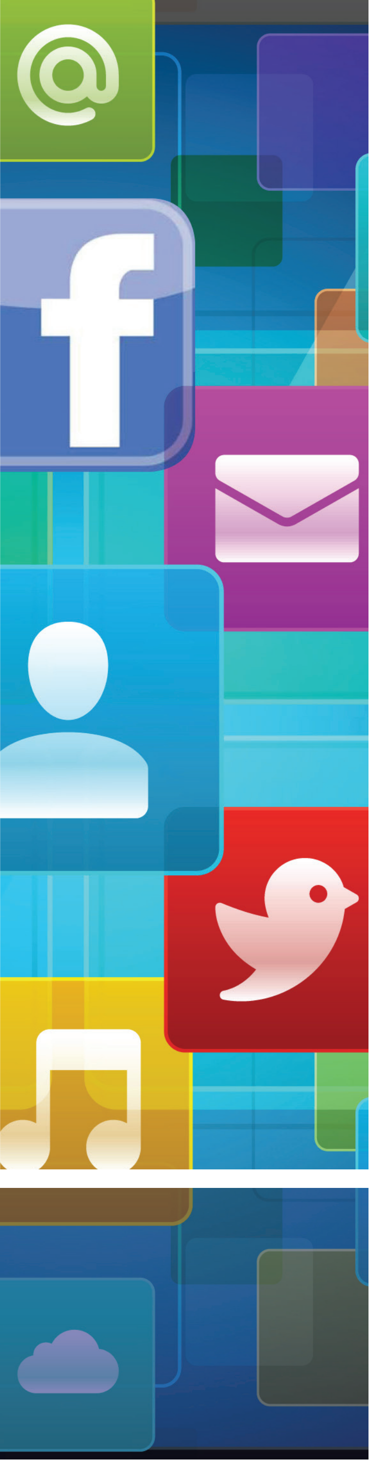

Digital and Social Media Marketing and Advertising Collection

Victoria L. Crittenden, *Editor*

Digital Privacy in the Marketplace

Perspectives on the Information Exchange

George R. Milne

BEP BUSINESS EXPERT PRESS

Digital Privacy in the Marketplace

Digital Privacy in the Marketplace

Perspectives on the Information Exchange

George R. Milne
Professor of Marketing,
Isenberg School of Management,
University of Massachusetts Amherst

BEP BUSINESS EXPERT PRESS

First published in 2015 by
Business Expert Press, LLC
222 East 46th Street, New York, NY 10017
www.businessexpertpress.com

ISBN-13: 978-1-60649-848-4 (paperback)
ISBN-13: 978-1-60649-849-1 (e-book)

Business Expert Press Digital and Social Media Marketing and Advertising Collection

Collection ISSN: 2333-8822 (print)
Collection ISSN: 2333-8830 (electronic)

Cover and interior design by S4Carlisle Publishing Services Private Ltd., Chennai, India

First edition: 2015

10 9 8 7 6 5 4 3 2 1

Printed in the United States of America

Dedication

To Shalini, who came from the land of little privacy.

Abstract

This book examines digital privacy in the marketplace. It focuses on the data exchanges between marketers and consumers, with special attention to the privacy challenges that are brought about by new information technologies. The purpose of this book is to provide a background source to help the reader think more deeply about the impact of privacy issues on both consumers and marketers. It covers topics such as: why privacy is needed, the technological, historical and academic theories of privacy, how market exchange affects privacy, what are the privacy harms and protections available, and what is the likely future of privacy.

Keywords

Privacy, Information Exchange, Technology, Privacy Harms and Protections, Future of Privacy

Contents

Introduction

The information environment in which marketers and consumers operate is growing in complexity every day. New technological innovations have the accelerated the exchange of information between marketers and consumers, resulting in numerous privacy problems. Examples of such technologies that cause privacy problems include prediction models that identify pregnancies before families get to know, glasses that can take pictures of people unobtrusively in public, tracking software in phones that can be used to observe consumers movements throughout cities and within stores themselves, and facial recognition software that can be used to match consumer images with databases to identify individuals in public spaces. These advances raise the question of whether privacy is at all possible.

Managing the new information environment is akin to trying to drink water from a fire hose (Perreault 1992). There is simply a lot of data available. Data, when combined with other data, become information, and its value increases (Data and information are used interchangeably throughout this book). With the proliferation of new information technologies, marketers have access to more information than ever about individual consumer's purchase behaviors, their online browsing behaviors, and their social lives that they willingly document on social networks. Data mining and modeling techniques are helping marketers to connect disparate pieces of information about consumers together to create accurate purchase intention profiles. These developments can help marketers be more successful in "understanding what consumers want," but these actions also bring up privacy concerns.

It is imperative for marketers to address privacy concerns because not dealing with them can have negative impact on their market performance. In the current environment, the access and flow of information among consumers and businesses is creating tremendous opportunities and a foundation for economic growth. Yet, privacy concerns are not going away and in fact will continue to grow in severity. How privacy issues get resolved will have a direct impact on the economy. In order to reap the benefits of the big data environments and to protect consumer interests, it will be necessary for marketing managers to create information exchanges that at the same time preserve consumers' legitimate needs for privacy.

