasive and predominant method by which to collect Internet users' information. It would thus be beneficial to study the role of iGen's commitment to privacy and information security in their acceptance of online tracking.

CHAPTER VIII

CONCLUSION

It is necessary to identify and understand characteristics of iGen, the largest generation that is changing the world now and will continue influencing and lead the world in the next decades (Wiedmer, 2015). It is a consensus that iGen has a very distinguished perspective of the digital world (Carboni-Brito 2011). iGen has never known a world without social media and prioritizes personalization over privacy (WP Engine, 2017). They have experienced very important technological innovations such as the development of the personal computer, appearance of the internet, pervasion of social media, and new careers such as social media influencers or social media content creators. This can cause them to hold different beliefs and appreciate different values, and they have already made noteworthy changes that cannot be ignored (Hoxha and Zeqiraj, 2019). The most technologically influenced generation, iGen, will significantly change the world in their unique ways (McCrindle and Wolfinger, 2010).

iGen's intention to share information online is critical to online information privacy and security. The findings of this study show that iGen's trust of social media and compensation offered by social media directly and positively affect iGen's intention to share information on social media. Additionally, iGen individuals with strong continuance commitment have less trust on social media, but their perceived privacy

controls on social media boost their trust on social media. Moreover, strong normative commitment and affective commitment of iGen promote their continuance commitment.

While the findings of this research serve to make the discussion and research of information security, individuals' commitment, and iGen's attitude more complete. It is also hoped that this study will both contribute to the growing literature and enable prevention of iGen's oversharing on social media.

REFERENCES

Ab Hamid, M. R., Sami, W., & Sidek, M. M. (2017). Discriminant validity assessment: Use of Fornell & Larcker criterion versus HTMT criterion. In Journal of Physics: Conference Series (Vol. 890, No. 1, p. 012163). IOP Publishing.

Abel, R. (2018). Baby boomers more cybersecurity savvy than Gen-Z, study. SC Media. Retrieved from https://www.scmagazine.com/home/security-news/network-security/baby-boomers-more-cybersecurity-savvy-than-gen-z-study/

Abramovich, G. (2019).15 Mind-Blowing Stats About Generation Z. Adobe Blog. Retrieved from https://blog.adobe.com/en/publish/2019/06/28/15-mind-blowing-stats-about-generation-z.html#gs.mwfy0i

Abramson, P., & Inglehart, R. (1995). Value Change in Global Perspective. Ann Arbor: University of Michigan Press.

Alam, M., & Bokhari, M. U. (2007, December). Information security policy architecture. In International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007) (Vol. 4, pp. 120-122). IEEE.

AlHogail, A. (2015). Design and validation of information security culture framework. Computers in Human Behavior, 49, 567-575.

Alkire, L., O'Connor, G. E., Myrden, S., & Köcher, S. (2020). Patient experience in the digital age: An investigation into the effect of generational cohorts. *Journal of Retailing and Consumer Services*, *57*, 102221.

Allen, N. J., & Meyer, J. P. (1990). The measurement and antecedents of affective, continuance and normative commitment to the organization. Journal of occupational psychology, 63(1), 1-18.

Anderson, M. (2018). Understanding Gen Z through the lens of YouTube. *Think with Google.* Retrieved from https://www.thinkwithgoogle.com/marketing-strategies/video/gen-z-and-youtube/

Anderson, M., & Jiang, J. (2018). Teens, Social Media & Technology 2018. *Pew Research Center.* Retrieved from https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/

Backhouse, J., & Dhillon, G. (1996). Structures of responsibility and security of information systems. *European Journal of Information Systems*, 5(1), 2-9.

Bansal, G., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision support systems*, *49*(2), 138-150.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. Information & Management, 53(1), 1-21.

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security*, *59*, 9-25.

Beall, G. (2017). 8 Key Differences between Gen Z and Millennials. *Huffpost*. Retrieved from https://www.huffpost.com/entry/8-key-differences-between_b_12814200

Beck, K., & Wilson, C. (2000). Development of affective organizational commitment: A cross-sequential examination of change with tenure. Journal of vocational behavior, 56(1), 114-136.

Beck, L., & Wright, A. (2019). iGen: What You Should Know about Post-Millennial Students. *College and University*, *94*(1), 21-26.

Beckingham, K. (2019). Digital natives more prone to cyberattacks. *University Business.* Retrieved from https://universitybusiness.co.uk/news/digital-natives-more-prone-to-cyber-attacks/

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. The journal of strategic Information Systems, 11(3-4), 245-270.

Bennett, G., & Lachowetz, T. (2004). Marketing to lifestyles: Action sports and Generation Y. Sport Marketing Quarterly, 13(4), 239-243.

Bentley, J. P., & Thacker, P. G. (2004). The influence of risk and monetary payment on the research participation decision making process. Journal of medical ethics, 30(3), 293-298.

Berkowitz, E. N., & Schewe, C. D. (2011). Generational cohorts hold the key to understanding patients and health care providers: Coming-of-age experiences influence health care behaviors for a lifetime. *Health Marketing Quarterly*, *28*(2), 190-204.

Bilderlings (2018). Generation Z: Buyers Of The Future. *Bilderlings Blog.* Retrieved from: https://bilderlings.com/blog/generation-z-buyers-of-the-future/

Birzniece, I. (2018). Security Analytics: Dispelling the Fog. *In BIR Workshops* (pp. 160-169).

Borchers, A. (2001). Trust in Internet shopping: A test of a measurement instrument. AMCIS 2001 Proceedings, 156.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. European Journal of Information Systems, 18(2), 151-164.

Boucher, J. (2018). Top 10 Gen Z Statistics From 2018. The Center for Generational Kinetics. Retrieved from https://genhq.com/top-10-ways-gen-z-is-shaping-the-future/

Bourne, V. (2018). Is the next generation aware of cyber security's importance? *SANS Institute.* Retrieved from https://www.sans.org/igen-cyber-security-research-report

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. Journal of computer-mediated communication, 13(1), 210-230.

