A PRIVACY PARADOX:

THE POWER OF TECHNOLOGICAL SURVEILLANCE AND ITS EFFECT ON INFORMATION TECHNOLOGY USAGE BEHAVIOR

EMRE RENÇBEROĞLU

BOĞAZİÇİ UNIVERSITY

2016

A PRIVACY PARADOX:
THE POWER OF TECHNOLOGICAL SURVEILLANCE AND ITS EFFECT ON INFORMATION TECHNOLOGY USAGE BEHAVIOR

Thesis submitted to the

Institute for Graduate Studies in Social Sciences

in partial fulfillment of the requirements for the degree of

Master of Arts

in

Management Information Systems

by

Emre Rençberoğlu

Boğaziçi University

2016

DECLARATION OF ORIGINALITY

I, Emre Rençberoğlu, certify that

- I am the sole author of this thesis and that I have fully acknowledged and documented in my thesis all sources of ideas and words, including digital resources, which have been produced or published by another person or institution;
- this thesis contains no material that has been submitted or accepted for a degree or diploma in any other educational institution;
- this is a true copy of the thesis approved by my advisor and thesis committee at Boğaziçi University, including final revisions required by them.

Signature.....

Date .....07.06.2016.....

ABSTRACT

A Privacy Paradox: The Power of Technological Surveillance

and Its Effect on Information Technology Usage Behavior

Thanks to developing technologies, reaching information has become easier and the big data concept started to be used in various fields. Today, almost all of the technologies which are used widely, such as the internet, mobile phones, computers and smart TVs, are capable of collecting and storing data. The data gathering activity is a routine process for almost all private companies and governments, which can result in incidents of exploitation and misuse. Moreover, some sociological impacts, which include self-censorship and changing perceptions, are considered one of the results of increasing information privacy concerns.

The aim of this thesis is to contribute to the literature by investigating the multidimensionality of information privacy concerns. For this purpose, a survey was conducted with 641 participants to measure the relationship between information privacy concerns with regard to news, regulations, user agreements, public beliefs and perceptions. Additionally, the association between information technology (IT) usage behavior and the dimensions of the information privacy concerns are examined. According to the analysis of survey data, demographic differences are important in terms of privacy concerns. News and regulations are highly associated with privacy concerns, but security perception is only related to the data collection dimension. Another finding of the research is that there is not a significant relationship between the information privacy concerns and IT usage behavior, except general IT tools.

ÖZET

Mahremiyet Paradoksu: Teknolojik Gözetimin Gücü ve Bilgi Teknolojileri Kullanım Davranışı Üzerindeki Etkileri

Gelişen teknolojiler ile birlikte verilere ulaşım olanaklarının artması büyük veri kullanım alanlarını da arttırmıştır. Günümüzde her insanın kullandığı internet, cep telefonu, bilgisayar, akıllı televizyon gibi teknolojik aletlerin hemen hepsi veri toplama ve saklama kabiliyetine sahiptirler. Verinin kötü ve yanlış kullanımı ile sonuçlanabilecek veri toplama aktiviteleri genellikle bütün özel şirketler ve hükümetler için rutin bir uygulamadır. Ayrıca, kendi kendine sansür uygulama ve değişen algılar gibi bazı sosyolojik etkilerin de artan bilgi mahremiyeti endişelerinin sonuçlarından oldukları düşünülmektedir.

Bu tezin amacı bilgi mahremiyeti endişelerini çok boyutlu olarak araştırarak literature katkıda bulunmaktır. Bu amaçla, bilgi mahremiyeti endişelerinin, haberler, yasalar, kullanıcı sözleşmeleri, toplumsal inanış ve algılar gibi öncülleri ile olan ilişkilerini ölçümlemek amacıyla 641 katılımcı ile bir anket çalışması yapılmıştır. Ek olarak, bilgi teknolojileri (BT) kullanım davranışları ve bilgi mahremiyeti endişelerinin boyutları arasındaki bağlantı da incelenmiştir. Anket çalışmasının sonuçlarına demografik farklılıklar bilgi mahemiyeti endişeleri açısından önem taşımaktadır. Haberler ve yasalar, mahremiyet endişeleri ile yüksek oranda alakalıdırlar, ancak güvenlik algısı bilgi mahremiyetinin yalnızca veri toplanması boyutu ile ilişkilidir. Araştırmanın başka bir sonucu olarak da BT kullanım davranışı ve bilgi mahremiyeti endişeleri arasında anlamlı bir ilişki bulunamamıştır.

ACKNOWLEDGMENTS

Firstly, I want to present my thanks to my thesis advisor, Professor Zuhal Tanrıkulu, who encouraged me to work on this subject and motivated me with her visionary thoughts.

Also for their contributions and valuable comments I want to express my thanks to Assoc. Professor Bilgin Metin and Professor Sevinç Gülseçen.

I am also grateful to the Scientific Research Project Office of Boğaziçi University for their contribution to this research.

For certain, the help of Hakan Tunahan and Nilgün Tunahan was substantial during the research. Thus, I express my sincere gratitude to them.

My dear friends, who encouraged me to keep on working and lent a hand to my thesis, it is impossible to mention all of you, but I want you to know how much I appreciate your support.

To the person who stood by me in my rough times, Hatice Nur Akçakaya, I thank you for all your help, without which this work could not have been completed.

Last but not least, my precious family, who gave me the strength that I needed, has a significant share in this study. It is impossible to express my gratitude to you. Thank you for being with me.

To my father…

Festina lente…

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

LITERATURE REVIEW

1.1 Information privacy

In 1890, privacy was defined as "the right to be let alone", making reference to photography devices and newspapers as examples of the constraints on privacy (Warren & Brandeis, 1890). The meaning of privacy has expanded with different aspects of history. The "right to be let alone" phrase still makes sense in the explanation of privacy but it is not as inclusive as it was in 1890. Sociological and ideological alterations in time have paved the way for the development of the privacy notion. In particular, advances in the technology field enabled the true privacy evolution to come faster.

The Oxford Dictionary explains privacy in a similar way to Warren &and Brandeis, that is, as "a state in which one is not observed or disturbed by other people" ("Privacy," n.d.). However, different concepts of privacy have emerged over time, and some of them became more popular among the others. Information privacy is one of them. Clarke defines information privacy as:

> …the claims of individuals that data about themselves should generally not be available to other individuals and organizations, and that, where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. (Clarke, 1999, p. 60)

Bélanger and Crossler (2011) explain information privacy as the request of a person to have authority over their data. In the same article, they also mention increasing concerns about information privacy and the extended concepts of its notion, due to the technological developments. Discussions and conflicts about the information privacy notion currently exist in different research areas. As stated in an

article of Pavlou (2011), information privacy is a subject for law, economics, psychology, management, marketing and information systems together.

As technological developments initiated the information era, the severity of the threats to privacy began to rise, thanks to surveillance technologies and the exploitation of them (Shade, 2002). The media and technology revolutions can be shown as an example of technologies which have brought new habits and chances to communicate. User-generated content, online linked groups of interest, information sharing between the platforms are the features of these new practices (Boyd, 2008).

The progress of the information privacy notion shows a simultaneous path with the technological advances as mentioned above. Smith, Dinev and Xu explain the conceptual background of information privacy from 1945 (see Table 1).

Table 1. Evolution of the Information Privacy Concept

Period	Characteristics
Privacy Baseline 1945-1960	Limited information technology developments, high public trust in government and business sector, and general comfort with the information collection.
First Era of Contemporary Privacy Development 1961-1979	Rise of information privacy as an explicit social, political, and legal issue. Early recognition of potential dark sides of the new technologies (Brenton 1964), formulation of the Fair Information Practices (FIP) Framework and establishing government regulatory mechanisms established such as the Privacy Act of 1974.
Second Era of Privacy Development 1980-1989	Rise of computer and network systems, database capabilities, federal legislation designed to channel the new technologies into FIP, including the Privacy Protection Act of 1984. European nations move to national data protection laws for both the private and public sectors
Third Era of Privacy Development 1990-present	Rise of the Internet, Web 2.0 and the terrorist attack of 9/11/2001 dramatically changed the landscape of information exchange. Reported privacy concerns rose to new highs.

(Smith, Dinev, & Xu, 2011)

New social aspects that are accompanied by the increasing importance of information influence all kinds of daily activity, besides the notion of Warren and Brandeis. To emphasize the importance of information privacy in this respect, a report by UN Global Pulse can be shown. This report claims that privacy is an essential notion of human rights and it is required for democracy. Hence, it has to be protected even if the new technologies rule it out (Letouzé, 2012).

The information privacy concept is based on the collection and surveillance activities by diverse subjects with different methodologies and for various purposes in every step of one's daily life (Buchanan, Paine, Joinson, & Reips, 2007). These aspects of the information privacy notion are categorized and the literature in this regard is presented in the following sections.

1.1.1 Data collection and surveillance

Surveillance is one of the key aspects of the modern world and it profoundly affects daily life. In the course of the developing of technologies, the meaning of surveillance and the methods of it have evolved. Clarke defines "dataveillance" as the integrated organization of surveillance activities with data systems (Clarke, 1988). Another and more enlarged notion of surveillance is called "überveillance", which proposes a surveillance notion that accompany human body in everywhere and comprises all types of collected data from entire surveillance activities in any place or time via different types of technologies (Michael, Fusco, & Michael, 2008). Modern surveillance shows some differences compared to the old surveillance notion. Modern surveillance activities are less visible, do not require consent, are carried out by machines in a continuous real-time activity and the data are collected not only by specialists, while in the past it was more visible, more voluntarily, carried out by humans or animals in a specific period and location and the data were collected only by specialists (Marx, 2002).

In the modern world, there are many usage areas of surveillance technologies. One of them is security. Surveillance for security purposes usually expresses a control mechanism which aims to prevent undesired incidents or predict upcoming

events using the technological devices and statistical methods about future. This operation is possible by watching everything that moves (Bauman & Lyon, 2013). Besides this, research shows that computer-based models can predict personal behavior and seem more successful than friends or family of a person (Youyou, Kosinski, & Stillwell, 2014).

There are some beneficial sides of surveillance applications, as well. Health information from all over the world can be used to watch the route of an infection such as the instance of H1N1. These pandemic surveillance studies contribute to getting a vision about diseases and help to develop a treatment (Brownstein et al., 2010). Observing elderly people with video surveillance systems to catch falls because of health problems is an example of home surveillance application for health purposes (Foroughi, Aski, & Pourreza, 2008). Using GPRS technology, the emission rates of cars can be monitored. Thus, the environment can be protected (Lin et al., 2007). Oil spill sensors can be utilized by petroleum refineries to prevent oil disasters. These oil surveillance systems help to detect spills in the early period and to minimize harm to the nature (Jha, Levy, & Gao, 2008).

Surveillance may also increase life quality and opportunities, but in return, it diminishes privacy (Bennett, 2011). Besides the benefits of surveillance technologies, their applications and potential use areas are contradictive. In the past, personal supervision was applied only to suspected people in certain situations. However, the recent tendency is based on watching and recording every piece of personal information to utilize it in a time of need. To be exposed to the supervision of this strategic surveillance, individuals do not require to be suspected or guilty (Assange, Appelbaum, Müller-Maguhn, & Zimmermann, 2012).

Richards (2013) explains the harms of surveillance using two categories:

- Intellectual surveillance: Being under surveillance can cause people to keep themselves from creating new ideas and activities, and for that reason, it results in the lack of intellectual freedom in the society. Dictatorial governments have exploited this fact to suppress creativity and prevent menacing ideas for the future of the regime. The situation of being watched causes the person to question himself and emerges initiates a self-censorship movement in the society, which helps to create an adequate environment to rule the society easily by the oppressive regimes. A more detailed discussion on this subject was written by Foucault, known as *Discipline and Punish: The Birth of the Prison*, in 1977 (Foucault, 1977).

- Surveillance and power: In addition to intellectual surveillance, some harms of surveillance can be based on exogenous factors. To explain these factors, the watcher and the watched metaphor can be shown as an instance. The activity of surveillance causes an information asymmetry between the watcher and the watched. The watcher always has more information, compared to the watched. This asymmetry gives power to the watcher, who can be a company, a government agency or a third person, depending on the situation. This power of the watcher can be used for the purpose of blackmail, discrimination and persuasion.

According to the taxonomy of Solove (2008) the threats to information privacy are listed in four items:

- Information collection
- Information processing
- Information dissemination
- Invasion

These four groups have their subgroups as it is shown in the following taxonomy schema (see Fig. 1).

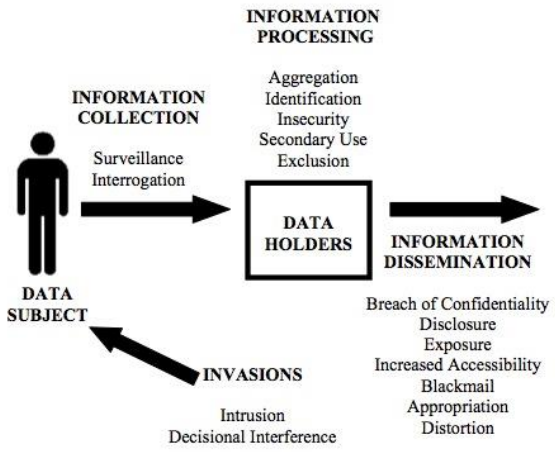

Fig. 1 Taxonomy of information privacy (Solove, 2008)

In the scheme of Solove, data gathering activities are represented by the Information collection group. This group contains all kinds of monitoring, watching and listening activities by governments or others. The next group, which is called Information processing, includes storing of data and exploiting activities. The third group in the schema is Information dissemination. This group lists activities related to distribution, revelation and transferring of the collected data to others. The last

group, Information dissemination, involves the possible dangers related to abuse of private information (Solove, 2008).

Also, Solove states that some people who think that they have nothing to hide argue that concerns about surveillance are redundant, but Solove points out that privacy is not so simple to define. According to him, surveillance prevents people from behaving freely and this thought supports the intellectual freedom idea of Richards. Moreover, Solove thinks that surveillance can create a power asymmetry between the person and the government and it can be used for political purposes (Solove, 2007).

1.1.1.1 Companies

In the modern business world, privacy became important by means of the critical role of information gathered from customers. Perri 6 calls consumer information the economic fuel of today and according to him, it is becoming the primary resource of the economy. Consumers' situations, attributes, choices, movements are the key factors for staying in a competitive market (6, 2006).

A study emphasizes the importance of data-driven decision making in the business field as explaining the relationship between data-driven decision-making activities and higher productivity (Brynjolfsson, Hitt, & Kim, 2011). The results show the indispensable value of the big data management for business. In addition, as mentioned in the McKinsey Global Institute report, big data has started a new information era, affecting all companies, management and governance principles. This report lists some of the main business changes that accompanied the big data revolution. The increase of the access of companies to information has caused

innovations in the fields such as supply chain management, manufacturing, operation, etc., thanks to the availability of data. To make decisions in the business sector, analysis is an important aspect for organizations. Having the adequate data to make the right decision is critical for every business. Besides, a system that enables one to access the customers' in real-time increases the importance of customer relationship management (CRM) and marketing, in addition to the fact that it also contributes to productivity (Brown, Chui, & Manyika, 2011).

Companies need the data of their customers to provide a better service in a market with high competition. Strategies, such as personalization, which is a popular way to acquire new consumers and gratify them, are required to collect the consumers' data. On the other hand, customers are willing to provide information without regarding privacy if the advantages of the personalized service satisfy them (Awad & Krishnan, 2006; McAfee & Brynjolfsson, 2012). Consumers assume that they will benefit from sharing their personal information when it is asked. Thus, they usually do not question the information demand of companies (Bauman & Lyon, 2013). Amazon realizes your purchase behavior, Spotify gets your music choice, Uber predicts your location, and Tinder thinks you are searching for a relationship in a short term. In common, all these companies aim to forecast one's personal daily life and the next move, inferred by the traces of the user (Maney, 2015). With all these traces left, keeping a diary is simpler than in the old times, says Garfinkel (2001). Every data entry of a daily life is stored in modern database systems even without of the awareness of an individual most of the time.

However, Ohm (2013) states that big data processes, the whole operation of a huge amount of integrated data, should be analyzed in terms of privacy and the outcomes for the society. Besides the benefits of the big data, the risks should also be

considered. In his article, Ohm gives the example of medical companies that demand the consent to use people's information, asserting the advantages of it. According to Tene and Polonetsky (2012), when benefits of analyzing data seem superior to privacy concerns, the legality is not questioned by the companies, even if there is no permission by the users.

Services such as Gmail and Google Docs help people in a wide range of tasks, and as a part of this help, they keep the users' information in the company's storages and monetize it, using it for commercial purposes. Also, in most of these cases, users are not aware that their data are being gathered. Sometimes this gathering is entirely transparent to the users; however, not all of the steps of the information gathering process are explicit (Andrejevic, 2007).

It is mentioned by experts that companies have a chance to gather more data than government agencies via technologies such as social media, smartphones, laptops, tablets, e-mail, online banking services, etc. The information sharing habit of people has a significant role in collecting information through these channels (Verble, 2014).

1.1.1.2 Government surveillance

In East Germany, the Ministry for State Security, known by the name STASI (Staatssicherheit), was the secret police service organization, infamous for its violent and authoritarian methodologies. It monitored and collected the information of the German citizens from 1957 to 1989, in order to protect the authority of the government. The motto of the organization was the "shield and sword of the Party",

clarifying the totalitarian purpose of STASI. The methods of the organization varied from eavesdropping to violent methods such as kidnapping (BStU, n.d.).