The Purpose of the Book

This book examines the privacy problem from both consumers' and businesses' perspectives. To address these issues, this book focuses on the data exchanges between marketers and consumers, with special attention to the privacy challenges the data exchanges present for both marketers and consumers. The perspective offered recognizes that information exchanges are beneficial to both businesses and consumers. Information helps businesses improve their marketing efforts and helps consumers have access to information to make better purchase decisions. At the same time, there are technological and marketplace developments that heighten the need to put more attention toward protecting information privacy. Advancements in information technology are happening at a pace that, without proper supervision or regulation, are creating privacy violations that end up offsetting the efforts of both businesses and consumers to benefit from the information exchanges.

To better understand the privacy dilemmas brought about by the new technologies, this book serves as a background source to help the reader think more deeply about how privacy issues affect both consumers and marketers. It covers topics such as why privacy is needed, the technological historical and academic theories of privacy, how market exchange is tied to privacy, what are the privacy harms and privacy protections available, and what is the likely future of privacy.

A core feature of the book is the review of the information exchange process, where the inhibitors and promoters of the process are highlighted. The book concludes with the importance of marketers and consumers reaching mutually agreed upon norms of behavior to eliminate the creepy and damaging marketing practices that are occurring today. It offers suggestions for change, including a call of putting privacy in the forefront of education and business practices.

The specifics of the following chapters are as such. In Chapter 1, the information environment and the privacy problem is reviewed, which is created by markers and consumers differing expectations for technology use. In Chapter 2, the question of whether privacy is dead is examined and privacy is reframed in terms of social norms. Then there is a review of the reasons why both consumers and marketers need privacy. In Chapter 3, there is a review of the history of privacy and technologies and an explanation of key modern academic theories of privacy that apply to the business world. The theoretical theories inform how marketers and consumers negotiate information exchanges that meet data and privacy requirements. In Chapter 4, privacy in the market place is discussed. Here, the role of social contracts is discussed within the context of the influencing factors attributed to marketers and consumers. Next, in Chapter 5, there is a review of privacy harms and a discussion of the marketing technologies that can lead to these harms. Following, in Chapter 6, there is a review of the forms of privacy protection offered through legal, self-regulatory, and technological avenues. In Chapter 7, the final chapter, there is a discussion about the direction privacy protection is likely to take in the future, a discussion of the creepy actions taken by marketers, recommendations for the establishment of mutually agreed upon norms between marketers and consumers, and suggestions for improving the role of privacy education and business practices.

CHAPTER 1

The Information Environment and the Privacy Problem

Chapter Overview

In this first chapter, you will learn about the data-driven marketing information environment, the personal data ecosystem, how technology is facilitating the collection and dissemination of information, and how the different privacy expectations for technological use are creating a privacy problem between marketers and consumers.

The Information Environment

We live in an information economy that is based on accessing and utilizing information from market exchanges. The acquired information is used by both consumers and businesses to make better decisions in the marketplace. In many respects information exchange, in our digital world, is the currency of the modern market economy. Every moment as consumers, we have access to a constant flow of digital information on our phones and computers that we use to make daily decisions including purchases. Although we are aware of exchanging money for goods and services during the time of purchase, there is a less recognized second exchange at this time, where information about consumers is provided to marketers and information about marketers and their goods and services is provided to consumers (Culnan and Milberg 1998). Moreover, there are many other information exchanges that occur that are not directly tied to purchasing; they are simply a function of having an online presence. While the flow of data from consumers to marketers is sometimes intentional, other times it is not, with consumers unaware of the data collection.

Indeed, the information exchange process benefits both consumers' and marketers' market transactions. Consumers, for example, gather and review information about marketers and the product and services they are considering purchasing either online or in stores. Using Internet technologies, consumers can easily compare competing products features, obtain reviews, and ask questions of other customers prior to buying. They also have the ability to get answers to post purchase consumer service questions from both marketers and other consumers. Marketers, on the other hand, use the Internet to access information about consumers and their preferences so they can better gauge demand. Information is used to tailor offers that best appeal to market segments, which in many cases are the size of one. Undoubtedly, having access to data helps marketers be customer oriented, which is the basic foundation of the marketing discipline.

Data-Driven Market Economy

Privacy issues aside for the moment, the information rich environment is seen by many marketers and policy makers as a good thing. It has been acknowledged that data driven marketing is a major source of growth for the U.S. economy. A 2013 study (Deighton and Johnson 2013, p. 1) finds that the data-driven marketing economy is adding $156 billion in revenue to the U.S. economy and contributed to 675,000 jobs in 2012. The data-driven economy is comprised of middlemen that gather and manipulate individual level data and supply the processed data to other firms for their marketing efforts. Concurrently, the influx of data has resulted in the United States leading the world in having data scientists in being able to model consumer behavior sophisticatedly. This enhanced targeted information based on data mining is sold to marketers who want to improve their marketing capabilities. Estimates have these marketing exchanges projected to account for up to 70 percent of the economic impact of the data driven economy (Deighton and Johnson 2013).