Bradley, R., (2018). How Marketers Can Prepare for Generation Z's Social Media Habits. *The Manifest.* Retrieved from https://themanifest.com/social-media/how-marketers-can-prepare-generation-zs-social-media-habits

Brooke, P. P., Russell, D. W., & Price, J. L. (1988). Discriminant validation of measures of job satisfaction, job involvement, and organizational commitment. *Journal of applied psychology*, *73*(2), 139.

Brosdahl, D. J., & Carpenter, J. M. (2012). US male generational cohorts: Retail format preferences, desired retail attributes, satisfaction and loyalty. Journal of Retailing and Consumer Services, 19(6), 545-552.

Brown, E. (2019). The Internet as a human experience is an integral part of Gen identity. ZD Net. Retrieved from https://www.zdnet.com/article/gen-z-willing-to-provide-their-personal-data-for-more-personalized-experiences/

Brown, L. (2020). How Demographic Shifts Will Impact the Global Workplace by 2030. GlobeSt.com. Retrieved from https://www.globest.com/2020/01/20/how-demographic-shifts-will-impact-the-global-workplace-by-2030/?slreturn=20201106085646

Bugental, D. B., Blue, J., & Cruzcosa, M. (1989). Perceived control over caregiving outcomes: Implications for child abuse. Developmental psychology, 25(4), 532.

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

Bush, V. D., Venable, B. T., & Bush, A. J. (2000). Ethics and marketing on this internet: Practitioners' perceptions of societal, industry and company concerns. Journal of business ethics, 23(3), 237-248.

Campbell, A. J. (1997). Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. Journal of Direct Marketing, 11(3), 44-57.

Carboni-Brito, A. L. (2011). Analysis of the Development of Internet and Social Media Organizational Policies and Practices–Are Policies and Practices Hindering or Enhancing the Acquisition and Use of Employees' Virtual Social Capital? (Doctoral dissertation, Department of Management, King's College London).

Carpenter, J. M., & Moore, M. (2005). Consumer preferences for retail formats: Implications for tenant mix strategies. Journal of Shopping Center Research, 12(1), 1–21.

Castellano, S. (2016, February). Welcome Generation Z to work. In Talent Development (Vol. 70, No. 2, p. 18).

Chai, K. H., Yap, C. M., & Wang, X. (2011). Network closure's impact on firms' competitive advantage: The mediating roles of knowledge processes. Journal of Engineering and Technology Management, 28(1-2), 2-22.

Chai, S., Das, S., & Rao, H. R. (2011). Factors affecting bloggers' knowledge sharing: An investigation across gender. Journal of Management Information Systems, 28(3), 309-342.

Chamberlain, L., (2017). Gen-Z Members Watch An Average Of 68 Videos Per Day. *Geo Marketing.* Retrieved from https://geomarketing.com/gen-z-members-watch-an-average-of-68-videos-per-day

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. Government Information Quarterly, 35(3), 445-459.

Chen, A., Lu, Y., Chau, P. Y., & Gupta, S. (2015). Classifying, measuring, and predicting users' overall active behavior on social networking sites. Journal of Management Information Systems, 31(3), 213-253.

Chen, S. C., & Dhillon, G. S. (2003). Interpreting dimensions of consumer trust in e-commerce. *Information Technology and Management*, 4(2-3), 303-318.

Clarke, R. (2019). Risks inherent in the digital surveillance economy: A research agenda. *Journal of Information Technology,* 34(1), 59-80.

Cobanoglu, C., & Cobanoglu, N. (2003). The effect of incentives in web surveys: application and ethical considerations. International Journal of Market Research, 45(4), 1-13.

Conger, J (1997). Changing of the Guard: How Generational Shifts Will Transform Organizational Life. The Organization of the Future.

Consultancy.uk (2015). UK Generation Z wants more emphasis on cyber security. *Consultancy.org.* Retrieved from https://www.consultancy.uk/news/3100/uk-generation-z-wants-more-emphasis-on-cyber-security

Corbett, J. M., & Lee, J. (2006). The impact of downsizing on employees' affective commitment. Journal of Managerial Psychology.

Corbett, S. (2013). The retention of personal information online: A call for international regulation of privacy law. Computer Law & Security Review, 29(3), 246-254.

Cosgrove, A. (2019). Why Diversity in Security Teams Can Give Organizations An Edge Over Cyber-criminals. Info Security. Retrieved from https://www.infosecurity-magazine.com/blogs/diversity-teams-edge/

Coss, D. L., & Dhillon, G. (2020). A framework for auditing and strategizing to ensure cloud privacy. *Journal of Information Systems*, 34(2), 47-63.

Costa, P. T., & McCRAE, R. R. (1999). A five-factor theory of personality. Handbook of personality, 2nd edn. Guilford Press, New York, 139-153.

Coupland, D. (1991). Generation X: Tales for an accelerated culture. Macmillan.

CSM Newsdesk (2019). Gen Z Rely on the Internet Primarily for Social Media and Entertainment. The Magazine for Customer Service Managers & Professionals. https://www.customerservicemanager.com/gen-z-rely-on-the-internet-primarily-for-social-media-and-entertainment/

Curtis, S. K. (2012). *Commitment to cybersecurity and information technology governance: A case study and leadership model* (Doctoral dissertation, University of Phoenix).

Curtis, S. K. (2012). Commitment to cybersecurity and information technology governance: A case study and leadership model (*Doctoral dissertation, University of Phoenix*).

Curtis, S. K. (2012). Commitment to cybersecurity and information technology governance: A case study and leadership model (Doctoral dissertation, University of Phoenix).

Dalgic, G. (2014). Organizational commitment and gender: A meta-analysis. *Issues in Educational Research* 24(2):133-151 2014

Davis, J. A. (2004). Did growing up in the 1960s leave a permanent mark on attitudes and values? Evidence from the General Social Survey. *Public Opinion Quarterly*, *68*(2), 161-183.

de Ruyter, K., Keeling, D. I., & Cox, D. (2019). Customer-supplier relationships in high technology markets 3.0. Industrial Marketing Management, 79, 94-101.

Demirtas, O., & Akdogan, A. A. (2015). The effect of ethical leadership behavior on ethical climate, turnover intention, and affective commitment. *Journal of Business Ethics*, *130*(1), 59-67.