With the developing technologies, surveillance methodologies like those used in East Germany changed. As an instance, documents of Edward Snowden, an American informer, revealed that the NSA's (National Security Agency) PRISM project allows government agencies to reach the database of high technology companies such as Yahoo, Google and Facebook when it is demanded. As a consequence of this revelation, US technology companies, which have cloud services globally, felt apprehension of losing users from other countries (Landau, 2013). According to the leaked reports, one of the goals of the NSA program is also to gather information through fiber-optic internet cables under the sea. Moreover, the reports show that other intelligence services, such as UK's GCHQ, are using similar methods with the NSA. These reports indicate the collaboration of different intelligence services to reach the global information in the entire internet. Some researchers argue that national services are not restricted by their nation in regard to these reports; they work globally through the big data, which is gathered thanks to digitization (Bauman et al., 2014).

A chart published by *The Guardian* points out the information providers to the NSA and the types of data they have provided (see Fig. 2).

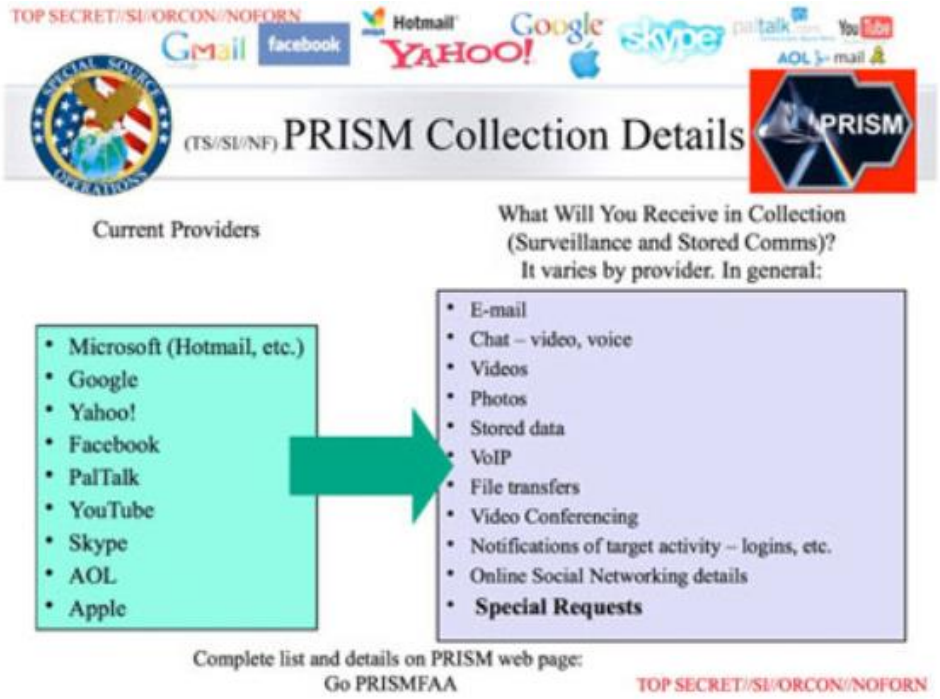

Fig. 2 Information providers to the NSA (Greenwald & MacAskill, 2013)

In the progress of time, the internet has become the weapon of modern governments, especially authoritarian regimes. Police services, censorships and propaganda operations are associated with the modern technological methodologies of governments. Modern governments watch every move of the citizens, track all information and keep that information in order to use it against dissidents, criminals, suspects, etc. In addition to the help of technology companies, governments have their ways to gather information. Some initiatives of governments for this purpose are directing the citizens to use e-mail services provided by the government. For the same reason, some governments work on creating a national search engine website and a national social network website (Morozov, 2011).

In most cases, the monitoring and watching actions of the governments expand on the grounds of national security reasons (Wolf, 2012). One of the reasons for increasing the power of government agencies are the security protocols that have

been made after the 9/11 attacks. Facilitated by the developing technologies, the NSA and other intelligence agencies became more powerful and influential in this period (Verble, 2014). The FBI uses surveillance software which enables it to access webcams, e-mails, files and the location of the PC, to watch the suspects (Timberg, 2013). Britain's intelligence service GCHQ tracks the webcam capture of online users as it is explained in the revealed NSA documents. Although the intelligence service argues this is completely proper and legal, according to the documents, explicit materials can be gathered in the webcam tracking process. In addition, the face recognition systems are also exploited in this process (Ackerman & Ball, 2014).

The reports of Snowden show the collaboration of the government agencies and technology companies, as well. Intelligence services regularly demand personal user data from technology and telecommunication companies. This close relationship, which was leaked with Snowden's files, between government and technology companies, damaged the technology business of the Silicon Valley companies, due to the perceived image that these companies secretly share their data. Compared to the time before the leakage, customers are more curious about where their data are stored and how they are used, and some of these customers are other governments such as Brazil. The companies including Microsoft and IBM are trying to restore their old reputation by spending billions of US dollars (Miller, 2014).

Despite this, in some cases, technologies generated by private companies can be shared with the government, as the example of the face recognition technology by Disney (Wolf, 2012).

1.1.2 Mobile phones

Recent versions of mobile phones include sensors such as gyroscope, GPS, microphone and camera as standard and these sensors are used by different kinds of applications. In addition, these applications collect the sensor data and use it to increase the scope of the service. For instance, personalized services are one of the fields that can be attained through the combination of different sensor data. These personalized services can also be used to affect the person's behavior by the way of services such as through targeted advertising (Lane et al., 2010).

On the other hand, modern mobile phones enable service providers and also the third parties to monitor the user. Research indicates that the location of iPhones can be watched and monitored with a feature inside the operating system, whether the user accepts it or not (Arthur, 2011). Moreover, a newspaper article explains some of the public surveillance methods of the NSA; eavesdropping on mobile phones and data collection from computers even when they are offline are some examples of them (CBS/AP, 2013).

A report of *The Guardian* states that databases of Verizon, one of the biggest SIM card producers, are tracked by the federal agencies and all of the phone calls are collected by the government (Greenwald, 2013). In addition, as stated by Griffin (2015), the user database of Gemalto, one of the biggest SIM card producers, has been stolen by the US and British intelligence agencies (NSA and GCHQ). Gemalto produces two billion SIM cards per year for 450 companies around the world. The report says that the takeover happened through the encryption keys of the SIM cards while the company was unaware of that. This case is the indication that such a huge

interception is possible with appropriate technology. Gemalto is also one of the SIM card producers for Turkish mobile phone service providers (Can, 2015).

According to another report, mobile phone applications using sensors to gather data work with private information of users and therefore they need to secure privacy and anonymity (Kapadia, Kotz, & Triandopoulos, 2009). Research states that most Android mobile phone users are unaware of which permissions the applications are demanding and only 17% of the research's participants are careful about the permissions they give to the application in the installing process (Felt, Ha, Egelman, & Haney, 2012).

Uber, a mobile phone application which enables one to call a taxi is accused of the exploitation of their data to suppress the media. The company's executive confessed they organized a team for this purpose, aiming to reach personal information of media workers. Moreover, the article states that the activities of government agencies are more visible than those of companies; on the other hand, big technology companies have a chance to get the information which people are reluctant to share (Foxton, 2014). Users are concerned about their privacy while using location-based services, like these applications, because of the scrutiny threat of the service providers. Users are not able to confirm the consequences of their data sharing after they are collected by location-based services and whether it results in a privacy problem (Barkhuus, 2004).

1.1.3 The internet and social media

Boyd and Ellison (2007) describe social network sites as:

> …web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. (p. 211)

Recent online platforms such as social media websites have the features to collect, save and analyze personal data of their users. Additionally, these features make it possible to predict the habits of the users and enable the marketing usage of the personal data (Fuchs, 2011). Privacy settings have a major role in controlling the information sharing; however, most of the time Facebook users have a problem adjusting privacy preferences and this results in a mismatch between the desired and performed privacy settings (Liu, Gummadi, & Mislove, 2011).

People who aim to meet new friends make their privacy settings on social network sites more tolerating (Joinson, 2008). A study among Facebook users shows that the users who aim to become popular are more likely to disclose their information (Christofides, Muise, & Desmarais, 2009). Some experts argue that in social media, the pleasure of getting attention makes one gloss over the fear of disclosure (Bauman & Lyon, 2013). In addition, location sharing applications, which are used especially among the young generation to indicate their current location, usually do not cause privacy concerns (Lindqvist, Cranshaw, Wiese, Hong, & Zimmerman, 2011).

On the other side, the CEO of Facebook, Mark Zuckerberg thinks privacy is not a social norm any more. He says the new social media altered the habits of the users and make them generous in publishing their information online (Johnson, 2010).

There are some services of Facebook that have been questioned regarding the privacy aspect of the users. As an example, a study states that the 'like' button gadget of Facebook on other websites provides the information of the web users to Facebook, even if they are not a user of Facebook (Roosendaal, 2011). For example, this 'like' button provides the company with a chance to follow the users' moves while browsing other websites on the web. This activity gives Facebook an opportunity to uncover the thoughts, political and religious opinions, physical and mental conditions of the users (Efrati, 2011). As another example, the relationship between social media websites and governments is a subject that always raises curiosity. A remarkable security note was released by Facebook regarding this on 16 October 2015, which says Facebook will notify the users when an attempt to monitor the user's account by a government is spotted. This means users of Facebook will be informed and requested to be careful with a message (see Fig. 3).

Fig. 3 Privacy warning message on Facebook (Stamos, 2015)

It is not surprising to associate social media with political tools. Most people think social media has a big potential to create collaboration and political association in the society like the Occupy movements; however, some researchers state that social media's presence enables the tracking of the users and gathering of their information. Due to this surveillance power of social media, its numerous potentials are also restricted (Bauman & Lyon, 2013).

A research shows that information sharing behavior of a person in a virtual community is related to the trust level for the service provider (Hsu, Ju, Yen, & Chang, 2007). Another research asserts that users of Facebook are concerned that their information may be gathered for malicious intentions without their awareness or approval (Young & Quan-Haase, 2009).

1.1.4 Smart devices and technological data collection

It is not only mobile phones and the internet that are data collection tools, but also other instruments such as smart devices are commonly used to collect information in every step of life. According to an article in *Consumer Reports*, these devices have capabilities to connect to the internet and send data to each other or a server to be stored. Due to their capability of connection, the system created by these devices is called the "internet of things". Some examples of smart devices are refrigerators, TVs, thermostats, toys, coffeemakers, door locks, etc. These devices can send their information to a server generally without the awareness of the users. Production of data by smart devices is increasing in time. For example, the count of wearable smart devices was 109 million by the end of 2014 and the data produced monthly by these devices are equal to millions of gigabytes thanks to their built-in sensors ("In the

Privacy of Your Own Home," 2015). A research claims that everyday life activities of a person such as transportation, visited locations, daily routines and other ordinary actions can be procured by the GPS data with a high accuracy (Liao, Fox, & Kautz, 2007).

Smart electricity consumption metering devices are common in households and a study shows that these devices collect detailed consumption patterns, which gives a chance to find out the population of the house, living routines, etc., of the householders (Molina-Markham, Shenoy, Fu, Cecchet, & Irwin, 2010). Moreover, another research points out that with the help of smart meters, TV watching habits and the model of the TV in a household can be determined (Greveler, Justus, & Loehr, 2012).

According to the privacy policy of Samsung, smart TVs can capture the voice of the users and provide this information to third party companies, and without encryption, these TVs can easily be used as an eavesdropping tool (Harris, 2015). On the other hand, when using face recognition systems embedded in smart TVs, watching TV can be more personalized in return for sharing more personal data (Lee, Sohn, Kim, Kim, & Kim, 2012).

As another example of widely used tracking technologies, RFID can be shown. RFID means radio frequency identification and it refers a technology which is used to recognize automatically things or humans with the help of wireless data carried by microchips. There are lots of application instances of RFID in daily life such as the examples in retail shopping markets, libraries, passports, etc. On the other hand, this technology reveals the concern for surveillance. Moreover, privacy concerns rise when the RFID tags are used with personal information as in the example of RFID-enabled loyalty cards of shopping markets (Juels, 2006). Hoven

and Vermaas (2007) point out that nanotechnology and RFID will make all items a possible data carrier and everything can become traceable through this technology in the future.

1.2 Information privacy concerns

As stated in an article, information is a thing that can be gathered, collected, analyzed and traded by governments, companies and agencies, usually without permission or awareness of the owner. In every step of life, using online and offline technologies makes it possible to collect and interpret information about a person's actions and moves, which results in concerns about personal information (Buchanan et al., 2007). Technological revolutions, such as computers, smart phones, etc., boosted fears of the society about privacy, but whereas researches point out information privacy concerns are common among the society, people are still likely to share their information online (Solove, 2008). On the other hand, a study argues that public privacy concerns showed a decreasing trend from 1996 to 2006. In this study, it is asserted that the increasing familiarity of people with the new technologies and decreasing anticipation in terms of privacy are the two main reasons for this change (Anthony, Stablein, & Carian, 2015).

The increasing use of technology in all areas makes it easy to gather information for companies. For an example, according to Gmail's policy, even after you erase your e-mails from your Gmail accounts, Google has the right to keep them on its offline servers (Andrejevic, 2007). Services such as personalization allow tech companies like Amazon and Google to analyze consumer data and to make forecasts

in regard to the users. With the increasing precision of these forecasting services, privacy concerns of users rise (Toch, Wang, & Cranor, 2012).

According to a report by McAfee (2014), personal information of 40 million people in the US has been stolen in 2013, while 54 million in Turkey, 20 million in Korea, 16 million in Germany and more than 20 million people in China experienced personal information theft in the year 2013. In light of these numbers, a research conducted among Facebook users about privacy concerns points out identity theft is the most prominent fear; furthermore, accessing of personal data by others is another common concern. The same article groups the concerns of social media users into five categories: financial, digital world, physical world, mate-attitudes and general fears, where financial and digital world concerns have a higher share than others (see Table 2).

Table 2. Privacy Concerns Associated with Specific Consequences

	Main Privacy Concern	Potential Negative Consequences
Financial		
Identity Theft	40%	35%
Financial Loss	11%	23%
TOTAL	51%	58%
Digital World		
Access to Personal Data	14%	8%
Account Hacking	11%	3%
Misuse of Personal Data	5%	2%
Unwanted Solicitations/Spam	3%	6%
Social Ramifications	3%	3%
Computer Virus	2%	2%
Unwanted As Targeting	1%	2%
TOTAL	42%	26%
Physical World		
Offline Threats	6%	5%
Harm to Family	2%	2%
Stalkers	1%	3%
Employment Risks	0.3%	2%
Hassle to Recover	0%	4%
TOTAL	9%	15%

(Staddon, Huffaker, Brown, & Sedley, 2012)

Pötzsch (2008) explains the advantages and disadvantages of online information sharing using two categories: e-commerce and Web communities. The listed costs of disclosure by Pötzsch point out the third party privacy threats in general (see Table 3).

Table 3. Advantages and Disadvantages of Online Information Sharing

	Benefits	Costs
e-Commerce	-Convenience -Automated processes -Price premiums -Selected information	-Price discrimination -Marketing spam -Identity theft
Web Communities	-Social exchange -Relationships -Collaborations -Reputation	-Identity theft -Marketing spam -Stalking, Kidnapping -Negative reputation in other contexts

(Pötzsch, 2008)

The report of the Pew Research Center shows that Americans do not feel very confident about the privacy and security of their information collected by companies and government agencies (Madden, Rainie, Perrin, Duggan, & Page, 2015). The Pew report states that only 6% of people feel very confident about the privacy of their records at government agencies, while the confidence level changes to 5% for cell phone companies, 2% for search engine providers and 1% for social media websites (see Fig. 4).

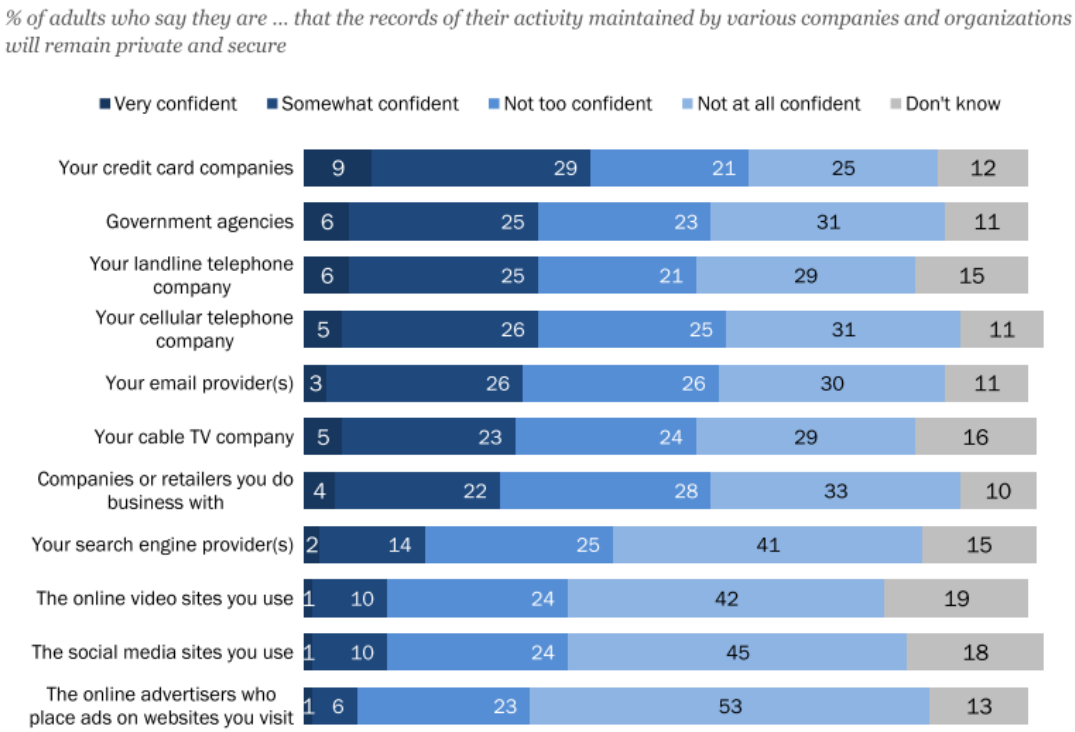

Fig. 4 Information privacy confidence rates (Madden et al., 2015)

1.2.1 Dimensions of information privacy concerns

A research by Milberg, Smith, Burke and Hall (1996) specifies four subgroups of information privacy concerns:

- Collection: Concern for collecting mass amounts of personal data in databases.
- Unauthorized Secondary Use: Concern for using the collected data for reasons other than the purpose they were collected for.
- Improper Access: Concern for the accessing of personal data by people without permission.
- Errors: Concern for insufficiency to prevent unintended errors in personal data.