The authors of the 2013 study suggest that their findings are conservative and the economic impact could be larger since they focused on expenses and not benefits. The innovation of data-driven marketing has provided substantial benefits to many businesses. Due to the availability of data, small businesses and start-ups have low barriers to entry. Advertising is easier and access to consumers continues to grow with the growth of ecommerce. Competition in markets is also increasing as businesses are forced to be more consumer centric. Start-ups that deliver such value are able to compete effectively with big established businesses. Overall this leads to more efficient markets, making the process of marketing more efficient—with pin point segmentation, targeting, and measurement. All of this ultimately benefits the consumer by offering them more targeted choices.

Personal Data Ecosystem

Personal data is data about consumers. It can be *individually provided* by consumers through photos, blogs, e-mails and tweets, or through online transaction data, such as a job application or registration for a website. It can be *observed* through internet browsing records, surveillance videos, location data from cell phones, or detailed call records. It can be *inferred* through credit scores, consumer profiles, predictive traffic flows, and targeted advertisements. Of interest is that fact that collection of observed and inferred data is increasing the fastest and is being acquired without consumers being aware.

The personal data ecosystem is a network of businesses that collects and processes personal consumer data and uses it to target consumers with marketing and other actions. This ecosystem, which contains consumer personal data, functions because of data exchanges among:

- Data collectors (sources),
- Data brokers, and
- Data users.

While most people are aware of data collectors and data users, the role and sheer number of data brokers that exist are not well understood. Figure 1.1, adapted from the FTC report, "Protecting Consumers in an Era of Rapid Change," highlights the various entities that are involved in the personal data collection and dissemination business (Federal Trade Commission, 2012).

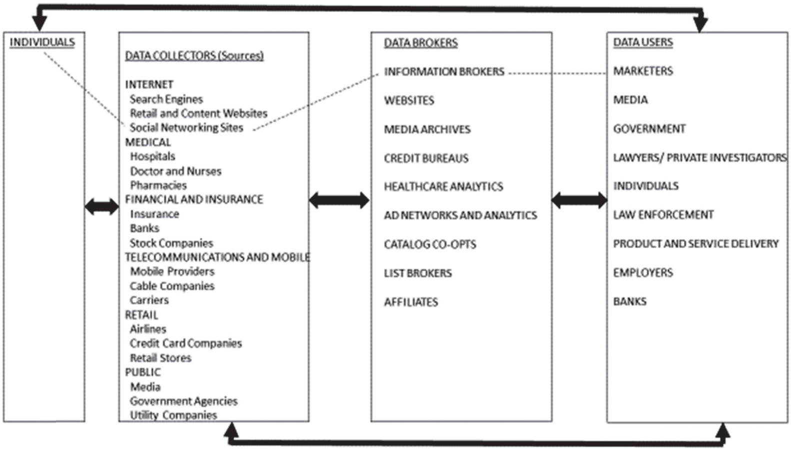

Figure 1.1 The personal data ecosystem

Figure 1.1 shows the path of how an individual's data get acquired by companies who use the data. One path is shown by the solid black lines that indicate data from individuals are acquired by data collectors who then pass it on to data brokers and then to data users. Other paths show data transfers between consumers and data users as well as between data collectors and data users. The ecosystem is complex in that for data collectors, data brokers, and data users, there are many sectors and actors. As a more specific example, the figure shows dashed lines that indicate data is collected from social media networking sites that forward the data to information brokers, who then repackage the data to pass it on to marketers who use the data for targeting and advertising purposes. While only an abstraction of some major types of organizations in the data ecosystem, the figure nonetheless illustrates that there are many organizations in the data environment that are working behind the scenes of most consumers' knowledge.

Data Collectors and Sources of Data

As shown in the figure, the sources of the data used by the data collection come from the following sectors:

- Internet,
- Medical,
- Financial and insurance,

- Telecommunications and mobile,
- Retail, and
- Public sector.

The sectors shown in the figure are known for their information intensity. The data available in these sectors is of value to marketers because gathered data can enhance the marketers' efficiencies, effectiveness, and provide new income streams.

As an illustration, marketers are much interested in digitized medical data, as well as financial and insurance data. Websites that collect data about the consumers who seek content on diseases and loan rates are able to sell and transfer this data to companies looking for leads. Data from the telecommunications and mobile industries is also sought, not only for the communication patterns based on smart phone usage but also from geographical positioning information transmitted by the phone. Retail data, both offline and online, is sought by marketers to help customize and target future communications with consumers. Finally, many marketers are able to gather data from public records, such is the case from the real estate industry and court records. Both marketers and consumers use People finder services, which aggregate much of the public data and make dossiers on people available for sale. Increasingly, across all these data sources the data is observed or inferred. This suggests that a great amount of data is acquired through various data collectors without consumer awareness.

In addition to the lack of consumer awareness, some of the data gathered can be quite sensitive. In the medical sector, there are lists that contain sensitive information such as genetic diseases sufferer's lists, dementia sufferer's lists, Aids and HIV infection sufferer's lists, and the addictive behaviors, alcohol and drugs mailing list (Dixon 2014). Similarly, data from financial lists, such as the Derogatory Credit Consumers mailing list, can be harmful to consumers. Data from insurance lists can reveal lifestyle characteristics. Even data gathered from public records can be problematic for individuals who wish to keep their lives private. In these situations, consumers find it difficult and costly to remove their names from online white pages and in the end may find it nearly impossible (Labrecque et al. 2012).