Dhillon, G., Abdul Talib, Y. Y., & Picoto, W. N. (2020). The Mediating Role of Psychological Empowerment in Information Security Compliance Intentions. *Journal of the Association for Information Systems*, 21(1), 5.

Dhillon, G., Oliveira, T., & Syed, R. (2018). Value-based information privacy objectives for Internet Commerce. *Computers in Human Behavior*, 87, 292-307.

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security*, 56, 63-69.

Dimock, M., (2019). Defining generations: Where Millennials end and Generation Z begins. *Pew Research Center.* Retrieved from https://www.pewresearch.org/fact-tank/2019/01/17/where-millennials-end-and-generation-z-begins/

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research*, *17*(1), 61-80.

Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer–seller relationships. Journal of marketing, 61(2), 35-51.

Dou, W., Wang, G., & Zhou, N. (2006). Generational and regional differences in media consumption patterns of Chinese generation X consumers. *Journal of Advertising*, *35*(2), 101-110.

Duma, F., & Gligor, R. (2018). STUDY REGARDING ROMANIAN STUDENTS'PERCEPTION AND BEHAVIOUR CONCERNING THE FINTECH AREA WITH A FOCUS ON CRYPTOCURRENCIES AND ONLINE PAYMENTS. *Online Journal Modelling the New Europe*, (27).

Dunham, C. C. (1998). Generation units and the life course: A sociological perspective on youth and the anti-war movement. Journal of political and military sociology, 26(2), 137.

Dutton, J. E., Ashford, S. J., O'Neill, R. M., & Lawrence, K. A. (2001). Moves that matter: Issue selling and organizational change. Academy of Management journal, 44(4), 716-736.

Dwyer, P. D., Gilkeson, J. H., & List, J. A. (2002). Gender differences in revealed risk taking: evidence from mutual fund investors. Economics Letters, 76(2), 151-158.

E. Mccallister, T. Grance, K. Scarfone, (2010). Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). National Institute of Standards and Technology, U.S. Department of Commerce. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

Elbeltagi, I. and Agag, G. (2016), E-retailing ethics and its impact on customer satisfaction and repurchase intention: A cultural and commitment-trust theory perspective. *Internet Research,* Vol. 26 No. 1, pp. 288-310.

Fischer, E. A. (2016). Cybersecurity issues and challenges: In brief. *Congressional Research Service* 7-5700 R43831

Fisher, M. (2014). A comparison of professional value development among pre-licensure nursing students in associate degree, diploma, and bachelor of science in nursing programs. Nursing Education Perspectives, 35(1), 37-42.

Fisher, T. F., & Crabtree, J. L. (2009). Generational cohort theory: Have we overlooked an important aspect of the entry-level occupational therapy doctorate debate? *American Journal of Occupational Therapy*, *63*(5), 656-660.

Floridi, L., & Taddeo, M. (2016). What is data ethics? *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 374*.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. Journal of marketing research, 18(1), 39-50.

Gabisch, J. A., & Milne, G. R. (2014). The impact of compensation on information ownership and privacy control. Journal of Consumer Marketing.

Gao, (2008). Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information. U.S. Government Accountability Office. Retrieved from http://www.gao.gov/new.items/d08536.pdf2008.

Gardner, S., & Eng, S. (2005). What students want: Generation Y and the changing function of the academic library. portal: Libraries and the Academy, 5(3), 405-420.

Gautam, T., Van Dick, R., & Wagner, U. (2004). Organizational identification and organizational commitment: Distinct aspects of two related concepts. Asian Journal of Social Psychology, 7(3), 301-315.

Geiger, E. (2018). Who Are the iGeneration and What Does Research Tell Us?. Retrieved from https://ericgeiger.com/2018/01/who-are-the-igeneration-and-what-does-research-tell-us/

Gellatly, I. R. (1995). Individual and group determinants of employee absenteeism: Test of a causal model. Journal of organizational behavior, 16(5), 469-485.

Geyskens, I., Steenkamp, J. B. E., Scheer, L. K., & Kumar, N. (1996). The effects of trust and interdependence on relationship commitment: A trans-Atlantic study. International Journal of research in marketing, 13(4), 303.

Goldberg, L. R. (1992). The development of markers for the Big-Five factor structure. *Psychological assessment*, *4*(1), 26.

González, T. F., & Guillen, M. (2008). Organizational commitment: A proposal for a wider ethical conceptualization of 'normative commitment'. Journal of Business Ethics, 78(3), 401-414.

Goodwin, C., and Nicholas, J. P (2015). A framework for cybersecurity information sharing and risk reduction. Microsoft.

Goodwin, C., Nicholas, J. P., Bryant, J., Ciglic, K., Kleiner, A., Kutterer, C., ... & Storch, T. (2015). A framework for cybersecurity information sharing and risk reduction. *Microsoft*.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. Journal of Accounting and Public Policy, 34(5), 509-519.

Govani, T., & Pashley, H. (2005). Student awareness of the privacy implications when using Facebook. Unpublished paper presented at the "Privacy poster fair" at the Carnegie Mellon university school of library and information science, 9, 1-17.

Greenberg, A. (2003, October). New generation, new politics: As Generation Y steps into the polling booths, how will political life change? American Prospect, pp. A3–A5.

Greenberg, J. (2003). Metadata and the world wide web. Encyclopedia of library and information science, 3, 1876-1888.

Griffin, M. L., Hogan, N. L., Lambert, E. G., Tucker-Gail, K. A., & Baker, D. N. (2010). Job involvement, job stress, job satisfaction, and organizational commitment and the burnout of correctional staff. *Criminal Justice and behavior*, *37*(2), 239-255.

Grothaus, M. (2019). Gen Z think they're better at online security than they actually are. *FAST Company.* Retrieved from https://www.fastcompany.com/90343839/gen-z-think-theyre-better-at-online-security-than-they-actually-are

Gundlach, G. T., & Murphy, P. E. (1993). Ethical and legal foundations of relational marketing exchanges. Journal of marketing, 57(4), 35-46.

Gustafsod, P. E. (1998). Gender Differences in risk perception: Theoretical and methodological erspectives. Risk analysis, 18(6), 805-811.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (1998). Multivariate data analysis (Vol. 5, No. 3, pp. 207-219). Upper Saddle River, NJ: Prentice hall.