The model prepared by Milberg and Smith is called CFIP – Concern For Information Privacy –.

After the CFIP model, various models are asserted related to this topic. One of them is the IUIPC –Internet Users' Information Privacy Concerns– model. The IUIPC model lists the dimensions affecting information privacy concerns using three subgroups that are different from the CFIP model: collection, control and awareness of privacy practices (Malhotra, Kim, Agarwal, Tech, & Peachtree, 2004).

Hong and Thong's (2013) conceptualization work about online privacy concerns classify the concern dimensions, which were mentioned in the literature mostly, into six groups: collection, secondary usage, errors, improper access, control, awareness.

As stated in an article, people are likely to demand assurance about the correctness of their collected data. The probability of making a mistake causes anxiety among them. Moreover, the loss of control over the data and the obscurity on the usage of the data are the other reasons for the anxiety. People desire to keep their control over the data after they share it and in case needed, they want to have a right to remove or change their information. Similarly, the darkness on the usage areas of the stored information is another undesired situation and hence it causes fear among users (6, 2006).

In addition, a study conducted among IT specialists asserts that users demand that online service providers protect their private information and avoid unauthorized reveals (Martin, Rice, & Martin, 2015).

Regarding the fears in the society, some legislative processes have been conducted, as well. For example, by the decision of the European Court of Justice in 2014, users gained the right to demand to remove data from a search engine. After

this decision, in the first five months, Google got 180,000 remove requests and accepted 40% of them. However, it is argued by Newman that this right is only a part of the information privacy structure, which consists of data gathering, how the gathered data are used, processed and stored, etc. (Newman, 2015).

According to a report from the Pew Research Center, the American society is concerned about their privacy and Americans think that they are under surveillance in every aspect of public life: 93% of Americans say that being in control of who can reach the information about them is critical and 90% of them think the same for being in control of what information about them is gathered (see Fig. 5).

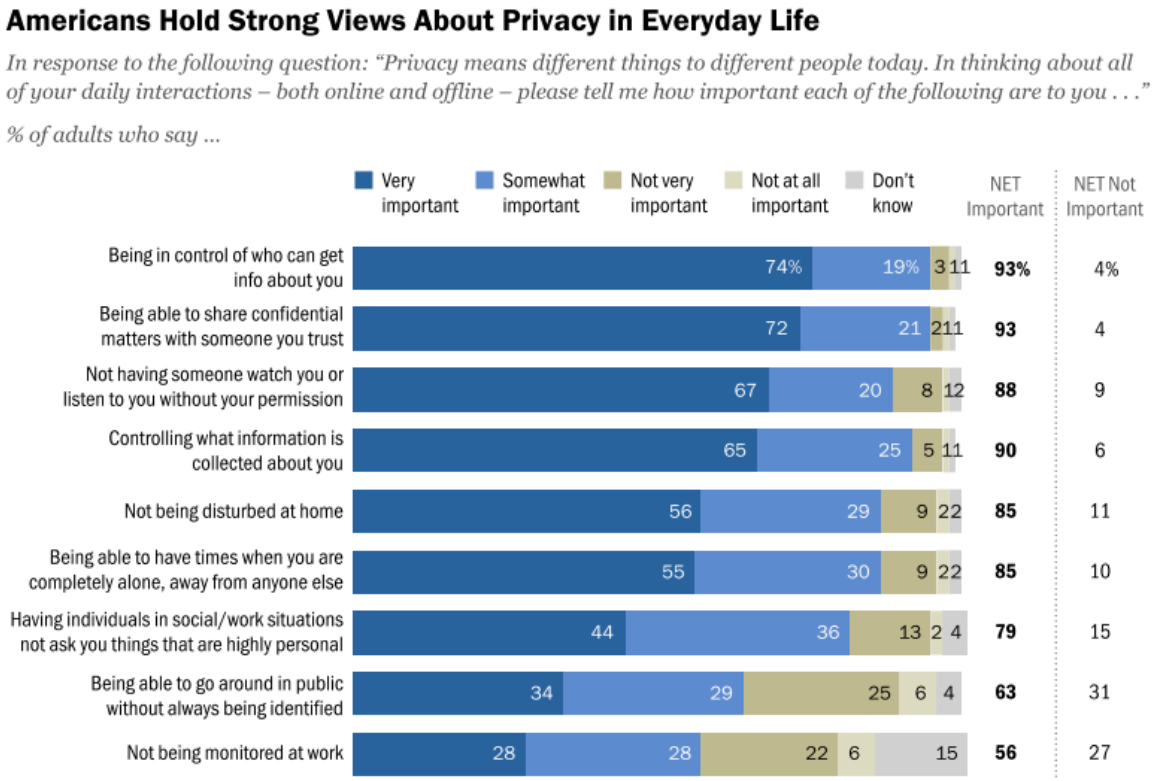

Fig. 5 Information privacy perception survey (Madden et al., 2015)

A study by Turow, Hennessy and Draper (2015) states that 55% of Americans refuse to give permission for using their information in return of a better service and

71% are reluctant to use free of charge Wi-Fi services if the company can monitor their activity. In addition, 84% of Americans desire to have control over their information being perceived by marketers, while 65% of them think that they have limited control over their information collected by the marketers (see Fig. 6).

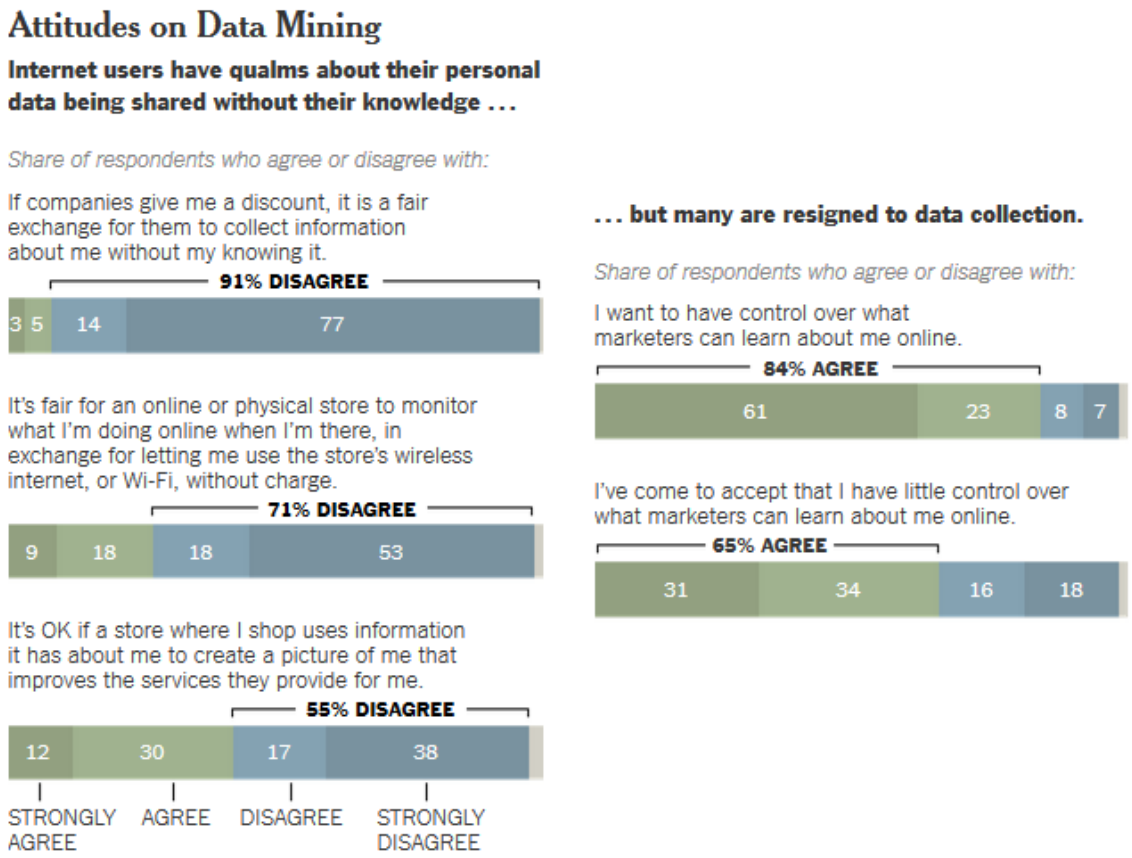

Fig. 6 Attitudes of the users about data mining (Singer, 2015)

1.2.2 Antecedents of privacy concerns

According to the literature research, antecedents of information privacy concerns are grouped into the four items:

- Demographic Differences
- News
- Regulations and Agreements
- Beliefs and Perceptions

1.2.2.1 Demographic Differences

Several studies indicate that demographic differences among people have an effect on the privacy concern level. These demographic differences can be seen in groups depending on internet literacy, gender, education level, socio-economic status and age.

- Internet Literacy: Internet literacy stands for the familiarity of the user with the internet and the usage intensity degree. Studies in the literature mention internet literacy in regard to information privacy. The people who use the internet less than others are more likely to be concerned about potential dangers of the internet. Additionally, they rely less on the internet and seem more distrustful of information and activities online (Dutton & Shepherd, 2006).

- Gender: Males and females may have divergent reactions in the matter of information privacy concerns. Studies point out that women are more concerned about their online privacy and as a result of that they are less generous to share their information than men (Fogel & Nehmad, 2009; Wills & Zeljkovic, 2011).

- Education Level: Education level is another demographic difference that is considered an attribute associated with the information concern level. According to a research, education level affects the level of online privacy concern, where higher educated people are more concerned than lower educated ones, according to a study (Sheehan, 2002).

- Socio-Economic Status: Socio-economic status stands for income level and the living standard of the individual. Groups with different socio-economic status levels also have a varied perception about information privacy. A study asserts that socio-economic status might have an impact on privacy concern of a person (Yao, Rice, & Wallis, 2007).

- Age: Age is another demographic attribute which is mentioned in the literature in terms of information privacy concerns. From young individuals to older ones the concern levels can be considered varied; however, according to a study, there is no significant difference between different generations regarding information privacy concerns (Regan, Fitzgerald, & Balint, 2013).

As seen in the literature review phase, people who have different demographic attributes can also have different attitudes in terms of their information privacy concerns.

1.2.2.2 News

According to the article by Slovic (1987), media have an impact on the society's risk perception of technologies. This argument can be supported by the example of the sale rates of Orwell's dystopian novel *1984*. After the leak of the NSA's intelligence documents, the sale of George Orwell's novel *1984* showed a rapid rise up to 10,000 percent in the sale list of Amazon. This incident can be a demonstration that readers associate the activities of government intelligence services with Orwell's novel, which describes a totalitarian regime with strong surveillance executions (Gold, 2013). The Big Brother phenomenon of George Orwell is usually interpreted as the association between technology and personal freedom regarding information privacy aspects. The term "Big Brother" represents a dictatorial government which disrupts individual independence and liberty of the citizens using the technological surveillance power in the novel (Palen & Dourish, 2003).

Contrary to the traditional thoughts, Moynihan argues that in a dystopian state such as the one described in the book *1984*, this kind of books could not be sold freely and the scandals of surveillance leaks could not be published by the media. He thinks surveillance scandals are not enough to say that we live in a dystopian world but in a flawed system (Moynihan, 2013).

In some cases, mass media are used by the government to create a risk perception and convince the society of the need for public surveillance for reasons of security. Monahan (2010) argues that insecurity of individuals in all aspect of

modern life, such as criminality, livelihood, health, make them more likely to accept the laws, security applications and technological surveillance. The potential perceived risk of criminals, terrorists, immigrants and others make people cede their privacy willingly to protect themselves. In addition, Monahan states that the worry about security is worked up by politicians with the support of mass media to manage the society.

On the other hand, Wikimedia Group accused the NSA of violating individual privacy and they brought their claim to the US court. They argue that people are concerned about their privacy after the NSA's mass surveillance activities were revealed by Edward Snowden and therefore people became more hesitant to share their information (Ingram, 2015).

1.2.2.3 Regulations and agreements

A survey shows the impact of regulations and policies on people's information privacy concerns. According to this survey, regulations and agreements are essential to decrease the privacy concerns (Wirtz, Lwin, & Williams, 2007).

As stated in an article by Werner, Brown, and Altman (2004), modern life with its technological devices and new ways of communication makes privacy regulations mandatory, and they recommend some steps for the future:

> 1 - People should have reasonable control over others' access to them and people's access to others.
> 2 - People may need a new or enhanced repertoire of regulatory mechanisms to control openness and closedness during the technological era.
> 3 - A dynamic privacy regulation system, with the ability to shift desired openness and closedness as circumstances change, will continue to be necessary and may require innovative applications of technology.
> 4 - Awareness of the importance of privacy regulation must be at the forefront of technological innovations. (p. 109)

Besides regulations, user agreements are important for information privacy, as well. Privacy agreements contribute to the protection of sensitive data. For example, policies may necessitate removal of accidentally gathered private data after an analysis (King, 2011). According to Fisher and Monahan (2008), a surveillance application in a hospital to organize inventory, patients and personnel make the workers feel always being tracked and stressed. Researchers suggest preventing this situation by using policies that indicate how and when the gathered data will be used.

People who read privacy agreements are more likely to decline to give their information to a website than people who do not read them. In addition, asking to erase their information and demanding protection of information are more common among the policy readers (Milne & Culnan, 2004).

Both policies and regulations are needed to organize and control information sharing by devices. However, it is argued that the evolution of technology is faster than laws and this makes it harder to regulate ("In the Privacy of Your Own Home," 2015).

The effort to regulate information privacy protection is seen in many countries as technology continues to develop. However, the complexity and the wide scope of the subject make it harder to regulate. Incidents like terrorist attacks have an increased effect on the anxiety in the society and it is an obstacle for the regulation studies of privacy (Raab, 2006). On the other hand, sometimes regulations can have an increased effect on the concerns as in the case of the EU courts, as well. European Union courts demanded from phone and internet companies to keep their consumer data for a period in order to receive information when needed for security purposes, but experts argue that this execution is inconvenient with regard to privacy (White, 2014).

1.2.2.4 Beliefs and perceptions

There are different opinions about privacy in the society and it makes it harder to prepare a commonly agreed-upon regulation (Stalder, 2002). As mentioned in section 1.2.2.2 of this thesis, the perceived need for public security is one of the factors that make the society consent to the loss of information privacy.

Räty (2010) argues that incidents such as terrorist assaults increase the demand for protection of people. This demand causes the government to raise security precautions and surveillance systems have a big role in these precautions. According to the researcher, governments and companies work hard on smart surveillance systems, data analysis programs, location determination systems, etc. In the same article, it is also stated that the primary goal of these technologies, which contain video surveillance, audio surveillance and sensors systems, is to determine criminal cases before they happened through real-time monitoring.

Predicting and forecasting future events is one of the prerequisites to prevent crime. This requires one to gather information and use it (Haggerty, Wilson, & Smith, 2011). Therefore, the perceived need for government surveillance affects information concern of the people who think it is mandatory for security. A research indicates that government surveillance aiming to provide the security usually does not trigger information privacy concerns among people because of the thought that the government needs to reach and collect the information of citizens to maintain public order and minimize security risks (Dinev, Hart, & Mullen, 2008).

In addition, poor technological experience of users is another factor affecting the opinion and the level of information privacy concerns. Getting an indecent and

insulting e-mail is the most common adverse internet experience, followed by computer viruses and fraud attempts, as stated by Dutton and Shepherd (2006)(see Fig. 6).

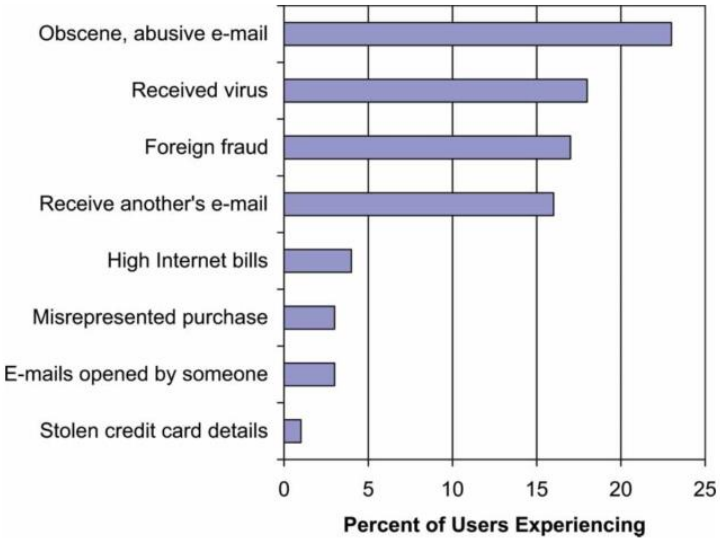

Fig. 7 Adverse internet experiences of users (Dutton & Shepherd, 2006)

1.3 Information privacy and effects on usage of technology

If users have a perception of low privacy, it results in the loss of willingness to use the online service (Featherman, Miyazaki, & Sprott, 2010). Consumers care highly about the consequences of the sharing their information with companies and most of them want to have more control over their information. They want to know how companies manage these data. Moreover, it affects their purchasing intention and privacy concerns (Phelps, Nowak, & Ferrell, 2000). A study shows that information privacy concerns of Facebook users result in the decrease of information disclosing. Moreover, people who have a high level of privacy concern are more likely to

remove their tags on the photos or remove photographs completely and confine their profile to visits by specific groups (Young & Quan-Haase, 2009).