Data Brokers

Across all these information sectors, there are data brokers—the hidden layer that is generally unknown to consumers. Data brokers function as middlemen to aggregate and compile data in a usable form to sell to data users. They can be classified in terms of:

- Information brokers,
- Websites,
- Media archives,
- Credit bureaus,
- Healthcare analytics,
- Ad networks and analytics,
- Catalog co-opts,
- List brokers, and
- Affiliates.

Data brokers are in the position to gather data and repackage and resell it to others. Data brokers (also referred to as Information brokers) collect and sell information used for targeted ads, market research, and customer scoring. Their customer files and contact information are often sold in lists, which are organized by demographics or behaviors. It is estimated that there are between 3,500 and 4,000 data broker companies (Dixon 2014). While this industry has a few large companies, such as Acxion, there is a very long tail of many other smaller companies. Interestingly, the business models of data brokers vary considerably. For example, Acxion, a very large data broker, hosts some of its own data collection and also buys original data. Other companies, such as Datalogix, primarily score existing consumer data. Others, like Itellius, sell data online. Broadly speaking, the activities of data brokers include list brokering, data analytics, predictive analytics and modeling, scoring, CRM, online, offline, APIS, cross channel, mailing preparation, campaigns, and database cleansing (Dixon 2014). In their 2012 investigation of data brokerage companies (FTC to Study Data Broker Industry's Collection and Use of Consumer Data, 2012), the FTC focused on nine: (1) Acxiom, (2) Corelogic, (3) Datalogix, (4) eBureau, (5) ID Analytics, (6) Intelius,

(7) Peekyou, (8) Rapleaf, and (9) Recorded Future. These represent some of the largest and well-known companies. Nonetheless, there are many others.

The data gathered by the data brokers are gathered from public and non-public sources and often are resold to other data brokers and eventually to end users. In turn, these users will incorporate the purchased data in the target marketing and data processing activities. Besides marketing efforts, the uses of data include processing records to determine eligibility or whether the records need to be suppressed and specific processing algorithms for authentication, anti-fraud detection, and identity verification, and back ground lifestyle checks. The algorithms for these techniques rely upon a range of data including proxy credit scores and medical data (Dixon 2014). Of concern to privacy advocates is the use of proxy scores, which is an approach to circumvent existing privacy laws. This practice is unfair, in part to the difficulty for consumers to opt out of the data compilation reports and the lack of consumer rights and knowledge of consumer scoring algorithms that are used to make decision about the type of relationship consumers have with data users.

Data Users

According to the FTC ecosystem, the data users include:

- Marketers,
- Media,
- Government,
- Lawyers/public investigators,
- Individuals,
- Law enforcement,
- Product and service delivery,
- Employers, and
- Banks.

Data users rely on information to create efficiencies and more effective decision making. Some examples include marketers use GPS location transmitted by cell phones to send geographically targeted advertisements, media companies help websites serve up advertisements targeted to individual consumers based on the past websites they visited, the government monitors social media and phone communications for national security, individuals check out other individuals prior to meeting them the first time on social and work occasions, law enforcements use predictive analytics to determine prisoner paroles, delivery companies use GPS for improving deliveries, employees track keystrokes to measure employee productivity, and banks track credit card usage to thwart fraud. To date much of the focus has been on the data users. However, as apparent through seeing the data ecosystem, there are many parties involved in the collection, trading, and use of information.

In response to this unregulated data ecosystem, the FTC report suggested that data brokers need to make disclosures with regard to type of data they collect and sell. These include (1) the nature and source of information, (2) the use, maintenance, and dissemination of information, and (3) whether consumers have a chance to correct erroneous information. Not surprisingly, the industry lobbyists are trying to stop such requirements citing it would be too cumbersome and expensive to implement. Whether or not this suggestion eventually is enacted into law, there are reasons for both marketers and consumers to be aware of the information flows that are occurring.

The studies, Data Driven Marketing and the FTC Report on Privacy, suggest two important points. First, that data driven marketing will continue to grow and prosper. Second, given the externalities of privacy issues that continue to be raised in public discourse and by regulatory bodies, it is incumbent on both marketers and consumers to better understand the ramifications of information exchange.

Technology Is Facilitating Information Exchange

It is apparent that technology is rapidly providing businesses and consumers with abundance of information, and, at the same time, creating an information environment where it is challenging to keep track of how information is collected and shared. Marketers and consumers are constantly presented with new technologies to use and help facilitate the exchange of information with each other. This includes hardware advances from laptops, tablets, mobile phones, and watches to software advances including social networks, cloud-based software, and mobile apps. However, the acceptance and understanding of the appropriate use of such technologies is not always widely embraced or understood. Research has shown that the acceptance of marketing focused on information technologies is very asymmetric, with businesses being earlier adopters and some segments of consumers lagging in their acceptance and understanding of the privacy implications (Milne and Bahl 2010). Once the ramifications and implications of the new information technologies are understood, this mismatch in expectations causes dissatisfaction about the information exchanges. What is occurring is a scene akin to the Mad Magazine's spy versus spy comic (Spy vs Spy 2010), where each side would try to innovate to outsmart the other. In this case, some marketers are introducing new technologies to covertly access consumer information and some lead consumer advocates are introducing privacy enhancing technologies to thwart these efforts. The problem is that this just leads to innovation that is destructive to the relationship. Right now, the marketers seem to have the upper hand in this escalation of new information technologies.