Hair, J. F., Henseler, J., Dijkstra, T. K., & Sarstedt, M. (2014). Common beliefs and reality about partial least squares: comments on Rönkkö and Evermann.

Hair, J. F., Ringle, C. M., and Sarstedt, M. 2011. PLS-SEM: Indeed a Silver Bullet. *Journal of Marketing Theory and Practice* 19 (2): 139-151.

Hajli, M. N. (2014). A study of the impact of social media on consumers. International Journal of Market Research, 56(3), 387-404.

Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics*, *133*(1), 111-123.

Halliday, S., & Astafyeva, A. (2014). Millennial cultural consumers: co-creating value through brand communities. Arts Marketing.

Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. Journal of Management Information Systems, 24(2), 13-42.

Harrison, M., (2018). Gen Z Might be the Answer to the Cybersecurity Workforce Shortage. *CyberSecuritySummit.* Retrieved from https://www.cybersecuritysummit.org/2018/09/14/gen-z-cybersecurity-careers/

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the academy of marketing science, 43(1), 115-135.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106-125.

Herosmyth (2020). 75 Eye-Opening Statistics on How Each Generation Uses Technology. *Herosmyth.* Retrieved from: https://www.herosmyth.com/article/75-eye-opening-statistics-how-each-generation-uses-technology

Hofstede, G. (1984). Culture's consequences: International differences in work-related values (Vol. 5). sage.

Holgate, J. A. & Hardy, C. A. (2012). Information Security Governance: Investigating Diversity in Critical Infrastructure Organizations. In Bled eConference (p. 13).

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *Mis Quarterly,* 275-298.

Horzum, M. B. (2016). Examining the relationship to gender and personality on the purpose of Facebook usage of Turkish university students. Computers in Human Behavior, 64, 319-328.

Hoxha, V., & Zeqiraj, E. (2019). The impact of Generation Z in the intention to purchase real estate in Kosovo. *Property Management,* Volume 38 Issue 1

Hsu, C. W. (2009). Frame misalignment: interpreting the implementation of information systems security certification in an organization. European Journal of Information Systems, 18(2), 140-150.

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security–a neo-institutional perspective. The Journal of Strategic Information Systems, 16(2), 153-172.

Huffman, M., (2017).Millennials less worried about cybersecurity than older generations. *Consumeraffairs*. Retrieved from: https://www.consumeraffairs.com/news/millennials-less-worried-about-cybersecurity-than-older-generations-101817.html

Hui, K. L., Teo, H. H., & Lee, S. Y. T. (2007). The value of privacy assurance: an exploratory field experiment. Mis Quarterly, 19-33.

Inglehart, R., 1977. The Silent Revolution: Changing Values and Political Styles Among Western Publics. Princeton University Press, Princeton

Jackson, S. E., Joshi, A., & Erhardt, N. L. (2003). Recent research on team and organizational diversity: SWOT analysis and implications. Journal of management, 29(6), 801-830.

James, L. (2018). Artificial Threat Intelligence: Using Data Science to Augment Analysis. MIS Training Institute. Retrieved from https://misti.com/infosec-insider/artificial-threat-intelligence-using-data-science-to-augment-analysis

Jaros, S. (2007). Meyer and Allen model of organizational commitment: Measurement issues. The Icfai Journal of Organizational Behavior, 6(4), 7-25.

Jarvenpaa, S. L., & Staples, D. S. (2001). Exploring perceptions of organizational ownership of information and expertise. Journal of management information systems, 18(1), 151-183.

Jenkins, J. M. (1993). Self-monitoring and turnover: The impact of personality on intent to leave. Journal of Organizational Behavior, 14(1), 83-91.

Jenkins, R. (2017). Forget millennials — here are 8 things you'll want to remember about Gen Z. *Business Insider.* Retrieved from https://www.businessinsider.com/forget-millennials-here-are-8-things-to-know-about-gen-z-2017-7

Jha, S. (2011). Influence of psychological empowerment on affective, normative and continuance commitment. Journal of Indian Business Research.

Johnson, A. M. (2009). Business and security executives views of information security investment drivers: Results from a delphi study. Journal of Information Privacy and Security, 5(1), 3-27.

Joinson, A. N., Reips, U. D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. Human–Computer Interaction, 25(1), 1-24.

Jones, A. L. (2011). Generational cohort differences in types of organizational commitment among nurses in Alabama.

Jones, A. L. (2014). Generational cohort differences in types of organizational commitment.

Jones, C., & Hosein, A. (2010). Profiling university students' use of technology: where is the NET generation divide?. The International Journal of Technology Knowledge and Society, 6(3), 43-58.

Kahneman, D., & Tversky, A. (1986). Rational choice and the framing of decisions. *Journal of business*, *59*(4), 251-278.

Kahneman, D., & Tversky, A. (2013). Prospect theory: An analysis of decision under risk. In *Handbook of the fundamentals of financial decision making: Part I* (pp. 99-127).

Kapoor, M., (2020). TikTok: designing digital products for the Generation-Z mindset. *UX Collective.* Retrieved from https://uxdesign.cc/tiktok-designing-digital-products-for-the-millennial-mindset-864aa42652bf

Kaur, J., & Sharma, S. K. (2015). Measuring organizational commitment: scale validation for Indian financial services sector. *IUP Journal of Organizational Behavior*, *14*(4), 28.

Keith, M. J., Maynes, C., Lowry, P. B., & Babb, J. (2014, December). Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure. In *International Conference on Information Systems (ICIS 2014), Auckland, New Zealand, December* (pp. 14-17).

Kennedy, M. L. (2018). *Moving Beyond Open Access to Digital Fluency: The Opportunities to Create an Information Environment for Tomorrow's Science: EN Ecosistemas del Acceso Abierto*. Ediciones Universidad de Salamanca.

Kim, J. W., & Chock, T. M. (2017). Personality traits and psychological motivations predicting selfie posting behaviors on social networking sites. Telematics and Informatics, 34(5), 560-571.