However, marketing activities are one of the important factors that affect the privacy perception. According to a study, marketing campaign offers have an influence on privacy decisions of users, even if the benefit level of the campaigns is low (Acquisti & Grossklags, 2005).

As another factor, privacy and government intrusion concerns are influencing online shopping behaviors and the thought of the users negatively that their activity is watched and the information is gathered increases the concerns and reduces the e-commerce rate (Dinev et al., 2006). Similarly, high risk perception influences user's information disclose rate negatively and if the interest level of the information with the purpose of the collection is low, the tendency of the user to share information decreases (Zimmer, Arsal, Al-Marzouq, & Grover, 2010). According to a research, people are likely to choose to shop in websites where the privacy rules are strict and they feel more comfortable when they share information with these websites (Castañeda & Montoro, 2007). For example, users of location-based services consider three points before sharing their information: which demands, why it is demanded and what detail of information it demands. These aspects have a big role on the user's determination process of the location sharing (Consolvo et al., 2005).

Referring to government applications, a citizen's intentions of using e-government services are dependent on the trustworthiness perception by the users. If they do not trust the government or the internet, they tend not to use e-government services (Carter & Bélanger, 2005; Welch, Hinnant, & Moon, 2005).

In addition to government services, collaborations of private companies with the government services might have an effect on the IT usage intensions of

individuals, especially after the leaked reports of the government agencies. The companies which are mentioned in these reports are now working to gain the trust of their customers and prove that information privacy is an important aspect for them.

On the contrary, Best (2010) argues that although worrying about being monitored can bring to mind the idea of stopping to use information technologies, it is impractical because of the fact that most technologies are adopted in everyday life as a fundamental component.

CHAPTER 2

THEORETICAL FRAMEWORK

This study aims to measure the relationship between information privacy concerns in the society and technology usage attitudes. To present antecedents of privacy concerns is another purpose in the scope of this study.

Subsequent to the literature review, previous researches on this topic and the theoretical models used in this research have been investigated. Additionally, the hypotheses tested in the past studies have been examined. As seen in the literature review section, information privacy is a subject whose scope expands continuously with the developing technologies. These expansions create new research areas related to information privacy concerns. The relationship between such concerns and technological usage habit is one of the main topics that attract interest.

Technological habits take part in every person's life, in every place or work. In other words, modern life partly obliges the individual to use technology to maintain his or her life. However, usage attitudes show variety among people and with their increasing importance, privacy concerns should be considered while researching this subject. Although numerous works have been published on privacy concerns, an in-depth study that examines the relationship between different dimensions of information privacy concerns and technology usage habits lacks in the literature.

Additionally, to understand the antecedents of information privacy concerns is another aim of this study. Examining some notions such as security beliefs, media and privacy agreements and their relationship with privacy concerns can help one understand the antecedents. Likewise, variations in different demographic groups

regarding information privacy concerns are another topic that must be investigated. Considering these facts, these arguments are included in the theoretical framework as the antecedents of the concerns. Furthermore, the dimensions of the concerns are examined differently and due to this reason, the relationships are discussed in 16 different hypotheses for the antecedents.

Antecedents that have an effect on information concerns are specified after reviewing the literature. In total, 15 items are determined as the antecedents and they are classified into four different groups. These are demographic differences, beliefs and perceptions, regulations and agreements, news.

The first antecedent of information privacy concerns is demographic differences. The effect of demographic differences on information privacy concerns of people has been seen in the literature review phase. Variables such as age, income level, education level, gender, internet literacy and virtual attack experience are the items of the demographic differences antecedent.

The second antecedent of information privacy concerns is beliefs and perceptions. As seen in the literature review part, beliefs and perceptions of the society help to form public concerns. Hence, they have a role in information privacy concerns in the society. The belief in the requirement for public surveillance and perceptions about the regime has an effect on public concerns. Considering security reasons and the rules of the social order, people can renounce their privacy. The items in beliefs and perceptions are security need, surveillance for crime rate decrease and surveillance for public order.

Regulations and agreements can be counted as the third antecedent. Government regulations and personal agreements are considered as a factor associated with public information privacy concern. IT agreement literacy, IT

agreements for information security, regulations for information security, censorship regulations, privacy-protective regulations are the items in regulations and agreements.

The fourth and the last antecedent of information privacy concerns in this study is news. News is the main channel for the public to get information about information privacy cases. Sometimes these news reports can create reactions and affect the concern levels. The items of the news antecedent are privacy news interest, information privacy news interest, exploring news about privacy.

To measure the relationship between the privacy concern antecedents, which are mentioned above, and information privacy concerns of a person is one of the purposes of this study. To measure this relationship deeply, the dimensions of information privacy concerns are classified into four different groups. These concern dimensions are data collection, unauthorized secondary usage, improper access and control. The groups are determined through the literature review of previous studies on information privacy concerns. These groups are the most mentioned concerns in the conceptualization articles in this field. The concerns consist of 14 items and they are distributed to the groups considering their interests. In this study, it is aimed to measure the effect of the referred antecedents on all the concern groups differently.

The first concern about information privacy is data collection. This concern is about the reaction of people against the collecting of their information by different sources. The items in this concern are government's data collection, companies' data collection, malicious data collection and the data storing by social media.

The second information privacy concern category is unauthorized secondary usage. This concern is about the use of the collected data out of the collection purpose. The fear of the exploitation of information that is consciously shared by

people makes the people concerned. Unauthorized secondary usage of the collected data by e-commerce websites, government, familiar people, communication websites and banking websites are the five items in this concern.

Improper access is another category of information privacy concerns in this study. Users are likely to consider who, when and how can reach their information after they share it. The access conditions to their information reveal this kind of concern. The concern about improper access to the information shared with the government, companies, communication technologies and banks form the items in this category.

The fourth information privacy concern is control. To have control over the information after sharing it is important in terms of feeling that the information is secure. Hence, people desire to have a chance to change, modify or remove the data that they had already shared. The right to data removal, company data control and government data verification are the three items in the control category.

As the dependent variable of this study, IT usage habits of the users are investigated in relation to information privacy concerns. As seen in the literature review phase, different privacy concerns may have a role in the IT usage habits. Information technologies offer a wide range of opportunities, from the communication field to finance. Some of these technologies are seen critical in terms of security while others are not. Therefore, usage habits of the concerned user and their reactions can vary for different kinds of information technologies. In total 17 items are specified to present the relationship between information privacy concerns and IT usage. These items are: social media sharing with friends, social media sharing with everyone, political social media sharing, political social media sharing with friends, familial social media sharing, navigation, e-government, mobile apps,

mobile communication apps, business e-mail, personal e-mail, webcam for business, webcam for personal purposes, photo sharing apps, location sharing apps, online banking, mobile banking apps.

In the theoretical framework, the variables, which are included in the research model of the thesis can be seen (See Fig. 8).

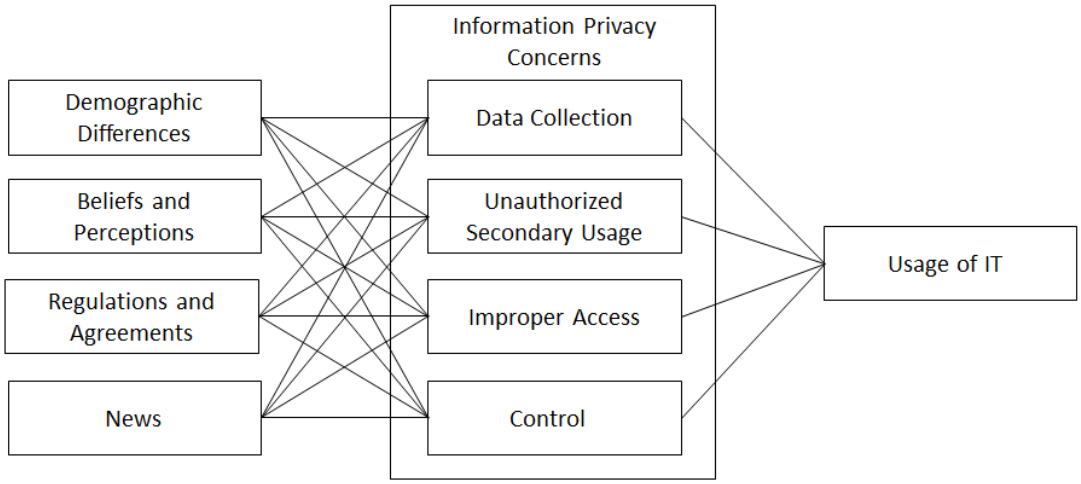

Fig. 8 Theoretical framework of the thesis

Usage of IT is associated to the information privacy concerns in this framework, while information privacy concerns, which are data collection, unauthorized secondary usage, improper access and control, are considered in a relationship with the antecedents of the information privacy concerns.

As seen in the framework in Figure 8, the relationship between the antecedents and information privacy concerns is examined differently for each context. The relationship between the four antecedents and four types of concerns can generate 16 hypotheses. Moreover, the relationship between information privacy concerns and the usage of IT generates four more hypotheses. A total 20 hypotheses will be tested in the scope of this research:

- H1: There are significant differences among different demographic profiles in terms of the concerns about data collection.
- H2: There are significant differences among different demographic profiles in terms of the concerns about unauthorized secondary usage of information.
- H3: There are significant differences among different demographic profiles in terms of the concerns about improper access to the information.
- H4: There are significant differences among different demographic profiles in terms of the concerns about the control of information.
- H5: There is a negative relationship between beliefs and perceptions and the concerns about data collection.
- H6: There is a negative relationship between beliefs and perceptions and the concerns about unauthorized secondary usage of information.
- H7: There is a negative relationship between beliefs and perceptions and the concerns about improper access to the information.
- H8: There is a negative relationship between beliefs and perceptions and the concerns about the control of information.
- H9: There is a positive relationship between regulations and agreements and the concerns about data collection.
- H10: There is a positive relationship between regulations and agreements and the concerns about unauthorized secondary usage of information.
- H11: There is a positive relationship between regulations and agreements and the concerns about improper access to the information.
- H12: There is a positive relationship between regulations and agreements and the concerns about the control of information.

- H13: There is a positive relationship between the news on information privacy and the concerns about data collection.
- H14: There is a positive relationship between the news on information privacy and the concerns about unauthorized secondary usage of information.
- H15: There is a positive relationship between the news on information privacy and the concerns about improper access to the information.
- H16: There is a positive relationship between the news on information privacy and the concerns about the control of information.
- H17: There is a negative relationship between the concerns about data collection and the usage of IT.
- H18: There is a negative relationship between the concerns about unauthorized secondary usage of information and the usage of IT.
- H19: There is a negative relationship between the concerns about improper access to the information and the usage of IT.
- H20: There is a negative relationship between the concerns about the control of information and the usage of IT.

The hypotheses with regard to the relationship between beliefs and perceptions and information privacy concerns indicate a negative relationship, similar to the relationship between regulations and agreements and information privacy concerns. As mentioned in the literature review part, public opinion on privacy can be affected by the conditions and to be secure is one of the significant indicators of these conditions. Concerns are likely to be left aside when the subject is security or public order. In addition, regulations and agreements seem as the assurance to the users for their information and they are considered as a protector.

Thus, they are expected to have a negative relationship with information privacy concerns.

However, news including information privacy topics contributes to the public concern. Exploitation of information, secret surveillance activities of government, and data processing by companies increase the fear of losing privacy. The cases examined in the literature review show the increasing popularity of the information privacy topic among the media and public reaction to this issue stands as an area to research.

The demographic differences context consists of variables such as age, income level, education level, gender, internet literacy. The relationship between these variables and information privacy concerns is expected to vary. According to the literature review, it is shown that some of these are already tested by different studies. However, in the scope of this study, it is aimed to examine the relationship between all these variables and information privacy concerns and get an outcome about the significance of demographic differences on privacy concerns.

The relationship between all information privacy concerns and the usage of IT is considered negative. As a general consideration, IT usage behavior is likely to be negatively affected by information privacy concerns. However, it is possible that different types of concerns may show a separate degree of effect on the behavior. One of the goals of this study is to test the effects of different types of concerns on IT usage behavior, in addition to measuring the concern in general.

CHAPTER 3

RESEARCH METHODOLOGY

In the scope of this study, a quantitative survey was conducted for the purpose of testing the hypotheses which are related to information privacy concerns (See Appendix A). The survey was conducted with regular technology users who use technological devices and the internet in their daily life. To reach people with different demographic characteristics and from different regions, the survey was presented to various groups of people.

The survey was applied in two ways: offline and online. All survey data that was collected offline was gathered from the survey participants via face-to-face sessions. The participants in these sessions were students, university researchers and some employees of various private technology companies. In this way, 140 people participated in the research.

For the purpose of gathering online forms, a website was created using PHP. The webpage was hosted at http://misprivate.boun.edu.tr/tanrikulu/un577/ghx875v.txt. This website consists of three pages: the first page presents the informed consent form to the participant, the second page includes the questions of the survey form and the last page delivers a thanks message after the form has been completed. With the completion of the form, the results were stored in a text file in an encrypted form securing the private information of the participants. Via the online form, 501 people participated the research. In total, 641 participants completed the online and offline forms to contribute to the study.

All individuals participated in the research voluntarily and all parts of the questionnaire were explained in beginning of the sections to keep the understanding high and to reach the maximum number of participants. All questions were presented as mandatory to fill and the participants were asked to select only one option for each question. No multi-answered or open-ended question was asked to the participants. The aim of the obligation to address every question was to gather valid and accurate data with no missing values. In this way, the challenges of missing values in the dataset were handled in the course of the survey period. Individuals younger than 18 were not allowed to participate in the research.

The questionnaire includes five sections, aiming to get an appropriate dataset in order to test the hypotheses of this study. In section one, the information about the research is presented with the abstract of the study and the participants are informed through a consent text. In the consent text, the approximate duration for participation in the survey, the aim of the questionnaire, privacy commitments and information about the researchers are mentioned. Underneath the first section, following the information and consent text, the participants are asked to fill in the name and the participation approval parts. The participation date, address and e-mail of the participants are also asked in this section. In the hard copy, a signature of the participant is requested, while in the soft copy, the participant is requested to fill the checkbox of the consent from.

The second section of the questionnaire consists of six questions about the demographic attributes of the participants. In this section, the age, overall monthly income, education status, gender, internet literacy and virtual attack experience of the participants are asked. The virtual attack experience question, which is the last of this

section, asks the participants if they have faced a virtual attack such as online hacking, identity theft, online fraud, etc.

The third section asks the opinions of the participants in regard to the antecedents of information privacy concerns. With this purpose, a Likert-scale of nine items is presented in this section. Three of these items are related to beliefs and perceptions, five of them are related to regulations and agreements, and the other three items are about news. The scale consists of five levels: strongly disagree, disagree, neither agree nor disagree, agree, strongly agree, where "1" represents the strongly disagree option, "5" represents strongly agree.

Information privacy concerns are the topic of the fourth section of the questionnaire. There are 14 items in this section, where four of them are about data collection, five of them are about unauthorized secondary usage, four are related to improper access and the last three are related to control. This section is in the Likert-scale form with the five options, too. Similar to section 3, the scale consists of five levels, from strongly disagree to strongly agree. The four concern types in this section question the thoughts of the participants in different ways. For example, questions focus on information concerns of the participants about governments or companies, both asked in different items to get a comparable dataset between them, in addition to the concern types. All questions are asked in this section in a positive way.

The goal of the fifth and the last section of this survey is to determine technology usage habits of the participants. Different kinds of technologies are asked in this section to measure the effects of the concerns in a wide variety. This section is formed as a Likert-scale, too. But unlike the other sections, the scale consists of five different levels of frequency: never, rarely, sometimes, often, always. The first five

items are related to the social media usage behaviors. The others are about mobile phones, e-mails, webcams, online websites, navigation devices, mobile applications and banking applications (See Appendix B).

The survey was provided to the participants who were eligible to participate in two different ways, online and offline. It was aimed to get an appropriate survey population to test the hypotheses properly. Hence, technology users from different groups were targeted while collecting the survey data.

The distribution method for the survey was nonprobability sampling for both online and offline surveys. Offline surveys were conducted with the appropriate people for study via face-to-face sessions. For this reason, the convenience sampling technique was used to gather the offline survey data. The people who were eligible for the study were asked to participate in the survey in different locations. For online surveys, the judgmental sampling technique was used. Different interest groups were targeted and the survey form was e-mailed to these groups. In addition, Facebook groups with different interests were used to distribute online survey forms. The people who responded to the communications participated in the survey voluntarily.

CHAPTER 4

ANALYSIS OF THE RESEARCH

4.1 Descriptive analysis

In this section, the descriptive analysis of the survey is presented as the first part of the research analysis. In this part, demographic distributions of the survey population are presented.

As shown in Table 4, distributions of the variables range between -2 and +2 for skewness and kurtosis values, which is indicated as the accepted range for assuming the distribution of a variable is a standard normal one (George & Mallery, 2010).

Table 4. Skewness and Kurtosis Values of Variables

		Skewness	Kurtosis
Antecedents of Information Privacy Concerns	Beliefs and Perceptions	.198	-.650
	Regulations and Agreements	-1.039	1.661
	News	-.117	-.014
Dimensions of Information Privacy Concerns	Data Collection	-.818	.771
	Unauthorized Secondary Usage	-.752	.836
	Improper Access	-.936	1.725
	Control	-.880	1.011
Information Technologies	IT Tools	-.960	.766
	Information Sharing	.461	-.084
	Political Sharing	.771	-.291
	Webcam	.585	-.424

In the Table 5, the age distribution of the participants in the survey is presented:

Table 5. Age Distribution

Age		
	Frequency	Percent
18-25	240	37.4%
26-35	225	35.1%
36-45	82	12.8%
46+	94	14.7%

18-25 and 26-35 age ranges are seen as the majority with 37.4% and 35.1% respectively. The people in this age range are the most frequent users of technology and the internet in Turkey (TurkStat, 2015). Thus, in the course of the survey research, the young population in these age ranges was aimed at the most. Furthermore, to keep the survey comprehensive in terms of all technology using population, other age groups are also included in the research: 36-45 and 46+ age ranges constitute the rest of the age distribution.