One recent example where information asymmetry has existed is social media technology. The social media sector is an area where historically there is much miscommunication. Even today, many users of social media are not aware of the extent that data provided by consumers is shared with marketers. This is due, in part, to unclear user agreements provided by companies and consumers' difficulty in understanding or keeping up with the privacy settings. It is also due, in part, to consumers' indifference toward information exchanges between social media companies and consumers.

While the shift to online commerce continues to grow, it was the growth of social media that has fueled the explosion of personal data that is contributed by consumers themselves. In many cases, consumers are not fully aware of the consequences of sharing personal photos, personal profiles on Facebook, and tweets. As of October 2012, the number of monthly active users of social media passed one billion. There are seven petabytes of photo content added to Facebook monthly, 300 million new photos added daily. There was an average of 175 million tweets sent every day in 2012 (Internet 2012 in numbers 2013). The availability of this new type of information is giving marketers and consumers the opportunity to learn more about each other than ever before.

The flood of data through technology is also giving consumers and marketers access to information throughout the day. Consumers, whether they are at home, at work, or out in public, are connected through their mobile phones, tablets, and laptop computers. At the end of 2012 there were 6.7 billion mobile subscribers and 1.1 billion of those were smart phone subscribers (Internet 2012 in numbers 2013). These technologies not only provide consumers access to information wherever they go but also provide marketers expanded access to consumers through their day. The consequences of this technological shift is that the boundaries between private and public space have eroded, creating a loss of anonymity. No longer is it possible to get lost in the crowd. With the pace of technological change, it is very difficult to understand where the boundaries are that a consumer will not be observed and what marketers should not examine.

At an increasing accelerated rate, new information technologies are facilitating the tracking of consumers. Examples include GPS monitoring, facial recognition, and biometrics. As these product features start to become mainstream, the implications for information exchange benefits and the downsides for privacy protection are starting to be explored. One of the newest developments is that information about consumers is being captured and transferred to other marketers by their machines (Scoble and Isreal 2013). The Internet of Things is comprised of sensors in products, which produce additional data on consumer behavior. For example, our cars are gathering information about our driving habits and making them available to insurance companies. Smart grids are monitoring out electricity consumption. Appliances are reporting to manufacturers when parts are malfunctioning. With their smart phones, consumers are able to operate many of their appliances in their house remotely.

What They Know

Consumers have long been in the dark about marketers' ability to gather information. Much light was shown on this topic by the *Wall Street Journal*, which in 2010 wrote a series of articles in a series called What They

Know (n.d.). As part of this investigative reporting, the *Wall Street Journal* conducted a study that showed how the web was becoming a gold mine of information to marketers. To show how businesses were spying on American consumers they measured marketers' use of cookies and surveillance technologies for tracking consumers. They found the top 50 websites, representing 40 percent of webpages viewed in the United States, installed an average of 64 pieces of tracking equipment, often with no warning to consumers. Overall, these 50 websites placed 3,180 tracking files into the computer that was used for testing. One-third of the tracking files were harmless (i.e., used to remember passwords); however, the other two-thirds were not and were used to help businesses track online consumers and create consumer databases (Angwin 2010).

The *Wall Street Journal* series, which ran for three years, went on to report on the intersection of corporate and government surveillance. It later reported on the ubiquitous surveillance of everyday mundane activities that are becoming the defaults.

While the unknown collection of data is disturbing, it is the use of the data that is the big story. One specific case that highlights the extent to which marketers can leverage customer data to anticipate consumer behavior is the case of Target (Duhigg 2012). A few years ago, Target was busy building pregnancy prediction models using historical data from their pregnancy registry tied to consumers shopper IDs. The idea was that if a person could be identified early enough in the pregnancy stage, they could provide the expectant mother coupons which then would establish a habit for the mother to buy all her baby and child related items from Target. As a result of the modeling, they found that pregnant women in the first 20 weeks bought a lot of zinc and calcium. They also found that pregnant women were purchasing lotions without scents.

Because Target's prediction models were quite accurate, they did not want their communications to announce "Congratulations on your first child." Even if this was within the law, it would creep out consumers. Instead, they interspersed coupons for baby items with other coupons. However, in one particular case this did not work well and despite their intentions ended up being very creepy.

One day a man in Minneapolis, whose family had received coupons for baby items, went into a Target and demanded to see a manager. He was incensed that his teenaged daughter, who was in high school at the time, was receiving coupons for baby clothes and cribs. He accused Target of trying to encourage her to become pregnant. The manager apologized and was not aware of the database efforts. When the manager called the upset customer a few days later to apologize, the customer ended up apologizing to the store manager. The customer in the interim had found out that his daughter was indeed pregnant. Target's predictive model had correctly identified this girl as pregnant based on her purchasing patterns. Nonetheless, this story puts into question when are actions are too creepy. The fact that a database marketers know, even before the daughter's family knew that she was pregnant, begs the question of is there any privacy left?