Kircaburun, K., Alhabash, S., Tosuntaş, Ş. B., & Griffiths, M. D. (2018). Uses and gratifications of problematic social media use among university students: A simultaneous examination of the Big Five of personality traits, social media platforms, and social media use motives. International Journal of Mental Health and Addiction, 18(3), 525-547.
Kircaburun, K., Alhabash, S., Tosuntaş, Ş. B., & Griffiths, M. D. (2018). Uses and gratifications of problematic social media use among university students: A simultaneous examination of the Big Five of personality traits, social media platforms, and social media use motives. International Journal of Mental Health and Addiction, 18(3), 525-547.
Kitchen, P. J., & Proctor, T. (2015). Marketing communications in a post-modern world. Journal of business strategy.

Kitchin, R., & Dodge, M. (2019). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. Journal of urban technology, 26(2), 47-65.

Kline, R. B. (2011). Principles and practice of structural equation modeling (3rd ed.). New York: Guilford Press.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: management's effect on culture and policy. Information Management & Computer Security.

Koontz, L. D. (2008). *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*. DIANE Publishing.

Koulopoulos, T., & Keldsen, D. (2014). Gen Z Effect: The Six Forces Shaping the Future of Business. Bibliomotion. Inc., New York.

Kracher, B., & Corritore, C. L. (2004). Is there a special e-commerce ethics?. Business Ethics Quarterly, 71-94.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. Journal of information technology, 25(2), 109-125.

Kreamer, J. (2018). Are Gen Z'ers going to make data security a bigger issue? *Hanzo.* Retrieved from https://www.hanzo.co/blog/are-gen-z-going-to-make-data-security-a-bigger-issue

Kupperschmidt, B. (2006). Addressing multigenerational conflict: Mutual respect and carefronting as strategy. Online Journal of Issues in Nursing, 11(2).

Landrum, S. (2017). Millennials, Trust And Internet Security. *Forbes.* Retrieved from https://www.forbes.com/sites/sarahlandrum/2017/06/28/millennials-trust-and-internet-security/?sh=835e6965555e

Lantos, G. P. (2011). Consumer Behavior in Action: Real-life Applications for Marketing Managers. New York: M. E. Shape.

Lee, K., Carswell, J. J., & Allen, N. J. (2000). A meta-analytic review of occupational commitment: relations with person-and work-related variables. *Journal of applied psychology*, *85*(5), 799.

Lee, W., Tyrrell, T., & Erdem, M. (2013). Exploring the behavioral aspects of adopting technology. Journal of Hospitality and Tourism Technology.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. European Journal of Information Systems, 18(2), 177-187.

Levin, M., (2017). 6 Things You Need to Know About Generation Z Before Hiring Them. *Mansueto Ventures, INC.* Retrieved from https://www.inc.com/marissa-levin/6-things-you-need-to-know-about-the-gen-z-generati.html

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*(3), 434-445.

Li, X., & Santhanam, R. (2008). Will it be disclosure or fabrication of personal information? An examination of persuasion strategies on prospective employees. *International Journal of Information Security and Privacy (IJISP)*, *2*(4), 91-109.

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. MIS quarterly, 59-87.

Lin, X., Featherman, M., Brooks, S. L., & Hajli, N. (2019). Exploring gender differences in online consumer purchase decision making: An online product presentation perspective. Information Systems Frontiers, 21(5), 1187-1201.

Lin, X., Li, Y., Califf, C. B., & Featherman, M. (2013). Can social role theory explain gender differences in Facebook usage?. In 2013 46th Hawaii International Conference on System Sciences (pp. 690-699). IEEE.

Lissitsa, S., & Kol, O. (2016). Generation X vs. Generation Y–A decade of online shopping. Journal of Retailing and Consumer Services, 31, 304-312.

Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2005). Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. Information & Management, 42(2), 289-304.

Lu, Y. & Ramamurthy, K. (2011). Understanding the Link Between Information Technology Capability and Organizational Agility: An Empirical Examination. MIS Quarterly, 35(4), 931-954

Lumley, E. J., Coetzee, M., Tladinyane, R., & Ferreira, N. (2011). Exploring the job satisfaction and organisational commitment of employees in the information technology environment. *Southern African business review*, *15*(1).

Lumley, E. J., Coetzee, M., Tladinyane, R., & Ferreira, N. (2011). Exploring the job satisfaction and organisational commitment of employees in the information technology environment. Southern African business review, 15(1).

Lunarline (2018). Gen Z, Millennials Most Likely to Be Victims of Tech Support Scams. Lunarline. Retrieved from https://lunarline.com/gen-z-millennials-tech-support-scams/

Maguire, L., (2020). Gen Z is Reinventing Social Media Marketing. Vogue Business. Retrieved from https://www.voguebusiness.com/consumers/gen-z-reinventing-social-media-marketing-tiktok-youtube-instagram-louis-vuitton

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information systems research, 15(4), 336-355.

Manifest, (2019). Why Generation Z Loves YouTube. The Manifest. Retrieved from https://medium.com/@the_manifest/why-generation-z-loves-youtube-ec64643bd5b2

Mannheim's, K. A. R. L. (1952). Ideologie und Utopie. Frankfurt/Main, 19523.

Mastroianni, B. (2016). How Generation Z is changing the tech world. CBS News. Retrieved from https://www.cbsnews.com/news/social-media-fuels-a-change-in-generations-with-the-rise-of-gen-z/

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of management review, 20(3), 709-734.

McCrindle, M. (2014). The A, B, C of XYZ understanding the global generations. University of New South Wales Press, Sydney (237 pp.). 9781742230351. Bella Vista: McCrindle Research Pty Ltd.

McCrindle, M., & Wolfinger, E. (2010). Generations defined. Ethos, 18(1), 8.

McCullough, K. (2018). 10 Things You Need to Know About Gen Z. Retrieved from https://www.karenmccullough.com/10-things-you-need-to-know-about-gen-z/

McFadzean, E., Ezingeard, J. N., & Birchall, D. (2006). Anchoring information security governance research: sociological groundings and future directions. Journal of Information System Security, 2(3), 3-48.