From low to high, the ranges of income level can be seen in the Table 6.

Table 6. Income Distribution

Income		
	Frequency	Percent
1000 TL >	137	21.4%
1000 - 1999 TL	95	14.8%
2000 - 2999 TL	90	14.0%
3000 - 3999 TL	97	15.1%
4000 - 5999 TL	130	20.3%
6000 TL <	92	14.3%

Income rates of the participants in the research show a balanced distribution. Four categories in the income table range from 90 to 97, whereas the other two categories, 1000 – 1999 TL and 4000 – 5999 TL, represent 137 and 130 participants respectively. Similarly, the percentages of the six income categories range between 14.0% and 21.4%.

The education levels of the survey participants can be seen in the Table 7

.

Table 7. Education Level Distribution

Education Level		
	Frequency	Percent
High school or Lower	161	25.1%
Bachelor's	366	57.1%
Master's or Higher	114	17.8%

The education levels of the survey participants can be seen in the figure above. The education status distribution consists of three groups. The education level table of the participants shows the status of the participants according to their last degree earned. The high school or lower group includes not only high school graduates but also uneducated people, elementary school graduates. Similarly, the master's or higher group includes people who have a Ph.D. or a higher degree. As can be seen in the Table 7, the majority of the participants are bachelor's graduates. The Table 8 describes the gender distribution of the survey participant:

Table 8. Gender Distribution

Gender		
	Frequency	Percent
Male	313	48.8%
Female	328	51.2%

As it is seen in the Table 8, the number of female participants is slightly higher than that of male participants, where male participants are 313 with 48.8% and females are 328 with 51.2%.

Table 9 presents daily internet usage hours of the participants:

Table 9. Internet Usage Distribution

Internet Usage (Hour/Day)		
	Frequency	Percent
0-2	170	26.5%
3-4	240	37.4%
5-7	127	19.8%
8 <	104	16.2%

Most of the participants state that they use the internet 3-4 hours a day. The second most stated usage range is 0-2, which is followed by 5-7 and 8<.

Additionally, it is asked in the survey whether the participants experienced a virtual attack such as hacking, fraud or identity theft online. In the Table 10, the ratio of the answers can be seen.

Table 10. Virtual Attack Experience Distribution

Virtual Attack Experience		
	Frequency	Percent
Yes	197	30.7%
No	444	69.3%

30.7% of the participants responded to this question “yes”, while 69.3% answered “no”. This data resembles the results of a research that argues 31% of the citizens in Turkey faced similar online security problems in the last 12 months (TurkStat, 2015).

4.2 Reliability and factor analysis

Cronbach's alpha is one of the most popular methods that are used for indicating the reliability of a scale in social sciences. Cronbach's alpha represents internal consistency of the items in a group and the number of items also affects Cronbach's alpha value. A high level of Cronbach's alpha means the measurement of the items in the scale is correlated while lower levels do not.

According to George and Mallory (2003), the rules of thumb for Cronbach's alpha are given (See Table 11).

Table 11. Rules of Thumb for Cronbach's Alpha

Cronbach's alpha	Internal consistency
≥ 0.9	Excellent
≥ 0.8	Good
≥ 0.7	Acceptable
≥ 0.6	Questionable
≥ 0.5	Poor
0.5 >	Unacceptable

(George & Mallery, 2003)

The antecedents and the dimensions of information privacy concerns consist of three and four scales, respectively. Demographic differences are not included in this analysis because the scale for demographic differences is not appropriate. The scales that are presented in the table below are based on the 5-point Likert scale model. In Table 12, Cronbach's alpha value and the count of the items in this variable are presented. As seen in the table, all scales in this section have the alpha value above the acceptable level. These levels can be interpreted as they are eligible to be considered that they have adequate internal consistency.

Table 12. Reliability Analysis

Reliability Analysis		
Variable	Cronbach's Alpha	N of Items
Beliefs and Perceptions	.797	3
Regulations and Agreements	.719	3
News	.783	3
Data Collection	.716	3
Unauthorized Secondary Usage	.810	5
Improper Access	.774	4
Control	.703	2

4.3 Factor analysis

The last section of the survey aims to measure IT usage habits of the participants. For this purpose, 17 questions are addressed to the participants. Every question in this section represents a different technology or a different feature of similar technologies. As in the other sections, in this part of survey a 5-point Likert scale model is used.

To reduce the dimensions of the IT habits section, a factor analysis with the principal component method is used in this chapter. The factor analysis results in four factors and their loadings according to the rotated component matrix are as follows (See Table 13).

Table 13. Factor Analysis of IT Usage

Factors	Item	Loading
1. IT Tools Variance explained: 28.1%	Mobile Banking Apps	.802
	Online Banking	.794
	Business Email	.754
	Mobile Apps	.691
	Navigation	.686
	Personal Email	.671
	Mobile Communication Apps	.655
	E-government	.370
2. Information Sharing Variance explained: 16.8%	Social Media Sharing With Friends	.831
	Social Media Sharing With Everyone	.769
	Location Sharing Apps	.746
	Photo Sharing Apps	.697
	Familial Social Media Sharing	.579
3. Political Sharing Variance explained: 8.9%	Political Social Media Sharing With Friends	.862
	Political Social Media Sharing	.852
4. Webcam Variance explained: 7.6%	Business Webcam	.831
	Personal Webcam	.815

The factor analysis of IT usage items has 0.790 Kaiser-Meyer-Olkin measure of sampling adequacy value and Bartlett's test is significant with 0.000. These outcomes indicate that the samples are appropriate for the factor analysis.

Four factors are revealed via the analysis. These factors can be grouped under the names of *IT Tools*, *Information Sharing*, *Political Sharing* and *Webcam*. The *IT Tools* group contains banking, e-government services, mobile applications, navigation and e-mail tools. Additionally, this group explains 28.1% of the total variance. The second group includes the items about information sharing on social media, location and photo sharing services. This group explains 16.8% of the total variance. The third group consists of social media, but for political sharing only, and *Webcam* is the last group, which contains the items about the use of webcams.

Furthermore, the third and fourth groups explain 8.9% and 7.6% of the total variance, respectively.

Cronbach's alpha values of the factors that are created via the analysis are listed in Table 14.

Table 14. Reliability Analysis of IT Usage Factors

Factors		Cronbach's Alpha	N of Items
Factor 1	IT Tools	.845	8
Factor 2	Information Sharing	.808	5
Factor 3	Political Sharing	.815	2
Factor 4	Webcam	.727	2

According to the reliability analysis table of the IT usage groups, all factors have higher Cronbach's alpha values than 0.7, which is an acceptable level of reliability.

4.4 t-Test analysis

In this part of the study, independent-samples *t*-test is used to measure some of the hypotheses. This type of test is used to compare two different samples with identical distribution in terms of a variable. As a result of the test, it is inferred whether there is a significant difference in regard to the variable between the two independent sets of the population. Additionally, in this test, variables should be in scale format.

Within the scope of the study, the gender and experience of virtual attack features are tested in regard to the dimensions of information privacy concerns.

4.4.1 Gender

Gender is one of the two demographic variables which are used in the *t*-test analysis to validate the hypotheses. This variable consists of two groups: female and male. The purpose of this test is to obtain a result about the difference between these two groups in terms of the dimensions of privacy concerns.

There is not a significant difference between female and male participants in terms of information privacy concerns for all dimensions, because the significance value for all dimensions is over 0.05 (See Table 15). On the other hand, it can be seen that the means of the concerns are slightly higher for female participants, compared to males, but it cannot be interpreted as significant.

Table 15. t-Test Analysis of Gender Variable

Dimensions Of Concerns	Gender	N	Mean	Std. Deviation	*t*	p
Data Collection	Female	328	3.8862	.79194	.989	.323
	Male	313	3.8211	.87418		
Unauthorized Secondary Usage	Female	328	3.9915	.75431	1.568	.117
	Male	313	3.8965	.77956		
Improper Access	Female	328	4.1227	.72736	1.934	.054
	Male	313	4.0104	.74335		
Control	Female	328	3.9771	.84697	.907	.365
	Male	313	3.9169	.83271		

4.4.2 Virtual attack experience

Virtual attack experience is another question which is addressed to the participants in the survey. It asked the participants to answer whether they experienced an incident like hacking, fraud or identity theft. The answers consist of two options, “yes” or “no”, and these are also the groups of this variable. To see the difference between the users who experienced such an incident and users who did not experience it, an independent-samples *t*-test is performed.

The results of the independent-samples *t*-test can be seen in Table 16. Based on the values of the table, there is a significant difference between the two populations in regard to the concern dimensions except the control dimension, shown by the significance values, which are under 0.05. For the data collection, unauthorized secondary usage and improper access dimensions, it can be seen that the mean value of the users who had experienced a virtual attack before is significantly higher than others. However, when it comes to the control dimension of information privacy concerns, there is not a significant difference between the two populations, because its significance value is 0.119.

Table 16. t-Test Analysis of Virtual Attack Variable

Dimensions Of Concerns	Virtual Attack	N	Mean	Std. Deviation	*t*	*p*
Data Collection	Yes	197	3.9611	.74013	2.302	.022
	No	444	3.8071	.86776		
Unauthorized Secondary Usage	Yes	197	4.1096	.72094	3.650	.000
	No	444	3.8721	.77712		
Improper Access	Yes	197	4.2107	.70623	3.294	.001
	No	444	4.0045	.74195		
Control	Yes	197	4.0254	.90878	1.561	.119
	No	444	3.9133	.80617		

4.5 Analysis of variance (ANOVA)

Analysis of variance (ANOVA) is a statistical method that is used to compare two or more sets of data's variances and means in regard to a parametric dependent variable. The test is represented by the *F* value and if this value is significant, in other words lower than 0.05, it can be said that there is a significant difference between the populations in terms of the mean and variance.

In this section, different demographic variables like age, income, education and internet usage literacy are tested, and it is examined if there are significant differences between the groups of these variables in regard to the dimension of information privacy concerns.

4.5.1 Age

The variable consists of four age groups: 18-25, 26-35, 36-45 and 46+. To examine the difference between these groups in regard to the dimension of concerns ANOVA is used. The descriptive analysis of age distribution is presented in Table 17.

Table 17. Descriptive Analysis of Age Distribution

Dimensions of Concerns	Age	N	Mean	Std. Deviation
Data Collection	18-25	240	3.73	.861
	26-35	225	3.88	.826
	36-45	82	3.95	.817
	46+	94	4.02	.754
	Total	641	3.85	.833
Unauthorized Secondary Usage	18-25	240	3.83	.809
	26-35	225	3.98	.751
	36-45	82	4.10	.780
	46+	94	4.03	.649
	Total	641	3.95	.768
Improper Access	18-25	240	3.99	.812
	26-35	225	4.11	.695
	36-45	82	4.12	.749
	46+	94	4.13	.599
	Total	641	4.07	.737
Control	18-25	240	3.94	.837
	26-35	225	3.97	.825
	36-45	82	3.86	.976
	46+	94	4.00	.758
	Total	641	3.95	.840

The results of the ANOVA show that there is a significant difference between the age groups in terms of data collection and unauthorized secondary usage, with 0.14 and 0.18 significance values, while there is not for the improper access and

control dimensions, with 0.184 and 0.706, respectively (See Table 18). Moreover, *F* values of data collection and unauthorized secondary usage are 3.565 and 3.368.

Table 18. ANOVA Analysis of Age Groups

		Sum of Squares	df	Mean Square	*F*	P
Data Collection	Between Groups	7.334	3	2.445	3.565	.014
	Within Groups	436.854	637	.686		
	Total	444.188	640			
Unauthorized Secondary Usage	Between Groups	5.888	3	1.963	3.368	.018
	Within Groups	371.219	637	.583		
	Total	377.107	640			
Improper Access	Between Groups	2.628	3	.876	1.619	.184
	Within Groups	344.795	637	.541		
	Total	347.423	640			
Control	Between Groups	.988	3	.329	.466	.706
	Within Groups	450.511	637	.707		
	Total	451.499	640			

When the Table 17 is investigated, it can be seen that the means of the concern levels show an increasing trend for the data collection and unauthorized secondary usage dimensions, which have a significant value. Only the 46+ group slightly interrupts the upward trend of unauthorized secondary usage concerns for the means, while the others have an increasing trend with the age.

For the post-hoc analysis, Levene's statistical values for the data collection and unauthorized secondary usage variables are investigated, which are 0.780 and 2.393, respectively ($p>0.05$). Due to their significance value, they are "equal variances assumed" and the LSD post-hoc test is applied to the variables (Myers & Well, 2003).

According to the LSD test, there is a significant difference between the 18-25 and other age levels in regard to the data collection concern, but for the other age levels there is not (See Table 19).

Table 19. LSD Test for Age Groups – Data Collection

Data Collection	26-35	36-45	46+
18-25	-0.153*	-0.222*	-0.292**
26-35		-0.68	-0.138
36-45			-0.7

Similar to the data collection concern, in terms of the unauthorized secondary usage concern there is a significant difference between the 18-25 and other age levels, while for the relationships among the other age levels this cannot be said (See Table 20).

Table 20. LSD Test for Age Groups – Unauthorized Secondary Usage

Unauthorized Secondary Usage	26-35	36-45	46+
18-25	-0.146*	-0.266**	-0.194*
26-35		-0.119	-0.047
36-45			-0.072

4.5.2 Income

The income variable has six different groups: 1000 TL >, 1000 - 1999 TL, 2000 - 2999 TL, 3000 - 3999 TL, 4000 - 5999 TL, 6000 TL <. These groups cover all possible income levels, and to see if there is a difference between them in terms of the concerns, the ANOVA test is conducted. The descriptive analysis of income distribution can be seen in Table 21.

Table 21. Descriptive Analysis of Income Distribution

Dimensions of Concerns	Income	N	Mean	Std. Deviation
Data Collection	1000 TL >	137	3.71	.948
	1000 - 1999 TL	95	3.73	.844
	2000 - 2999 TL	90	3.86	.788
	3000 - 3999 TL	97	3.93	.810
	4000 - 5999 TL	130	3.98	.735
	6000 TL <	92	3.93	.809
	Total	641	3.85	.833
Unauthorized Secondary Usage	1000 TL >	137	3.82	.833
	1000 - 1999 TL	95	3.91	.805
	2000 - 2999 TL	90	4.01	.719
	3000 - 3999 TL	97	3.89	.790
	4000 - 5999 TL	130	4.02	.699
	6000 TL <	92	4.06	.727
	Total	641	3.95	.768
Improper Access	1000 TL >	137	3.96	.841
	1000 - 1999 TL	95	4.06	.775
	2000 - 2999 TL	90	4.12	.694
	3000 - 3999 TL	97	4.07	.692
	4000 - 5999 TL	130	4.12	.664
	6000 TL <	92	4.10	.717
	Total	641	4.07	.737
Control	1000 TL >	137	3.89	.865
	1000 - 1999 TL	95	3.96	.810
	2000 - 2999 TL	90	3.78	.945
	3000 - 3999 TL	97	3.97	.825
	4000 - 5999 TL	130	4.08	.785
	6000 TL <	92	3.97	.798
	Total	641	3.95	.840

According to the results, none of the dimensions of information privacy concerns show a significant difference between different income levels. All significance values are equal to or over 0.05. Although the data collection concern has 0.05 value, it is not accepted as significant due to the definition of significance (See Table 22). In the descriptive analysis of the income levels, a slight positive

relationship between data collection and income can be seen but cannot be interpreted as significant (See Table 21).

Table 22. ANOVA Analysis of Income Groups

		Sum of Squares	df	Mean Square	F	P
Data Collection	Between Groups	7.652	5	1.530	2.226	.050
	Within Groups	436.536	635	.687		
	Total	444.188	640			
Unauthorized Secondary Usage	Between Groups	4.827	5	.965	1.647	.146
	Within Groups	372.280	635	.586		
	Total	377.107	640			
Improper Access	Between Groups	2.225	5	.445	.819	.537
	Within Groups	345.198	635	.544		
	Total	347.423	640			
Control	Between Groups	5.586	5	1.117	1.591	.160
	Within Groups	445.913	635	.702		
	Total	451.499	640			

According to the results, none of the dimensions of information privacy concerns show a significant difference between different income levels. All significance values are equal to or over 0.05. Although the data collection concern has 0.05 value, it is not accepted as significant due to the definition of significance. In the descriptive analysis of the income levels, a slight positive relationship between data collection and income can be seen but cannot be interpreted as significant.

Because there is not a significant difference for information privacy concerns in terms of income levels, post-hoc tests are not suitable to apply.

4.5.3 Education

The education variable has three different levels in this research: High school or Lower, Bachelor's, Master's or Higher. Lower levels than high school, like elementary school, are included in the High school or Lower groups, while levels like Ph.D. are included in Master's or Higher. The descriptive analysis of the education groups are presented in Table 23.

Table 23. Descriptive Analysis of Education Groups

Dimensions Of Concerns	Education	N	Mean	Std. Deviation
Data Collection	High school or Lower	161	3.75	.857
	Bachelor's	366	3.88	.837
	Master's or Higher	114	3.92	.780
	Total	641	3.85	.833
Unauthorized Secondary Usage	High school or Lower	161	3.82	.752
	Bachelor's	366	3.98	.785
	Master's or Higher	114	4.01	.717
	Total	641	3.95	.768
Improper Access	High school or Lower	161	3.98	.718
	Bachelor's	366	4.09	.750
	Master's or Higher	114	4.11	.717
	Total	641	4.07	.737
Control	High school or Lower	161	3.90	.810
	Bachelor's	366	3.95	.868
	Master's or Higher	114	4.00	.793
	Total	641	3.95	.840

There is not a significant difference among the education levels in terms of information privacy concerns, shown by the significance values which are over 0.05 (See Table 24).