The Privacy Problem

With so much data driven by new and improved information technologies and the emerging data-driven economy, consumer privacy is being eroded at an increasing rate. Not only is more data available, but it is easily stored and is being combined with other data that enables marketers to know more about consumers than they are comfortable sharing. A privacy problem exists because there is a mismatch of expectations between marketers and consumers (see Figure 1.2). Marketers, not knowing where the line of consumer expectations exists, often cross it and engage in actions that consumers and other observers find creepy. Marketers cross the line because they are enamored with the benefits of the technology to help them understand the consumer better without considering the circumstances of such actions. Marketers might not understand that some consumer groups are more vocal that others which may lead to a negative public reaction.

Figure 1.2 illustrates that there is a mismatch between the amount of information that a consumers wants to keep private opposed to whether a marketer should have access to any of this information. If an equilibrium was reached the marketers would only access the information that the consumer was making public. However, the problem is that technology is giving marketers access to most of consumers' digital information. As a consequence, consumers are often not aware of this capability or of marketers collecting the information. When they are aware, there is generally

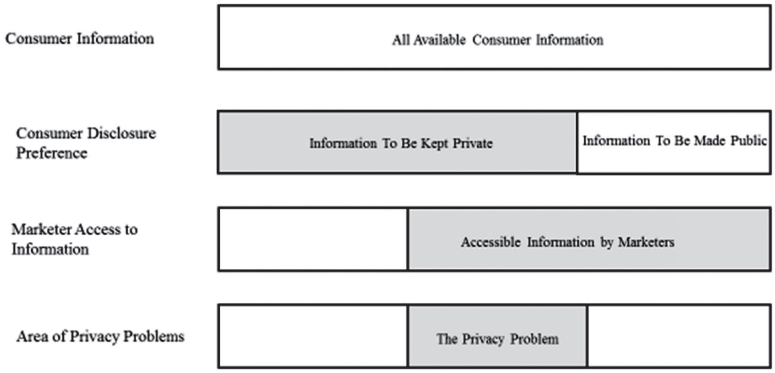
Consumer Information
All Available Consumer Information
Consumer Disclosure Preference
Information To Be Kept Private
Information To Be Made Public
Marketer Access to Information
Accessible Information by Marketers
Area of Privacy Problems
The Privacy Problem

Figure 1.2 The privacy problem

not a process for them to conveniently control access to, or restrict the use of, the information.

When the privacy line is crossed, consumers are harmed through disclosure of information they wanted to keep private. Their personal self-boundaries are crossed and their lives are interrupted. Such violations can lead to psychological, social, financial, and physical harms. These harms can occur when marketers miscalculate in the areas of information collection, processing, and dissemination as well with customer contact (Solove 2007). Marketers also have a privacy problem in that they also want to create a positive reputation for dealing with consumers. When marketers do not safeguard data or act in a manner that violates consumer trust, this can result in market place or potential legal harms. Market place harms are due to shifting customer preferences or other competitors exploiting the privacy misstep. Legal harms can include fines from the FTC and cease and desist orders.

Chapter Summary

The data ecosystem helps drive the data-driven economy. It is comprised of data collectors, data brokers, and data users who engage in data exchanges. If the economy is to continue to grow and prosper, both marketers and consumers need to address privacy issues surrounding the data exchanges. The challenge is that with technology accelerating the rate of data collection and exchange, there are asymmetric expectations between marketers and consumers about the level of privacy control needed. The privacy problem lies in this mismatch of expectations. Marketers, through the use of these technologies, are able to learn more about and communicate with consumers with pinpoint accuracy. Because of this, many have argued that privacy is dead.

Because of the benefits of protecting privacy for consumer and marketers, it is important to redefine expectations and undergo procedures to protect privacy in the future. Consumers have a need to control the collection and dissemination of sensitive information. Privacy is required by consumers for creativity, protecting communications in relationships, and maintaining their human dignity and freedom. Marketers should be concerned about consumer privacy in order to maintain customer trust, avoid media harm, avoid legal issues, and to gain a competitive advantage. The purpose of the remaining book is to examine the privacy problem from both consumer and marketer perspectives and present an argument for the development of new norms of behavior by both parties.

CHAPTER 2

Why Privacy Is Needed

Chapter Overview

In this chapter, you will consider claims that privacy is dead and why the maintenance of privacy is important to the marketplace of information exchange. You will also learn about why consumers need privacy and why it is in marketers' best interests to provide privacy protection.

The Death of Privacy?

In 1999 Scott McNealy, the CEO of Sun Microsystems, commented to the press that "You have zero privacy anyway, get over it." This resulted in sharp reaction from other industry observers who thought his normative comments would affect consumer behavior. The director of the Bureau of Consumer Protection at the Federal Trade Commission (FTC), Jodie Bernstein, commented that, "Millions of American Consumers tell us that privacy is a grave concern to them when they are thinking about shopping online." Sprenger (1999) noted Bernstein felt that McNealy's remarks were out of line. Indeed, these comments created a firestorm of strong reactions from other businesses and industry commentators.