McHenry, W. K., & Ash, S. R. (2010). Generational Responses to Knowledge Management and Collaboration: Are GenX and GenY as Different As We Think?. In 2010 43rd Hawaii International Conference on System Sciences (pp. 1-10). IEEE.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research*, *13*(3), 334-359.

Meyer, J. P., & Allen, N. J. (1991). A three-component conceptualization of organizational commitment. Human resource management review, 1(1), 61-89.

Meyer, J. P., & Allen, N. J. (1997). Commitment in the workplace: Theory, research, and application. Sage.

Meyer, J. P., & Herscovitch, L. (2001). Commitment in the workplace: Toward a general model. Human resource management review, 11(3), 299-326.

Meyer, J. P., Stanley, D. J., Herscovitch, L., & Topolnytsky, L. (2002). Affective, continuance, and normative commitment to the organization: A meta-analysis of antecedents, correlates, and consequences. Journal of vocational behavior, 61(1), 20-52.

Milne, G. R. (1997). Consumer participation in mailing lists: A field experiment. *Journal of Public Policy & Marketing*, *16*(2), 298-309.

Milne, G. R., & Boza, M. E. (1999). Trust and concern in consumers' perceptions of marketing information management practices. Journal of interactive Marketing, 13(1), 5-24.

Miranda, S. M., & Saunders, C. S. (2003). The social construction of meaning: An alternative perspective on information sharing. Information systems research, 14(1), 87-106.

Misoch, S. (2015). Stranger on the internet: Online self-disclosure and the role of visual anonymity. Computers in Human Behavior, 48, 535-541.

MobileIDWorld (2017). The Future of Digital Experience: Gen Z Wants Authenticity, All Want Security. *MobileIDWorld.* Retrieved from https://mobileidworld.com/gen-z-wants-authenticity-012065/

Moorman, C., Zaltman, G., & Deshpande, R. (1992). Relationships between providers and users of market research: The dynamics of trust within and between organizations. Journal of marketing research, 29(3), 314-328.

Moschis, G. P., Lee, E., Mathur, A., Moschis, G., & Strautman, J. (2000). The maturing marketplace: Buying habits of baby boomers and their parents. Greenwood Publishing Group.

Mothersbaugh, D. L., Foxx, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of service research*, *15*(1), 76-98.

Moynihan, L. M., Boswell, W. R., & Boudreau, J. W. (2000). The influence of job satisfaction and organizational commitment on executive withdrawal and performance.

Nardi, B. A., Whittaker, S., & Schwarz, H. (2002). NetWORKers and their activity in intensional networks. Computer Supported Cooperative Work (CSCW), 11(1-2), 205-242.

Niemczyk, A., Seweryn, R., & Smalec, A. (2019). Z generation in the international tourism market. Economic and Social Development: Book of Proceedings, 123-132.

Nolan, A. (2015). Cybersecurity and information sharing: Legal challenges and solutions (pp. 7-5700). Congressional Research Service.

Nowak, G. J., & Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. *Journal of Direct Marketing*, *9*(3), 46-60.

Nunnally, J. C. (1978). Psychometric theory (2nd ed.). McGraw-Hill.

Obama, B., (2013). Improving Critical Infrastructure Cybersecurity. Presidential Executive Order #13636. Retrieved from http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

Oblinger, D. (2003, July/August). Boomers, Gen-Xers, and Millennials: Understanding the new students. Educause Review, pp. 37–47.

Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. Journal of economic psychology, 25(2), 243-262.

Oltsik, J. (2019). *The life and times of cybersecurity professionals 2018*. Research report. Enterprise strategy group and information systems security associate.

organizations: Examining the motivations of Gen Y cohorts, International Journal of Information Management , 36,

Padayachee, K. (2017). The myths and realities of generational cohort theory on ICT integration in education: A South African perspective. *The African Journal of Information Systems*, *10*(1), 4.

Palley, W. (2012). Gen Z: Digital in their DNA. New York, NY: Thompson. Retrieved from http://www.jwtintelligence.com/wpcontent/uploads

Parment, A. (2013). Generation Y vs. Baby Boomers: Shopping behavior, buyer involvement and implications for retailing. Journal of Retailing and Consumer Services , 20(2), pp. 189– 199. https://doi.org/10.1016/j.jretconser.2012.12.001

Patnayakuni, R., & Patnayakuni, N. (2014). Information security in value chains: A governance perspective.

Pavlou, P. A., & Gefen, D. (2005). Psychological contract violation in online marketplaces: Antecedents, consequences, and moderating role. Information systems research, 16(4), 372-399.

Pearson (2018). Beyond Millennials: The Next Generation of Learners. *Global Research & Insights.* Retrieved from https://www.pearson.com/content/dam/one-dot-com/one-dot-com/global/Files/news/news-annoucements/2018/The-Next-Generation-of-Learners_final.pdf

Pedersen, D. M. (1982). Personality correlates of privacy. *The Journal of Psychology*, *112*(1), 11-14.

Perry, R. P., Hladkyj, S., Pekrun, R. H., & Pelletier, S. T. (2001). Academic control and action control in the achievement of college students: A longitudinal field study. Journal of educational psychology, 93(4), 776.

Perry, R. W. (2004). The relationship of affective organizational commitment with supervisory trust. Review of public personnel administration, 24(2), 133-149.

Poague, E. (2018). Gen Z Is Shaping a New Era of Learning: Here's What you Should Know. Linkedin Learning Blog. Retrieved from https://www.linkedin.com/business/learning/blog/learning-and-development/gen-z-is-shaping-a-new-era-of-learning-heres-what-you-should-kn

Pond, S. B., Nacoste, R. W., Mohr, M. F., & Rodriguez, C. M. (1997). The measurement of organizational citizenship behavior: Are we assuming too much? *Journal of Applied Social Psychology*, 27, 1527–1544.

Ponemon, L. (2013). Cost of data breach study: Global analysis. *Poneomon Institute sponsored by Symantec*.

Porter, L. W., Steers, R. M., Mowday, R. T., & Boulian, P. V. (1974). Organizational commitment, job satisfaction, and turnover among psychiatric technicians. Journal of applied psychology, 59(5), 603.

Prensky, M. (2001), "Digital natives digital immigrants", On the Horizon, Vol. 9 No. 5, pp. 1-6.