Table 24. ANOVA Analysis of Education Groups

		Sum of Squares	df	Mean Square	F	p
Data Collection	Between Groups	2.543	2	1.272	1.837	.160
	Within Groups	441.645	638	.692		
	Total	444.188	640			
Unauthorized Secondary Usage	Between Groups	3.495	2	1.747	2.984	.051
	Within Groups	373.612	638	.586		
	Total	377.107	640			
Improper Access	Between Groups	1.653	2	.826	1.525	.218
	Within Groups	345.770	638	.542		
	Total	347.423	640			
Control	Between Groups	.730	2	.365	.516	.597
	Within Groups	450.769	638	.707		
	Total	451.499	640			

Examining the Table 24, it can be interpreted that the means of the concerns grouped by education levels show an increasing trend from lower to higher education levels; in spite of this, it could not be accepted as a significant result.

Similar to the income levels, there is not a significant difference for information privacy concerns in terms of the education levels; therefore the post-hoc analysis is not required in this case.

4.5.4 Internet usage literacy

The internet usage literacy of the users is measured by the daily Internet usage hours in this study. The usage variable consists of four different hour ranges, which are 0-2, 3-4, 5-7 and 8<. To examine the difference among these groups in regard to the dimensions of concerns, the ANOVA test is applied. The descriptive analysis of internet usage groups can be seen in Table 25.

Table 25. Descriptive Analysis of Internet Usage Groups

Dimensions of Concerns	Daily Internet Usage Hours	N	Mean	Std. Deviation
Data Collection	0-2	170	3.74	0.869
	3-4	240	3.90	0.801
	5-7	127	3.84	0.887
	8 <	104	3.95	0.767
	Total	641	3.85	0.833
Unauthorized Secondary Usage	0-2	170	3.84	0.822
	3-4	240	3.96	0.710
	5-7	127	3.99	0.838
	8 <	104	4.04	0.700
	Total	641	3.95	0.768
Improper Access	0-2	170	3.98	0.762
	3-4	240	4.06	0.715
	5-7	127	4.13	0.792
	8 <	104	4.15	0.663
	Total	641	4.07	0.737
Control	0-2	170	3.82	0.910
	3-4	240	3.92	0.804
	5-7	127	4.00	0.879
	8 <	104	4.16	0.709
	Total	641	3.95	0.840

According to the ANOVA results for the internet usage literacy groups, there is a significant difference among the groups in terms of the control concerns, whereas it cannot be stated for another dimension of the information privacy concerns (See Table 26). Data collection, unauthorized secondary usage and improper access concerns do not have a significantly different means for different internet usage levels.

Table 26. ANOVA Analysis of Internet Usage Groups

		Sum of Squares	df	Mean Square	F	p
Data Collection	Between Groups	3.655	3	1.218	1.762	.153
	Within Groups	440.532	637	.692		
	Total	444.188	640			
Unauthorized Secondary Usage	Between Groups	3.258	3	1.086	1.850	.137
	Within Groups	373.849	637	.587		
	Total	377.107	640			
Improper Access	Between Groups	2.630	3	.877	1.620	.184
	Within Groups	344.793	637	.541		
	Total	347.423	640			
Control	Between Groups	8.187	3	2.729	3.921	.009
	Within Groups	443.312	637	.696		
	Total	451.499	640			

The control dimension has 0.009 significance value with 3.921 *F* value, which indicates that it is significant, while the other dimensions have a significance value over 0.05. In addition, the means of the control dimension according to the usage hours show an increasing trend from low usage to high. The other dimensions have weaker trends, compared to control. Hence, ANOVA tests are not conducted as per significance in the results.

When Levene's statistics value is calculated for the control concerns among the internet usage groups, 1.661 value with significance is obtained (p>0.05). Thus, the LSD test, which is suitable in the case of "equal variances assumed", is examined:

Table 27. LSD Test for Internet Usage Groups – Control

Control	3-4	5-7	8 <
0-2	-0.103	-0.178	-0.345*
3-4		-0.075	-0.242*
5-7			-0.167

Table 28 shows that there is a significant difference between the people who use the internet more than 8 hours a day and the people who use it 0-2 or 3-4 hours a day, regarding the information privacy concern of control.

4.6 Correlation analysis

The bivariate correlation analysis is used to assess the relationship between two variables. To conduct this analysis, the variable should be measured in parametric scale format; hence, it cannot be used for nominal and ordinal types of variables. Similar to the other analysis in this study, as a significance indicator, the Pearson correlation coefficient is expected to be lower than 0.05. Moreover, examining the power of the relationship, the *r* value is considered. The *r* value of the correlation analysis ranges from -1 to 1 and it indicates not only the power of the relationship but also the direction of it.

With the help of this analysis, the hypotheses 5 to 20 in the theoretical model are tested. First, to assess the antecedents, except demographic differences and their relationship to the dimensions of information privacy concerns, the correlation analysis tests are conducted. Furthermore, the relationship between the dimension of information privacy concerns and IT usage behavior is also examined in the scope of this study. IT usage behavior tests are conducted to the IT groups that were created by the factor analysis in the previous sections.

4.6.1 Antecedents of the concerns

The correlation analysis of the antecedents of information privacy concerns are expressed in this section. The variables, which are analyzed in terms of the relationship to the dimensions of privacy concerns, are:

- Beliefs and Perceptions
- Regulations and Agreements
- News

4.6.1.1 Beliefs and perceptions

The beliefs and perceptions variable stands for the opinion of the participants about government and company surveillance for the purpose of security and public order. This opinion's relationship with the dimensions of information privacy concerns is examined via the bivariate correlation analysis.

In Table 28, the correlation between beliefs and perceptions and the dimensions of information privacy concerns can be seen. This result shows that the only significant relationship is between the beliefs and perceptions variable and the data collection dimension with -0.096 for *r* and 0.015 for the significance values, while the other dimensions do not have a significant relationship with the beliefs and perceptions variable, shown by the high significance values of them.

Table 28. Correlation Analysis of Beliefs and Perceptions

		Data Collection	Unauthorized Secondary Usage	Improper Access	Control
Beliefs and Perceptions	Pearson Correlation	-.096*	-.072	-.046	-.069
	p-Value	.015	.068	.244	.079
	N	641	641	641	641

4.6.1.2 Regulations and agreements

The variable of regulations and agreements expresses the opinion of the participants about the necessity and benefits for such in regard to information privacy of IT. Furthermore, to assess its relationship with the dimensions of information privacy concerns, the bivariate correlation analysis is applied.

As it can be seen in Table 29, the outcome of the correlation analysis shows a significantly positive relationship between the regulations and agreements variable and all dimensions of privacy concerns. Moreover, the significance values equal to 0, which means high significance for all dimensions.

Table 29. Correlation Analysis of Regulations and Agreements

		Data Collection	Unauthorized Secondary Usage	Improper Access	Control
Regulations and Agreements	Pearson Correlation	.171**	.251**	.311**	.193**
	p-Value	.000	.000	.000	.000
	N	641	641	641	641

The participants who give importance to IT regulations and agreements are also concerned about their information privacy in all aspects. However, not all the

dimensions have the same relationship power. Improper access is the most related dimension with regulations and agreements, shown by its *r* rate of 0.311, which is followed by unauthorized secondary usage with the *r* rate of 0.251. Control and data collection dimensions are associated less, with their *r* rates of 0.193 and 0.171, respectively.

4.6.1.3 News

The news variable represents the interest of the participants in the news about information privacy and the related concern with it. In the scope of this research, the association of news with information privacy concerns is measured using the bivariate correlation analysis.

The result of the correlation analysis indicates that all dimensions of information privacy concerns are positively related to IT privacy news, shown by their significance rate of 0 (See Table 30).

Table 30. Correlation Analysis of News

		Data Collection	Unauthorized Secondary Usage	Improper Access	Control
News	Pearson Correlation	.242**	.256**	.206**	.165**
	p-Value	.000	.000	.000	.000
	N	641	641	641	641

Unauthorized secondary usage of data is the most associated concern according to the analysis, with the *r* rate of 0.256, whereas the second most

associated one is data collection concern with 0.242 *r* rate. These are followed by the improper access and control dimensions, with 0.206 and 0.165 *r* rates, respectively.

4.6.2 IT usage behavior analysis

In this section of the study, the relation of the IT usage behavior and information privacy concerns are examined using the survey data. For this purpose, the analysis are grouped in four IT factor in this study:

- IT Tools
- Information Sharing
- Political Sharing
- Webcam

4.6.2.1 IT tools

As an outcome of the factor analysis, information technologies in the last section are grouped into the four subgroups and *IT Tools* is the most comprehensive of them. This factor includes technologies like mobile apps, online banking apps, e-mails, navigation tools, e-government services and mobile communication apps. The correlation analysis of usage of these IT tools with different dimensions of information privacy concerns is presented in Table 31.

Table 31. Correlation Analysis of IT Tools

		Data Collection	Unauthorized Secondary Usage	Improper Access	Control
IT Tools	Pearson Correlation	.149**	.156**	.178**	.170**
	p-Value	.000	.000	.000	.000
	N	641	641	641	641

According to Table 31, it can be seen that the usage of these IT tools is significantly positively correlated with all dimensions of information privacy concerns. Significance values are under 0.01 for all dimensions and correlation values range from 0.149 to 0.178, while the improper access dimension has the highest value. The control dimension follows it with a correlation value of 0.170. Furthermore, the unauthorized secondary usage and data collection dimensions have 0.156 and 0.147 for the Pearson correlation value, respectively.

4.6.2.2 Information sharing

The second group of information technologies consists of technologies related to sharing. For example, social media services, location and photo sharing apps are some of these technologies. However, political sharing usages of IT is not included in this group, because of the fact that the factor analysis separated it as an independent factor from regular information sharing. The relationship between these technologies and the concern dimensions in Table 32.

Table 32. Correlation Analysis of Information Sharing

		Data Collection	Unauthorized Secondary Usage	Improper Access	Control
Information Sharing	Pearson Correlation	-.004	-.049	-.016	-.014
	p-Value	.919	.216	.684	.731
	N	641	641	641	641

The correlation table for information sharing technologies indicates that it has no significant correlation with any dimension of information privacy concerns, shown by the high significant values. The lowest significance value is 0.216, which belongs to unauthorized secondary usage, whereas the other dimensions have higher significance values than this in regard to the correlation with information sharing.

4.6.2.3 Political sharing

The political sharing variable is the second factor of information technologies and is different from the information sharing factor, as it contains only the items about political sharing on social media services. Political sharing of the participants and its relationship to information privacy concerns is examined in the correlation analysis (See Table 33).

Table 33. Correlation Analysis of Political Sharing

		Data Collection	Unauthorized Secondary Usage	Improper Access	Control
Political Sharing	Pearson Correlation	.050	.062	.035	.001
	p-Value	.210	.119	.378	.985
	N	641	641	641	641

According to Table 33, the correlation analysis of political sharing and the dimensions of concerns does not show a significant relationship between them. As presented by higher significance values than the acceptable alpha value of 0.05 or less, the correlations cannot be specified as significant.

4.6.2.4 Webcam

Last but not least, the webcam group of information technologies consists of the items about webcam usage for business and personal purposes. Examining the relationship between webcam usage and information privacy concerns, similarly, a correlation analysis is conducted (See Table 34).

Table 34. Correlation Analysis of Webcam

		Data Collection	Unauthorized Secondary Usage	Improper Access	Control
Webcam	Pearson Correlation	.068	.033	.073	.061
	p-Value	.087	.404	.064	.122
	N	641	641	641	641

In the outcome of the correlation analysis in Table 34, it is seen that the relationship between webcam usage and the dimensions of concerns has no significant relationship, shown by the significance values, which range from 0.064 to 0.404. Because the acceptable alpha value equals 0.05, the correlation analyses described are insignificant for all dimensions of information privacy concerns and webcam usage.

4.7 Findings

In the scope of this study, the literature about information privacy and concerns related with this topic are investigated. After the review of the literature, a theoretical model is created considering the lacks in the literature on information privacy concerns. According to this model, 20 hypotheses are determined to be tested.

Information privacy concerns are grouped into four different dimensions, which are data collection, unauthorized secondary usage, improper access and control. The research model is based on these concerns and it branch out into two parts. One of the parts is the relationship between these concerns and their antecedents like demographic differences, beliefs and perceptions, regulations and agreements and news. The other one is the association of these concerns with IT usage behavior. Afterward, IT usage behaviors are considered in four different groups, which are general IT tools, information sharing technologies, political sharing via IT tools and webcam. All variables, which are mentioned in the research model, are tested for every dimension of information privacy concerns differently.

In the test phase, a quantitative survey is conducted with 641 participants, who are IT users. The participant population is selected to make the survey representative of IT users as far as possible. The survey data are tested with the help of the SPSS program and *t*-test, ANOVA and correlation analysis are utilized in the validation process of the hypotheses. Regression analysis is not preferred in this study, because the theoretical framework does not include a predictive model.

The first four hypotheses of the study are about the relationship between the demographic differences and information privacy concerns.

- H1: There are significant differences among different demographic profiles in terms of the concerns about data collection.
- H2: There are significant differences among different demographic profiles in terms of the concerns about unauthorized secondary usage of information.
- H3: There are significant differences among different demographic profiles in terms of the concerns about improper access to the information.
- H4: There are significant differences among different demographic profiles in terms of the concerns about the control of information.

After the analysis, the relationship status of these variables can be seen in Table 35.

Table 35. Relationship Between Demographic Differences and Concerns

Demographic Variables	Data Collection	Unauthorized Secondary Usage	Improper Access	Control
Gender				
Virtual Attack Experience	*	**	**	
Age	*	*		
Income				
Education				
Internet Usage Literacy				**

In Table 35, the relationship situations of the demographic variables are presented with the '*' characters, where '*' means the relationship is significant ($p<0.05$), while '**' means the relationship is highly significant ($p<0.01$). The blank cells state that there is no significant relationship between the variables.

According to the results, virtual attack experience and age attributes seem associated with the concern for data collection. These same attributes are associated

with the concerns about unauthorized secondary usage of information, similarly. Concerns about improper access to the information show a highly significant relationship with only one demographic attribute, virtual attack experience. Last by not least, concerns about the control of the information are highly associated with the internet usage literacy, differently from other concern dimensions.

Therefore, all dimensions of information privacy concerns have relationships with some demographic attributes. On the other hand, none of the dimensions is related with all of the attributes. For this reason, hypotheses H1, H2, H3 and H4 are partially supported by the analysis.

In the scope of this study, the antecedents of information privacy concerns are examined, as well. As one of these antecedents, the beliefs and perceptions variable and its relationship to the concerns about information privacy is tested. The hypotheses H5, H6, H7 and H8 are about this relationship between these variables.

- H5: There is a negative relationship between beliefs and perceptions and the concerns about data collection.
- H6: There is a negative relationship between beliefs and perceptions and the concerns about unauthorized secondary usage of information.
- H7: There is a negative relationship between beliefs and perceptions and the concerns about improper access to the information.
- H8: There is a negative relationship between beliefs and perceptions and the concerns about the control of information.

Table 36 expresses the relationship situation of the beliefs and perceptions and the dimension of information privacy concerns.

Table 36. Relationship Between Beliefs and Perceptions and Concerns

	Data Collection	Unauthorized Secondary Usage	Improper Access	Control
Beliefs and Perceptions	*(-)			

The '*' and '**' characters show the significance level of the relationship, while blank cells mean no significant relationship. Moreover, the sign in the parenthesis indicates the direction of the relationship.

Statistical tests which are applied to the survey data show that beliefs and perceptions are negatively associated with information privacy concerns only about data collection. In addition, this means there are no significant relationships for the other dimensions of the privacy concerns. Consequently, H5 is supported, but H6, H7 and H8 are not supported, shown by the outcomes of the correlation analysis.

As another variable of the antecedents of information privacy concerns, the regulations and agreements variable is tested in terms of the relationship. The hypotheses H9, H10, H11 and H12 are about this relationship.

- H9: There is a positive relationship between regulations and agreements and the concerns about data collection.
- H10: There is a positive relationship between regulations and agreements and the concerns about unauthorized secondary usage of information.
- H11: There is a positive relationship between regulations and agreements and the concerns about improper access to the information.
- H12: There is a positive relationship between regulations and agreements and the concerns about the control of information.

The results of the correlation analysis, which indicate the relationship between the regulations and agreements variable and the dimensions of information privacy concerns, can be seen in Table 37.

Table 37. Relationship Between Regulations and Agreements and Concerns

	Data Collection	Unauthorized Secondary Usage	Improper Access	Control
Regulations and Agreements	**(+)	**(+)	**(+)	**(+)

According to Table 37, all dimensions of privacy concerns are highly related to the regulations and agreements variable. Additionally, the directions of the relationships are determined as positive. Thus, the hypotheses H9, H10, H11 and H12 are supported by the analysis.

News is the last variable of the antecedents and its relationship to information privacy concerns is tested with the correlation analysis similar to the other variables. In the hypotheses H13, H14, H15 and H16, the relationship between the news variable and the dimensions of information privacy concerns is mentioned.

- H13: There is a positive relationship between news on information privacy and the concerns about data collection.
- H14: There is a positive relationship between news on information privacy and the concerns about unauthorized secondary usage of information.
- H15: There is a positive relationship between news on information privacy and the concerns about improper access to the information.
- H16: There is a positive relationship between news on information privacy and the concerns about the control of information.

In regard to Table 38, which shows the relationship between the news variable and the dimensions of information privacy concerns, all dimensions of the concerns are significantly positively related to the news variable. Therefore, this outcome supports the hypotheses H13, H14, H15 and H16, which refer to these associations.