Up to this point, the public naïvely bought into the perception of Internet anonymity represented by the iconic cartoon "On the Internet, nobody knows you are a dog." This naivety eroded a decade later for when one was online, others not only knew whether you were a dog or not, but the type of breed as well.

As the years passed, McNealy's often misaligned remarks went from being inappropriate to prophetic. Indeed, he was not being normative but describing the situation of what was or was soon to be. This has become readily apparent in the era of social media. The problem with social media technology that compromises consumers' privacy is that many consumers were operating under the assumption that there was anonymity or information was just to be shared among friends.

In an interview with Bosker (2010), Facebook creator Zuckerman suggested that privacy was no longer a social norm. "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time . . . We view it as our role in the system to constantly be innovating and be updating what our system is to reflect what the current social norms are." Such a comment is an example of powerful interests trying to convince the masses that privacy is not an issue. However, those who claim privacy is dead are often those who have the best interests for it to be dead. Like reactions to McNealy's comments 14 years prior, there were calls for the public to take action. Consumer advocacy groups are countering the claims by Zuckerman and are keeping this issue in front of the public. An example of this is the website called Youhavezeroprivacy.com with the mission to convince people that instead of simply giving up, they need to try to fight back and be aware. Advocate organizations feel that privacy is still possible today.

Toward a Redefinition of Privacy and New Behaviors

The reach of businesses into the private lives of consumers has expanded through the use of information technologies. With this expansion, there is a growing awareness that privacy rights must be attended to or they will not exist in the near future. There is no turning back the clock of technology, but there is discussion that new norms need to be adopted and levels of respect between users of information given. Because information exchange is central to our economy, it behooves both consumers and marketers to make adjustments in behavior.

Ironically, such recognition of new approaches for handling information has extended to Mark Zuckerberg's sister Randi (Hill 2012). At a holiday gathering in 2012, Randi had taken pictures of her sisters trying out a new Facebook app on their phones at a family gathering. She posted this on her Facebook (to her supposed friends). One of these was a mediate, who subscribed to Zuckerman's feed, and assuming the photo was public, posted it on Twitter to her 40,000 followers. Well, Randi was angry. Observers were quick to point out that the slip up was due to Facebook's confusing privacy settings. However, the lessons learned from Randi's privacy invasion can be summed up by Randi Zuckerman's tweet: "Digital etiquette: always ask permission before posting a friend's photo publicly. It's not about privacy settings, it's about human decency."

Both the incorporation of better privacy settings and an accepted level of online behavior would help provide privacy in the case of Randi. Such lessons can also be expanded to other information exchanges whether among consumers or among consumers and marketers. There is no shortage of examples where companies are felt by consumer groups to have gone too far. New norms for information sharing need to be adopted by consumers. Marketers need to be aware of potential asymmetries between their and their consumers understanding of how technology can be used to collect consumer information as well as protect it. When asymmetries exist, marketers should take actions to reduce them since maintaining privacy benefits both consumers and marketers. The reason for the change in behavior by marketers is that consumers need and want privacy. This need and desire for privacy, as discussed next, has not gone away even if consumers sometimes act indifferent.

Why Consumers Want/Need Privacy

Control Sensitive Information

Consumers have a need to control the flow of their information because they do not want sensitive information getting in the wrong hands and creating financial, physical, psychological, and social harm. While sensitive information for one person may be different than another, almost everyone has a line between what sensitive information they will disclose and what they will not disclose. For those who suggest they do not want to keep anything private and have nothing to hide, most of them are liars. Ask them for their bank account number, social security numbers, passwords, and e-mail account and see what their reactions are.

Some of the most sensitive information can include financial information, health information, computer passwords, and personal identifying information. The financial and health information is so sensitive that there are privacy laws regulated these industries (Gram Leach Blily Act and for regulation of financial information and the Healthcare Insurance Privacy Protection Act for medical information). Personal identifying information is considered private because identity of individuals can be stolen or lives interrupted with intrusions. There is a controversy as to what constitutes personal identifiable information (PII). PII has been defined by the National Institute of Standards and Technology (NIST) (McCallister, Grane, and Scarfone 2010) as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." More broadly, PII is information that can be used to identify or locate a single person in context.

Because information is sensitive, consumers will use discernment in deciding who will get what information and under what conditions. Table 2.1, based on consumer research (Milne, Gabisch, Markos, and Phelps 2012), shows the relationship between how sensitive particular types of information is and how likely consumers are to provide it to marketers. As shown in the table, there is an inverse relationship between the type of information consumers find sensitive and what they are willing to share with marketers. At the extreme, the lowest willingness to share is demographic information that has low sensitivity. The interesting categories are the medium willingness/high sensitivity category that includes cell phone number and IP address, and the medium willingness/medium sensitivity that include GPS and Face image. Consumer evaluation of these technologies may change as marketers use these information types more and more in their tracking and marketing efforts.