Prince, C. (2018). Do consumers want to control their personal data? Empirical evidence. International Journal of Human-Computer Studies, 110, 21-32.

Prosser, W. (1960) Privacy, Calif. *Law Rev.* 48, pp. 383–422.

Pruett, M., (2018). Gen Z's Favorite Social Networks: YouTube, Instagram, Snapchat. *Criteo.* Retrieved from https://www.criteo.com/blog/gen-z-social-media/

Pruett, M., (2018). Millennials vs Gen Z: 4 Differences in What They Care About. *Criteo.* Retrieved from https://www.criteo.com/blog/millennials-vs-gen-z/

QuestionPro (2018). Organizational Commitment: Definition, benefits, and How to Improve It. *QuestionPro.* Retrieved from https://www.questionpro.com/blog/organizationalcommitment/#targetText=Organizational%20commitment%20is%20defined%20as,he%2Fshe%20is%20working%20for.

Randall, M. L., Cropanzano, R., Bormann, C. A., & Birjulin, A. (1999). Organizational politics and organizational support as predictors of work attitudes, job performance, and organizational citizenship behavior. *Journal of Organizational Behavior*, 20, 159–174

Rathi, N., & Rastogi, R. (2009). Assessing the relationship between emotional intelligence, occupational self-efficacy and organizational commitment. Journal of the Indian Academy of Applied Psychology, 35(1), 93-102.

Rideout, V. J., Foehr, U. G., & Roberts, D. F. (2010). Generation M2: Media in the lives of 8-18 year olds. Menlo Park, CA: Kaiser Family Foundation. Retrieved from http://kaiserfamilyfoundation.files.wordpress.com/2013/01/8010.pdf

Rogler, L. H. (2002). Historical generations and psychology: The case of the Great Depression and World War II. American psychologist, 57(12), 1013.

Rohm, A. J., & Milne, G. R. (2004). Just what the doctor ordered: the role of information sensitivity and trust in reducing medical information privacy concern. Journal of Business Research, 57(9), 1000-1011.

Rosen, L. D., (2010). Welcome to the iGeneration. *Psychology Today.* Retrieved from https://www.psychologytoday.com/us/blog/rewired-the-psychology-technology/201003/welcome-the-igeneration

Ryder, N. B. (1965). The cohort concept in the study of social change. American Sociological Review, 30, 843–861.

Salleh, M. S. M., Mahbob, N. N., & Baharudin, N. S. (2017). Overview of" Generation Z "Behavioural Characteristic and its Effect towards Hostel Facility. International Journal of Real Estate Studies, 11(2), 59-67.

Sarang, R., (2018). What the Mobile-Born Mean for IoT and Cybersecurity. *McAfee*. Retrieved from https://www.mcafee.com/blogs/consumer/mobile-and-iot-security/mobile-born-iot-cybersecurity/

Schiola, E. (2017). Generation Z Opts for Personalization Over Privacy: What That Means for WordPress. *Turque.* Retrieved from: https://torquemag.io/2017/12/generation-z-opts-personalization-privacy-means-wordpress/

Schiola, E. (2019). Why Generation Z is the Most Entrepreneurial Generation. *Turque.* Retrieved from: https://torquemag.io/2019/02/why-generation-z-is-the-most-entrepreneurial-generation/

Schlegelmilch, B. B., & Öberseder, M. (2010). Half a century of marketing ethics: Shifting perspectives and emerging trends. Journal of Business Ethics, 93(1), 1-19.

Schmoll, B. J., & Moses, Y. T. (2002). Responding to change and forces in higher education. Journal of Physical Therapy Education, 16(3), 14.

Schneider, J., (2015). How to Market to the iGeneration. *Harvard Business Review.* Retrieved from https://hbr.org/2015/05/how-to-market-to-the-igeneration

Schofield, D. J., & Fletcher, S. L. (2007). The physiotherapy workforce is ageing, becoming more masculinised, and is working longer hours: a demographic study. Australian Journal of Physiotherapy, 53(2), 121-126.

Schoo, A. M. M., Stagnitti, K., Mercer-Grant, C., & Dunbar, J. A. (2005). A conceptual model for recruitment and retention: allied health workforce enhancement in Western Victoria, Australia. Rural and Remote Health, 5, 477.

Schröder, M. K., & Theilen, A. T. (2019). Sharing Economy Services–Analysis of Customers' Motives and Concerns.

Security News Desk, (2016). Generation Z and Cybersecurity: can businesses balance both? Retrieved from https://securitynewsdesk.com/generation-z-and-cybersecurity-can-businesses-balance-both/

Sessa, V. I., Kabacoff, R. I., Deal, J., & Brown, H. (2007). Generational differences in leader values and leadership behaviors. *The Psychologist-Manager Journal*, *10*(1), 47-74.

Seymour, E.(2019). Gen Z: Born to Be Digital. VoA News. Retrieved from https://www.voanews.com/student-union/gen-z-born-be-digital

Shirish, A., Boughzala, I. and Srivastava, S. C. (2016) Adaptive use of social networking applications in contemporary organizations: Examining the motivations of Gen Y cohorts, International Journal of Information Management , 36, 6, Part A, 1111-1123.

Shoemaker, D., Kohnke, A., & Laidlaw, G. (2019). ETHICS AND CYBERSECURITY ARE NOT MUTUALLY EXCLUSIVE. *EDPACS*, *60*(1), 1-10.

Skill, T., (2019). The Coming Generation-Z Impact on Cybersecurity. *Education Technology Insights.* Retrieved from https://collaboration.educationtechnologyinsights.com/cxoinsights/the-coming-generationz-impact-on-cybersecurity-nid-585.html

Skinner, E. A. (1996). A guide to constructs of control. Journal of personality and social psychology, 71(3), 549.

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security, 60, 154-176.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. MIS quarterly, 989-1015.

Smithson, N. (2018). What Generation Z can teach you about marketing. Retrieved from https://nataliesmithson.com/what-generation-z-can-teach-you-about-marketing

Somers, M. J. (1995). Organizational commitment, turnover and absenteeism: An examination of direct and interaction effects. Journal of organizational Behavior, 16(1), 49-58.