Table 38. Relationship Between News and Concerns

	Data Collection	Unauthorized Secondary Usage	Improper Access	Control
News	**(+)	**(+)	**(+)	**(+)

Last but not least, IT usage behavior and its relationship to information privacy concerns are examined in this study. IT usage behavior is handled using the factor analysis to group information technologies, and the relationship between all these groups, which are created by the factor analysis, and information privacy concerns is tested by the correlation analysis. The last four hypotheses of this study, H17, H18, H19 and H20, are about this research subject.

- H17: There is a negative relationship between the concerns about data collection and the usage of IT.
- H18: There is a negative relationship between the concerns about unauthorized secondary usage of information and the usage of IT.
- H19: There is a negative relationship between the concerns about improper access to the information and the usage of IT.
- H20: There is a negative relationship between the concerns about the control of information and the usage of IT.

According to Table 39, general IT tools seem significantly positively related to all dimensions of information privacy concerns. However, the other IT groups, which represent a more specific grouping of the ITs such as information sharing technologies, political information sharing using IT and using a webcam, have no significant relationship to any kind of information privacy concern. Insignificant relationships are stated in the table with blank cells, similar to the other tables.

Table 39. Relationship Between IT Usage Behavior and Concerns

IT Usage Behavior	Data Collection	Unauthorized Secondary Usage	Improper Access	Control
IT Tools	**(+)	**(+)	**(+)	**(+)
Information Sharing				
Political Sharing				
Webcam				

Considering the correlation results in Table 39, there is a significant positive relationship between some IT types and information privacy concerns, but it cannot be said for all types of information technologies. The hypotheses H17, H18, H19 and H20 mention a negative relationship between the variables. Thus, the results of the analysis do not support these hypotheses.

CHAPTER 5

CONCLUSION

The outcomes of the research show that some of the demographic attributes are associated with information privacy concerns. One of the remarkable results is younger people seem less concerned about their information privacy, especially in the age group 18-25. The participants in this age group have significantly lower concern levels for two of the concern dimensions.

In addition, a virtual attack experience undoubtedly has an association with the concerns. This result can be a sign that people realize an issue and form a reaction to it better when they experience it.

As another outcome of the analysis, it can be seen that people who spend more time on the internet feel concerned about their information privacy in terms of the control. When the time spent on the internet increased, the disclosed information also can increase and this situation makes it hard to control.

Besides demographic variables, beliefs and perceptions have a relationship with the data collection dimension of information privacy concerns. This result indicates that some people think data collection is acceptable when it comes to security. Government policies on this subject after the 9/11 are one of the key factors in this consequence. In the case of the people who are forced to make a choice between their privacy and security, their perceptions affect their decisions.

Also, people who interested in regulations and agreements seem concerned about all dimensions of information privacy. After considering the increasing importance of privacy concerns in the modern technology era, this relationship becomes more sensible. Regulations are seen as a way for the protection of privacy

by most people. Moreover, user agreements, especially for technological products, are becoming more substantial in the mind of the society due to the new abilities of the technologies. The "internet of things" concept can be shown as an example of these new capabilities (Weber, 2010).

The interest in the news about information privacy is another factor which is positively related to information privacy concerns. This outcome can be examined with other factors. News is the main tool for creating a security perception in the society. The event of the 9/11 attacks are considerable in terms of shaping security perceptions of society (Lyon, 2007). In addition, the cases of Snowden and Assange are in the mind of all people who are interested in the news, and these play an important role in the forming of an opinion of the society.

In the other part of this study, information technology usage habits and information privacy concerns are investigated in terms of their association. As an outcome, it can be said that general IT tools, which include e-mail, mobile apps, online banking, etc., show a positive relationship with information privacy concerns. This result can be interpreted as follows: people who spend time with technological devices show more concern about their information privacy. However, for the other kind of IT groups, which are identified by the factor analysis, there is not a significant association with information privacy concerns. Information or political sharing do not show any significant relationship with the dimensions of information privacy concerns. The concern level for information privacy is unrelated with information sharing habits on the internet. Inversely, it cannot be stated that the people who are not concerned about information privacy are more or less likely to share it online. Even when the shared information includes any political thoughts, it does not make any difference. The concerned people could be considering online

information sharing activity meaningless for the purpose of taking any precautions or they can be paying no attention in this respect.

CHAPTER 6

DISCUSSION

The notion of Warren and Brandeis (1890) about privacy evolved to a new and far-reaching concept which affects the life of every individual due to modern technology. Information privacy concerns take part in various types of research and are regarded as a multi-disciplinary concept. Therefore, the outcomes of this study can be utilized in different research areas.

One of the research areas where information privacy concerns are important is the field of law. In order to respond to the opinion of the users, the thoughts of the society should be considered while preparing regulations and IT user agreements. In regard to the improvements in the technology era, the dynamic structure of the public order makes regulative reforms essential, with the aim of responding to the demand of the society. Thus, the antecedents that are mentioned in this study can be considered by the regulators as a preliminary work to analyze the requests about privacy concerns.

Another important research area to which the outcomes of this study can contribute is user experience investigations on information technologies. For example, in the theoretical creation phases of IT user acceptance models, information privacy concerns and the related IT usage behaviors should be taken into consideration. Moreover, IT users are more anxious about the privacy aspects of information technologies after the news about the surveillance activities of governments and companies. Therefore, research on this topic should include all aspects of information privacy concerns, including the antecedents.

Numerous foundations are actively working all around the world on the concept of information privacy concerns. These foundations are aiming to create awareness in the society and support people when it is needed with regards to information privacy. Thus, the analysis in this study on the relationship between IT usage behavior and information privacy concerns of individuals can help such organizations.

The study was conducted in Turkey and the outcomes reflect the information only for the country. This is can be shown as a limitation of this study. For further research, an international survey can be conducted to measure the difference between nations, as well.

Additionally to this study, the relationship of various aspects from different research areas can be examined in terms of information privacy concerns. As an instance, the psychological effect on a daily routine of the individual can be investigated with this notion. So, the significance of information privacy concerns can be understood more profoundly in such a multi-disciplinary study.

APPENDIX A

SURVEY

PARTICIPANT INFORMED CONSENT FORM

Supporting Foundation of Research: Boğaziçi University
Research Title: Privacy Paradox: Usage of technological power on the privacy and surveillance
Project Researchers: Prof. Dr. Zuhal Tanrıkulu/Emre Rençberoğlu
Address:UBYO-Yönetim Bilişim Sistemleri Bölümü, 34342, Bebek, İstanbul
E-mail: zuhal.tanrikulu @ boun edu tr / emre.rencberoglu @ boun edu tr
Phone: 90 0541 6219098

Project Abstract: Thanks to the developing technologies, reaching to the information has become easier and big data concept started to be used in various fields. Today, almost all of the technologies, which are used widely, like the internet, mobile phone, computer and smart TV are capable of collecting and storing data. Usually, the data gathering activity aims to improve the customer service, however the incidents like exploitation and misuse of the information can be seen. There are numerous cases which made reaction in the global public opinion on this subject. Besides the methodologies of the data collection, these topics are also should be discussed: who can use the collected data on what purpose, the effects of the data collection on the society and the consideration of the society on this subject. Within the scope of the project, in regard to the previous technological surveillance cases, the effects of the surveillance as pros and cons will be examined and the public opinion will be analyzed with the statistical methods. This research aims to examine the opinion and the awareness of the society about surveillance via technologies such as social media, e-mail, cameras, RFID, mobile phones, smart TVs, internet service providers.

The statistical researches will be held in the Management Information Systems Department by the consent of ethical committee.

Informed Consent: If you accept to participate the research, we request you to answer the questions in the survey form. It will take approximately 15 minutes to complete the form. This research is held on the scientific purposes and the information of the participants will be kept in private. In the survey form, your name will not be mentioned and instead of the name, a code id will be used. Your answers in the survey form will not be shared with any other foundation except Boğaziçi University, will be kept in private and not be used except scientific purposes. To participate the study is based on your own volition. We do not demand a fee from you and we will not pay to you. If you participate, you have a right to withdraw in any phase of the study. In case of withdraw, your data will be cancelled and not included in any analyses. Before signing this form, please ask your questions about this study. If you have a question later, you can ask to Emre Rencberoglu (90 541 6219098). Also, you can consult to local ethical committees about your rights.

If your address or phone number change, we request you to inform us, please.

I understand what has told me and the written text above. I accept to participate this study in these conditions of my own volition, without any press or force on me.

PLease choone one:

I took a copy of the form. ○ (In case of this the participant keeps this copy.)
I do not want to take a copy of the form. ○

Name and Surname:

E-mail:

Address (If available phone or fax number)
Country and City

Sign:

What is your age?

- Younger than 18
- 18-25
- 26-35
- 36-45
- 46-55
- Older than 56

What is your monthly overall income?

- Lower than $400
- 400-699 $
- 700-1099 $
- 1100-1499 $
- 1500-1799 $
- 1800-2299 $
- Higher than $2300

What is the highest level of education you have completed?

- Elemantary/Secondary School
- high School
- University-Bachelor Degree
- University-Master Degree
- PhD

What is your Gender?

- Female
- Male

How many hours in a day do you spend on internet?

- 0-2
- 3-4
- 5-7
- 8-10
- Lower than 10

Have you ever experienced a virtual attack on a digital environment?
Hacking, identity theft, fraud, ...

- Yes
- No

To what extent do you agree or disagree with each of the following statements.

	Strongly Disagree	Disagree	Neither Agree Nor Disagree	Agree	Strongly Agree
The surveillance of technological communication decreases the crime rate.	○	○	○	○	○
Government surveillance for security purpose is required.	○	○	○	○	○
Recording the activities of online IT users is beneficial in terms of the public order.	○	○	○	○	○
I think the user agreements, that indicate the using purposes, are necessary for the IT security.	○	○	○	○	○
I think the legal regulations, that indicate the using purposes, are necessary for the IT security.	○	○	○	○	○

I think that the legal regulations for the purpose of securing the personal data are beneficial.	○	○	○	○	○
I try to follow the news about the information privacy.	○	○	○	○	○
The news especially about the information privacy catch my attention.	○	○	○	○	○
I follow the old news about the information privacy and technological surveillance.	○	○	○	○	○

To what extent do you agree or disagree with each of the following statements.

	Strongly Disagree	**Disagree**	**Neither Agree Nor Disagree**	**Agree**	**Strongly Agree**
When I share my information on the internet, I am concerned that the information can be collected by the malevolent people.	○	○	○	○	○
I am concerned that the companies collect my information.	○	○	○	○	○
I am concerned that the governments collect my information.	○	○	○	○	○
When I shop online, I am concerned about the misuse of my information that I shared with the companies.	○	○	○	○	○
I am concerned about the misuse of the information that government collected about me from digital environment.	○	○	○	○	○
I am concerned about the misuse of the information that I share in an environment where only the close people to me can reach.	○	○	○	○	○
I am concerned about the misuse of the information that I share with the communication companies.	○	○	○	○	○
I am concerned about the unauthorized access to my information that I shared with the government.	○	○	○	○	○
When I shop online, I am concerned about the unauthorized access to my information, that collected by the companies.	○	○	○	○	○
I am concerned about the probability of unauthorized access to my information that I shared via communication technologies (e-mail, messaging, photo and file sharing etc.).	○	○	○	○	○
To cannot access and change the information that I share with the companies, makes me concerned.	○	○	○	○	○
Inability to control the truth of my information that collected by the government, makes me concerned.	○	○	○	○	○
I am concerned about the misuse of the information that banks have about me.	○	○	○	○	○
I am concerned that my information I share with banks can be collected by the malevolent people.	○	○	○	○	○

Please state the best suited usage frequency to you for the following technologies.

	Never	Rarely	Sometimes	Often	Always
I share my daily life activities via social media.	○	○	○	○	○
I share my daily life status with everyone via social media.	○	○	○	○	○
I share political posts with everyone via social media.	○	○	○	○	○
I share the information about me and my family via social media.	○	○	○	○	○
I share political posts with people ,who are close to me, via social media.	○	○	○	○	○
I regularly use navigation tools.	○	○	○	○	○
I use e-government tools.	○	○	○	○	○
I regularly use mobile phone applications.	○	○	○	○	○
I use online mobile phone communication applications (whatapp,...).	○	○	○	○	○
I regularly use e-mail tools for business purposes.	○	○	○	○	○
I regularly use e-mail tools for personal purposes.	○	○	○	○	○
I make online video calls for business purposes.	○	○	○	○	○
I make online video calls for personal purposes.	○	○	○	○	○
I share personal photos via photo sharing applications.	○	○	○	○	○
I share my location via location sharing applications.	○	○	○	○	○
I regularly use online banking tools.	○	○	○	○	○
I regularly use online banking tools on mobile phones or tablet computers.	○	○	○	○	○

APPENDIX B

ITEMS

Antecedents of Concerns	
Demographic differences	Age
	Income level
	Education level
	Gender
	Internet literacy
	Virtual attack experience
Beliefs and Perceptions	Surveillance for crime
	Security need
	Surveillance for public order
Regulations and Agreements	IT agreements for information security
	Regulations for information security
	Privacy protective regulations
News	Privacy news
	Information Privacy news
	Exploring news about privacy

Information Privacy Concerns	
Data Collection	Malicious data collection
	Companies' data collection
	Government's data collection
Unauthorized Secondary Usage	E-commerce secondary usage
	Government secondary usage
	Familiar people secondary usage
	Communication websites secondary usage
	Banking secondary usage
Improper Access	Government Improper access
	Companies Improper access
	Communication technologies Improper access
	Banking Improper access
Control	Company data control
	Government data verify

Information Technologies	
IT usage	Social media sharing with friends
	Social media sharing with everyone
	Political social media sharing

	Familial social media sharing
	Political social media sharing with friends
	Navigation
	E-government
	Mobile apps
	Mobile communication apps
	Business e-mail
	Personal e-mail
	Business webcam
	Personal webcam
	Photo sharing apps
	Location sharing apps
	Online banking
	Mobile banking apps

REFERENCES

6, P. (2006). The Personal Information Economy: Trends and Prospects for Consumers. In S. Lace (Ed.), *The Glass Consumer* (pp. 17–43). Bristol: The Policy Press.

Ackerman, S., & Ball, J. (2014). Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ. Retrieved March 21, 2015, from http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo

Acquisti, A., & Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making Traditional. *IEEE Security & Privacy*, 26–33.

Andrejevic, M. (2007). Surveillance in the Digital Enclosure. *The Communication Review*, *10*, 295–317. http://doi.org/10.1080/10714420701715365

Anthony, D., Stablein, T., & Carian, E. K. (2015). Big Brother in the Information Age : Concerns about Government Information Gathering over Time. *IEEE Security & Privacy*, *July/Augus*, 12–19.

Arthur, C. (2011). iPhone Keeps Record of Everywhere You Go. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears

Assange, J., Appelbaum, J., Müller-Maguhn, A., & Zimmermann, J. (2012). *Şifrepunk Özgürlük ve İnternetin Geleceği Üzerine Bir Tartışma*. Istanbul: Metis Yayınları.

Awad, N. F., & Krishnan, M. S. (2006). The Personalization Privacy Paradox: an Empirical Evaluation of Information Transparency and the Willingness To Be Profiled Online for Personalization. *MIS Quarterly*, *30*(1), 13–28. http://doi.org/10.2307/25148715

Barkhuus, L. (2004). Privacy in Location-Based Services , Concern vs Coolness. In *MobileHCI 2004*.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology*, *8*, 121–144. http://doi.org/10.1111/ips.12048

Bauman, Z., & Lyon, D. (2013). *Akışkan Gözetim*. Istanbul: Ayrıntı Yayınları.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4), 1017–1041.

Bennett, C. J. (2011). In Further Defence of Privacy. *Surveillance & Society*, *8*(4), 513–516.

Best, K. (2010). Living in the Control Society: Surveillance, Users and Digital Screen Technologies. *International Journal of Cultural Studies*, *13*(1), 5–24. http://doi.org/10.1177/1367877909348536

Boyd, D. (2008). Facebook's Privacy Trainwreck Exposure, Invasion, and Social Convergence. *Convergence: The International Journal of Research into New Media Technologies*, *14*(1), 13–20. http://doi.org/10.1177/1354856507084416

Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210–230. http://doi.org/10.1111/j.1083-6101.2007.00393.x

Brown, B., Chui, M., & Manyika, J. (2011). *Are You Ready for the Era of Big Data '? McKinsey Quarterly* (Vol. October).

Brownstein, J. S., Freifeld, C. C., Chan, E. H., Keller, M., Sonricker, A. L., Mekaru, S. R., & Buckeridge, D. L. (2010). Information Technology and Global Surveillance of Cases of 2009 H1N1 Influenza. *The New England Journal of Medicine*, *362*(18), 1731–1735.

Brynjolfsson, E., Hitt, L. M., & Kim, H. H. (2011). Strength in Numbers: How Does Data-driven Decision-making Affect Firm Performance? In *ICIS 2011 Proceedings* (p. 18). http://doi.org/10.2139/ssrn.1819486

BStU. (n.d.). Overview - Ministry of State Security. Retrieved from http://www.bstu.bund.de/EN/MinistryOfStateSecurity/Overview/_node.html

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of Measures of Online Privacy Concern and Protection for Use on the Internet. *Journal Of The American Society For Information Science And Technology*, *58*(2), 157–165.

Can, A. (2015). Dünyanın En Büyük SIM Kart Ureticisi Hack'lendi. Retrieved from http://www.hurriyet.com.tr/ekonomi/28258075.asp

Carter, L., & Bélanger, F. (2005). The Utilization of E-government Services: Citizen Trust, Innovation and Acceptance Factors. *Information Systems Journal*, *15*(1), 5–25. http://doi.org/10.1111/j.1365-2575.2005.00183.x

Castañeda, J. A., & Montoro, F. J. (2007). The Effect of Internet General Privacy Concern on Customer Behavior. *Electronic Commerce Research*, *7*(2), 117–141. http://doi.org/10.1007/s10660-007-9000-y

CBS/AP. (2013). NSA Can Spy On Offline Computers Wirelessly, Says Security Expert. *CBSNews*. Retrieved from http://www.cbsnews.com/news/nsa-can-spy-on-offline-computers-wirelessly-expert-jacob-applebaum-says/

Christofides, E., Muise, A., & Desmarais, S. (2009). Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? *Cyberpsychology & Behavior*, *12*(3), 341–345. http://doi.org/10.1089/cpb.2008.0226

Clarke, R. (1988). Information Technology and Dataveillance. *Communications of the ACM*, *31*(5), 498–512. http://doi.org/10.1145/42411.42413

Clarke, R. (1999). Internet Privacy Concerns Confirm the Case for Intervantion. *Communications of the ACM*, *42*(2), 60–67.

Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., & Powledge, P. (2005). Location Disclosure to Social Relations: Why, When, & What People Want to Share. In *CHI 2005 Conference on Human Factors in Computing Systems* (pp. 81–90). http://doi.org/10.1145/1054972.1054985

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). An Exploratory Study of Differences Between Internet Users ' Privacy Concerns and Beliefs About Government Surveillance : *Journal of Global Information Management*, *14*(December), 57–93.

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance - An empirical investigation. *Journal of Strategic Information Systems*, *17*, 214–233. http://doi.org/10.1016/j.jsis.2007.09.002

Dutton, W. H., & Shepherd, A. (2006). Trust in the Internet as an Experience Technology. *Information, Communication & Society*, *9*(4), 433–451. http://doi.org/10.1080/13691180600858606

Efrati, A. (2011). "Like" Button Follows Web Users. Retrieved March 24, 2015, from http://www.wsj.com/articles/SB10001424052748704281504576329441432995616

Featherman, M. S., Miyazaki, A. D., & Sprott, D. E. (2010). Reducing Online Privacy Risk to Facilitate E-service Adoption: the Influence of Perceived Ease of Use and Corporate Credibility. *Journal of Services Marketing*, *24*(3), 219–229. http://doi.org/10.1108/08876041011040622

Felt, A., Ha, E., Egelman, S., & Haney, A. (2012). Android Permissions: User Attention, Comprehension, and Behavior. In *Symposium on Usable Privacy and Security*.

Fisher, J. a., & Monahan, T. (2008). Tracking the Social Dimensions of RFID Systems in Hospitals. *International Journal of Medical Informatics*, *77*, 176–183. http://doi.org/10.1016/j.ijmedinf.2007.04.010

Fogel, J., & Nehmad, E. (2009). Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns. *Computers in Human Behavior*, *25*(1), 153–160. http://doi.org/10.1016/j.chb.2008.08.006

Foroughi, H., Aski, B. S., & Pourreza, H. (2008). Intelligent Video Surveillance for Monitoring Fall Detection of Elderly in Home Environments. *Proceedings of 11th International Conference on Computer and Information Technology, ICCIT*, (Iccit), 219–224. http://doi.org/10.1109/ICCITECHN.2008.4803020

Foucault, M. (1977). *Discipline and Punish: the Birth of the Prison*. Vintage.

Foxton, W. (2014). Uber Scandal: Worried about NSA Spying? It's Silicon Valley Billionaires You Need to Watch. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/technology/11237836/Uber-scandal-Worried-about-NSA-spying-Its-Silicon-Valley-billionaires-you-need-to-watch.html

Fuchs, C. (2011). New Media, Web 2.0 and Surveillance. *Sociology Compass*, *5*(2), 134–147. http://doi.org/10.1111/j.1751-9020.2010.00354.x

Garfinkel, S. (2001). *Database Nation*. O'Reilly Media.

George, D., & Mallery, P. (2003). *SPSS for Windows Step by Step: A Simple Guide and Reference* (4th ed.). Boston: Allyn & Bacon.

George, D., & Mallery, P. (2010). *SPSS for Windows Step by Step: A Simple Guide and Reference*. Boston: Pearson.

Gold, H. (2013). Boom in "1984" Sales in NSA Wake. Retrieved April 9, 2015, from http://www.politico.com/story/2013/06/1984-book-sales-nsa-leak-92632.html

Greenwald, G. (2013). NSA Collecting Phone Records of Millions of Verizon Customers Daily. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Greenwald, G., & MacAskill, E. (2013). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Greveler, U., Justus, B., & Loehr, D. (2012). Multimedia Content Identification Through Smart Meter Power Usage Profiles. *Computers, Privacy and Data Protection*.

Griffin, A. (2015). Sim Card Database Hacked: NSA and GCHQ Stole Details to Listen in on Phone Calls. *Independent*. Retrieved from http://www.independent.co.uk/life-style/gadgets-and-tech/news/sim-card-database-hacked-nsa-and-gchq-stole-details-to-listen-in-on-phone-calls-10058590.html

Haggerty, K. D., Wilson, D., & Smith, G. J. D. (2011). Theorizing Surveillance in Crime Control. *Theoretical Criminology*, *15*(3), 231–237.

Harris, S. (2015). Your Samsung SmartTV Is Spying on You, Basically. Retrieved from http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html

Hong, W., & Thong, J. Y. L. (2013). Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly*, *37*(1), 275–298.

Hoven, J. Van Den, & Vermaas, P. E. (2007). Nano-technology and Privacy: on Continuous Surveillance Outside the Panopticon. *The Journal of Medicine and Philosophy*, *32*, 283–297.

Hsu, M. H., Ju, T. L., Yen, C. H., & Chang, C. M. (2007). Knowledge Sharing Behavior in Virtual Communities: The Relationship Between Trust, Self-efficacy, and Outcome Expectations. *International Journal of Human Computer Studies*, *65*(2), 153–169.

In the Privacy of Your Own Home. (2015). Retrieved June 11, 2015, from http://www.consumerreports.org/cro/magazine/2015/06/connected-devices-and-privacy/index.htm

Ingram, D. (2015). NSA Sued by Wikimedia, Rights Groups Over Mass Surveillance. Retrieved March 10, 2015, from http://www.reuters.com/article/2015/03/10/us-usa-nsa-wikipedia-idUSKBN0M60YA20150310

Jha, M. N., Levy, J., & Gao, Y. (2008). Advances in Remote Sensing for Oil Spill Disaster Management: State-of-the-Art Sensors Technology for Oil Spill Surveillance. *Sensors*, *8*(1), 236–255. http://doi.org/10.3390/s8010236

Johnson, B. (2010). Privacy No Longer a Social Norm, Says Facebook Founder. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2010/jan/11/facebook-privacy

Joinson, A. N. (2008). "Looking at", "Looking up" or "Keeping up with" People? Motives and Uses of Facebook. *Chi 2008*, 1027–1036.

Juels, A. (2006). RFID Security and Privacy: A Research Survey. *IEEE Journal On Selected Areas In Communications*, *24*(2), 381–394.

Kapadia, A., Kotz, D., & Triandopoulos, N. (2009). Opportunistic Sensing: Security Challenges for the New Paradigm. *COMSNETS'09*, 127–136.

King, G. (2011). Ensuring the data-rich future of the social sciences. *Science*, *331*(6018), 719–721. http://doi.org/10.1126/science.1197872

Landau, S. (2013). Making Sense from Snowden : What's Significant in the NSA Surveillance Revelations. *IEEE Security & Privacy*, *July/Augus*.

Lane, N. D., Miluzzo, E., Lu, H., Peebles, D., Choudhury, T., & Campbell, A. T. (2010). A Survey of Mobile Phone Sensing. *IEEE Communications Magazine*, *48*(9), 140–150.

Lee, S.-H., Sohn, M.-K., Kim, D.-J., Kim, B., & Kim, H. (2012). Face Recognition of Near-infrared Images for Interactive Smart TV. *Proceedings of the 27th Conference on Image and Vision Computing New Zealand - IVCNZ '12*, 335–339.

Letouzé, E. (2012). *Big Data for Development: Challenges & Opportunities*. *UN Global Pulse*. Retrieved from http://www.unglobalpulse.org/sites/default/files/BigDataforDevelopment-UNGlobalPulseJune2012.pdf

Liao, L., Fox, D., & Kautz, H. (2007). Extracting Places and Activities from GPS Traces Using Hierarchical Conditional Random Fields. *The International Journal of Robotics Research*, *26*(1), 119–134. http://doi.org/10.1177/0278364907073775

Lin, C. E., Shiao, Y. S., Li, C. C., Yang, S. H., Lin, S. H., & Lin, C. Y. (2007). Real-time Remote Onboard Diagnostics Using Embedded GPRS Surveillance Technology. *IEEE Transactions on Vehicular Technology*, *56*(3), 1108–1118.

Lindqvist, J., Cranshaw, J., Wiese, J., Hong, J., & Zimmerman, J. (2011). I'm the Mayor of My House: Examining Why People Use Foursquare - a Social-Driven Location Sharing Application. *CHI '11 Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems*, *54*, 2409–2418.

Liu, Y., Gummadi, K. P., & Mislove, A. (2011). Analyzing Facebook Privacy Settings : User Expectations vs. Reality. *Education*, 61–70. http://doi.org/10.1145/2068816.2068823

Lyon, D. (2007). Surveillance, Security and Social Sorting: Emerging Research Priorities. *International Criminal Justice Review*, *17*(3), 161–170.

Madden, M., Rainie, L., Perrin, A., Duggan, M., & Page, D. (2015). *Americans' Attitudes About Privacy, Security and Surveillance*. Retrieved from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Malhotra, N. K., Kim, S. S., Agarwal, J., Tech, G., & Peachtree, W. (2004). Internet Users ' The Information the Scale , and a Causal (IUIPC): *Information Systems Research*, *15*(4), 336–355.

Maney, K. (2015). The Digital You Is Already Living in the Cloud, Applying for Credit Cards. Retrieved from http://www.newsweek.com/digital-you-already-living-cloud-applying-credit-cards-342565

Martin, N., Rice, J., & Martin, R. (2015). Behaviour & Information Technology Expectations of privacy and trust: examining the views of IT professionals Expectations of privacy and trust: examining the views of IT professionals. *Behaviour & Information Technology*. http://doi.org/10.1080/0144929X.2015.1066444

Marx, G. T. (2002). What's New about the "New Surveillance"?: Classifying for Change and Continuity. *Surveillance & Society*, *17*(1), 18–37.

McAfee. (2014). *Net Losses : Estimating the Global Cost of Cybercrime*. Retrieved from http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf

McAfee, A., & Brynjolfsson, E. (2012). Big Data. The Management Revolution. *Harvard Business Review*, *90*(10), 61–68.

Michael, M. G., Fusco, S. J., & Michael, K. (2008). A Research Note on Ethics in the Emerging Age of Uberveillance. *Computer Communications*, *31*(6), 1192–1199.

Miller, C. C. (2014). Revelations of N.S.A. Spying Cost U.S. Tech Companies. *The New York Times*. Retrieved from http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*(3), 15–29. http://doi.org/10.1002/dir.20009

Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., & Irwin, D. (2010). Private Memoirs of a Smart Meter. *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building - BuildSys '10*, 61–66.

Monahan, T. (2010). *Surveillance In The Time Of Insecurity*. Rutgers University Press.

Morozov, E. (2011). *The Net Delusion The Dark Side of The Internet Freedom*. New York: PublicAffairs.

Moynihan, M. (2013). Sorry We're not Living Orwell's 1984. *Newsweek*. Retrieved from http://www.newsweek.com/2013/06/19/sorry-were-not-living-orwells-1984-237604.html

Myers, J. L., & Well, A. D. (2003). *Research Design and Statistical Analysis* (2nd ed.). New Jersey: Lawrence Erlbaum Associates.

Newman, A. L. (2015). What the "Right to Be Forgotten" Means for Privacy in a Digital Age. *Science*, *347*(6221), 507–508.

Ohm, P. (2013). The Underwhelming Benefits Of Big Data. *University of Pennsylvania Law Review Online*, *161*, 339–346.

Palen, L., & Dourish, P. (2003). Unpacking "Privacy" for a Networked World. In *Proceedings of the conference on Human factors in computing systems - CHI '03* (p. 129).

Pavlou, P. A. (2011). State of the Information Privacy Literature: Where Are We Now and Where Should We Go? *MIS Quarterly*, *35*(4), 977–988.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Provide and Consumer Information Personal Privacy Concerns. *Journal of Public Policy & Marketing*, *19*(1), 27–41.

Pötzsch, S. (2008). Privacy Awareness: A Means to Solve the Privacy Paradox? *The Future of Identity in the Information Society*, *298*(216483), 226–236. http://doi.org/10.1007/978-3-642-03315-5_17

Privacy. (n.d.). Retrieved November 23, 2015, from http://www.oxforddictionaries.com/definition/english/privacy

Raab, C. (2006). Regulatory Provisions For Privacy Protection. In *The Glass Consumer* (pp. 45–67). Bristol.

Räty, T. D. (2010). Survey on contemporary remote surveillance systems for public safety. *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews*, *40*(5), 493–515. http://doi.org/10.1109/TSMCC.2010.2042446

Regan, P. M., Fitzgerald, G., & Balint, P. (2013). Generational Views of Information Privacy? *The European Journal of Social Science Research*, *26*, 1–2.

Richards, N. M. (2013). The Dangers Of Surveillance. *Harward Law Review*, *126*, 1934–1964.

Roosendaal, A. (2011). Facebook tracks and traces everyone: Like this! *Tilburg Law School Legal Studies Research Paper Series*, (03). Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563

Shade, L. (2002). Privacy. In *Encyclopedia of new media: An essential reference guide to Communication and Technology.* Sage Publications. Retrieved from http://search.credoreference.com/content/entry/sageeonm/privacy/0

Sheehan, K. B. (2002). Toward a Typology of Internet Users and Online Privacy Concerns. *The Information Society*, *18*(1), 21–32. http://doi.org/10.1080/01972240252818207

Singer, N. (2015). Sharing Data, but Not Happily. Retrieved June 26, 2015, from http://www.nytimes.com/2015/06/05/technology/consumers-conflicted-over-data-mining-policies-report-finds.html?_r=0

Slovic, P. (1987). Perception of Risk. *Science*, *236*.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: an Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989–1015.

Smith, H. J., Milberg, S. J., Burke, S. J., & Hall, O. N. (1996). Privacy : Concerns Organizational. *MIS Quarterly*, *20*(2), 167–196.

Solove, D. J. (2007). "I"ve Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review*, *44*.

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

Staddon, J., Huffaker, D., Brown, L., & Sedley, A. (2012). Are Privacy Concerns a Turn-off?: Engagement and Privacy in Social Networks. *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 1–13.

Stalder, F. (2002). Privacy is Not the Antidote to Surveillance. *Surveillance and Society*, *1*(1), 120–124.

Stamos, A. (2015). Notifications for Targeted Attacks. Retrieved October 22, 2015, from https://www.facebook.com/notes/facebook-security/notifications-for-targeted-attacks/10153092994615766

Tene, O., & Polonetsky, J. (2012). Privacy in the Age of Big Data: A Time for Big Decisions. *Stanford Law Review Online*, *64*, 63.

Timberg, C. ;Ellen N. (2013). FBI's Search for "Mo," Suspect in Bomb Threats, Highlights Use of Malware for Surveillance. *Washington Post*. Retrieved from http://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html

Toch, E., Wang, Y., & Cranor, L. F. (2012). Personalization and Privacy: A Survey of Privacy Risks and Remedies in Personalization-based Systems. *User Modelling and User-Adapted Interaction*, *22*, 203–220.

TurkStat. (2015). *Information and Communication Technology (ICT) Usage Survey in Households and Individuals*. Retrieved from http://www.tuik.gov.tr/PreHaberBultenleri.do?id=18660

Turow, J., Hennessy, M., & Draper, N. (2015). *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers And Opening Them Up To Exploitation*. *Annenberg School for Communication*.

Verble, J. (2014). The NSA And Edward Snowden : Surveillance In The 21st Century. *Computers & Society*, *44*(3), 14–20.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220.

Weber, R. H. (2010). Internet of Things – New Security and Privacy Challenges. *Computer Law & Security Review*, *26*(1), 23–30.

Welch, E. W., Hinnant, C. C., & Moon, M. J. (2005). Linking citizen satisfaction with e-government and trust in government. *Journal of Public Administration Research and Theory*, *15*(3), 371–391. http://doi.org/10.1093/jopart/mui021

Werner, C., Brown, B., & Altman, I. (2004). Privacy. In C. Spielberger (Ed.), *Encyclopedia of Applied Psychology*. Oxford: Elsevier Science & Technology.

White, A. (2014). EU Data-Retention Law Tramples on Privacy, Top Court Says. Retrieved from http://www.bloomberg.com/news/articles/2014-04-08/eu-data-retention-law-tramples-on-privacy-top-court-says

Wills, C. E., & Zeljkovic, M. (2011). A Personalized Approach to Web Privacy: Awareness, Attitudes and Actions. *Information Management & Computer Security*, *19*(1), 53–73.

Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and Consequences of Consumer Online Privacy Concern. *International Journal of Service Industry Management*, *18*(4), 326–348.

Wolf, N. (2012). The New Totalitarianism of Surveillance Technology. *The Guardian*. Retrieved from http://www.theguardian.com/commentisfree/2012/aug/15/new-totalitarianism-surveillance-technology

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting User Concerns About Online Privacy. *Journal Of The American Society For Information Science And Technology*, *58*(5), 710–722.

Young, A. L., & Quan-Haase, A. (2009). Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook. *C&T '09*, 265–274.

Youyou, W., Kosinski, M., & Stillwell, D. (2014). Computer-based Personality Judgments are More Accurate Than Those Made by Humans. *PNAS*, *112*(4), 1–5.

Zimmer, J. C., Arsal, R. E., Al-Marzouq, M., & Grover, V. (2010). Investigating Online Information Disclosure: Effects of Information Relevance, Trust and Risk. *Information and Management*, *47*(2), 115–123.