Somers, M. J. (1999). Application of two neural network paradigms to the study of voluntary employee turnover. Journal of Applied Psychology, 84(2), 177.

Sparks and Honey. (2017). Generation Z 2025: The Final Generation. Sparks and Honey, New York, NY.

Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in personnel and human resources management*, *8*(3), 349-411.

Straub, D. W. (1989). Validating instruments in MIS research. MIS quarterly, 147-169.

Stumbo, T., Thiele, A., & York, A. M. (2007). Generic abilities as rank ordered by Baby Boomer and Generation X physical therapists. Journal of Physical Therapy Education, 21(2), 48-52.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure?. Computers in Human Behavior, 29(3), 821-826.

Tajfel, H., & Turner, J. (1986). The Social Identity Theory of Intergroup Behavior. Psychology of Intergroup Relations, 5, 7-24.

Talabis, M., McPherson, R., Miyamoto, I., & Martin, J. (2014). Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data. Syngress.

Tandon, M. S., Ahmed, O., (2015). LMX And Job Attitudes: Impact On Service Performance. *Journal of International Academic Research for Multidisciplinary, 3(5), 132-153*.

Tari, A. (2011). Z generation. Tericum Könyvkiadó, Budapest.

Taylor, J. B. (2009). The need to return to a monetary framework. Business Economics, 44(2), 63-72.

Taylor, P., & Keeter, S. (2010). Millennials: Confident. Connected. Open to Change. Pew Research Center.

Techopedia, (2018). Information Sharing. Techopedia. Retrieved from: https://www.techopedia.com/definition/24839/information-sharing

Teo, H. H., Wei, K. K., & Benbasat, I. (2003). Predicting intention to adopt interorganizational linkages: An institutional perspective. MIS quarterly, 19-49.

Thangavel, P., Pathak, P., & Chandra, B. (2019). Consumer Decision-making Style of Gen Z: A Generational Cohort Analysis. *Global Business Review*, 0972150919880128.

The Center for Generational Kinetics (2020). Top 10 Generation Z Questions Answered. *The Center for Generational Kinetics.* Retrieved from https://genhq.com/igen-gen-z-generation-z-centennials-info/

Törőcsik, M., Szűcs, K., & Kehl, D. (2014). How generations think: research on generation z. Acta universitatis Sapientiae, communicatio, 1(1), 23-45.

Toronto, E. (2009). Time out of mind: Dissociation in the virtual world. Psychoanalytic Psychology, 26(2), 117-133. doi: 10.1037/a0015485

Turkle, S. (2011). Alone together: Why we expect more from technology and less from each other. *Hachette UK. New York, NY: Basic Books.*

Turner, A. (2015). Generation Z: Technology and social interest. *The journal of individual Psychology*, *71*(2), 103-113.

Turner, A. R. (2013). Generation Z: Technology's Potential Impact in Social Interest of Contemporary Youth. *A Research Paper Presented to The Faculty of the Adler Graduate School*, 1-79.

Twenge, J. (2017), Have Smartphones Destroyed a Generation?. Retrieved from https://www.theatlantic.com/magazine/archive/2017/09/has-the-smartphone-destroyed-a-generation/534198/

Van Dyne, L., & Ang, S. (1998). Organizational citizenship behavior of contingent workers in Singapore. *Academy of Management Journal,* 41, 692–703.

Velasco, H., (2017). Who is Gen Z? How teens are consuming content. *The Drum Digital Summit.* Retrieved from https://www.thedrum.com/news/2017/12/27/who-gen-z-how-teens-are-consuming-content

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MIS quarterly, 157-178.

Vojvodić, K. (2018). Generation Z in brick-and-mortar stores: A review and research propositions. *Business Excellence*, *12*(3), 105-120.

Walker, J. T., Martin, T., White, J., Norwood, A., & Haynie, L. (2006). Generational age differences impact the college classroom. Journal of the Mississippi Academy of Sciences, 51(4), 215-220.

Weber, R. H. (2009). Internet of things–Need for a new legal environment?. Computer law & security review, 25(6), 522-527.

Weiler, A. (2004). Information-seeking behavior in generation Y students: Motivation, critical thinking, and learning theory. The journal of academic librarianship, 31(1), 46-53.

Weinswig, D. (2016). Gen Z: Get ready for the most self-conscious, demanding consumer segment. Fung Global Retail & Technology, 1-19.

Wiedmer, T. (2015). Generations do differ: Best practices in leading traditionalists, boomers, and generations X, Y, and Z. Delta Kappa Gamma Bulletin, 82(1), 51.

Williams, K. C., & Page, R. A. (2011). Marketing to the generations. Journal of Behavioral Studies in Business, 3(1), 37-53.

WP Engine & The CGK (2017). The Future of Digital Experiences: How Gen Z is Changing Everything. Retrieved from https://wpengine.com/wp-content/uploads/2017/12/WPE-EBK-LT-GenZ-AUS_v04.pdf

WP Engine, (2017). WP Engine Study Reveals Generation Z Lives Through Digital Experience. *WP Engine.* Retrieved from: https://wpengine.com/blog/wp-engine-study-reveals-generation-z-lives-digital-experiences/

WP Engine, (2020). Generation Influence: results from the 2020 Gen Z report. *WP Engine.* Retrieved from: https://wpengine.com/gen-z-us/

Xie, E., Teo, H. H., & Wan, W. (2006). Volunteering personal information on the internet: Effects of reputation, privacy notices, and rewards on online consumer behavior. Marketing letters, 17(1), 61-74.

Yang, S., & Wang, K. (2009). The influence of information sensitivity compensation on privacy concern and behavioral intention. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 40(1), 38-51.

Yusoff, A. S. M., Peng, F. S., Abd Razak, F. Z., & Mustafa, W. A. (2019). Discriminant Validity Assessment of Religious Teacher Acceptance: The Use of HTMT Criterion. In Journal of Physics: Conference Series (Vol. 1529, No. 4, p. 042045). IOP Publishing.

Zhang, T. C., Omran, B. A., & Cobanoglu, C. (2017). Generation Y's positive and negative eWOM: use of social media and mobile technology. International Journal of Contemporary Hospitality Management.