Recent research (Markos 2010) has suggested that the audience who views the information affects the perceived sensitivity of the information. For example, depending on the type of information, there are differences in a consumer's likelihood to disclose information to strangers, friends,

Table 2.1 Information sensitivity and willingness to provide for different information types

	Low willingness	Medium willingness		High willingness
High Sensitivity	Financial accounts	Digital signature	Home phone	
	Passwords	Credit score	Home address	
	Social security #	Voice print		
	Health insurance #	Mothers maiden		
	Credit card #	Name		
	DNA profile	Medical history		
	Fingerprint	Cell phone		
	Driver's license #	IP address		
	VIN #			
	Law enforcement record			
		License plate #	Document of grievance	
Medium Sensitivity		GPS location	Social network profile	
		Handwriting sample	Signed petition	
		Picture-Face	Place of birth	
			Online screen name	
			Income level	
				Weight
Low Sensitivity				Zipcode +4
				Sexual preference
				Political preference
				Religion
				Height
				Occupation
				Race
				Number of children

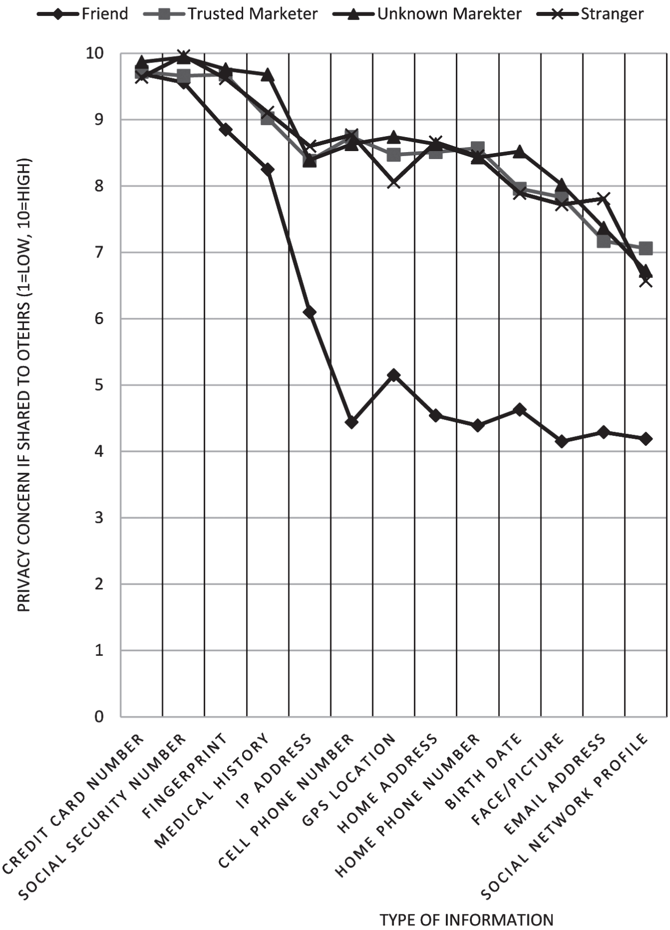

Figure 2.1 Privacy concern if shared to others

and marketers. Figure 2.1 shows the level of information sensitivity for 13 pieces of personal identifying information that would be shown to either friends, unknown marketers, trusted marketers, or strangers. The data reveal that the type of audience matters when deciding to disclose information. Overall, with exceptions of the most sensitive information, consumers were much more willing to share sensitive information with friends than with marketers (trusted and non-trusted) and strangers. Intuitively we would expect information to be considered sensitive for all viewers of credit cards, social security number, finger prints, and medical history. However, information is considered less sensitive if shared with friends than businesses. Not surprisingly, this is the case for phone numbers, GPS, and other contact information.

Consumers also consider some of their purchasing behavior private. While it might be apparent that consumers, due to social norms, would want to keep deviant behaviors, such as pornography, street drugs and prostitution, private, research (Goodwin 1992) has shown that consumer will also choose to keep some non-deviant consumption private. There are some consumptions, such as cosmetics, tobacco and liquor products, lingerie and underwear, that if revealed might cause the person embarrassed. For example, if the smoking of cigarettes was revealed, this information about one's actual self does not align with the ought self of the individual. Revealing this information might cause ridicule, criticism, embarrassment, agitation, or the disappointment from others. Thus, consumers will seek privacy to reduce the internal conflict that arises from these self-discrepancies.

Creativity

Creativity requires a safe zone where new ideas can be explored and new ways of doing things tried. Privacy removes the naysayers and the negative feedback that can squelch creative activities. Indeed, privacy is needed to give one the right to experiment, to try out new activities without the purview and judgment of others. This creates a safe space to think out of the box and try something new, which may seem crazy to others. Oftentimes when people are trying something new or learning something, they fail at the early stages. With YouTube and tutorials available, there is ample opportunity to try something new. People can learn new skills that may extend themselves and be out of their comfort zones. This is consistent with the trend toward independent self-learning. Privacy provides individuals the protection to practice unobserved before they are ready to publically display their new skills. It provides an environment where one is not judged.

Protected Communication in Relationships

Protected communication is needed to create trust, honesty, and to maintain one's dignity. As such, privacy is expected in several relationships in society, (e.g., law, financial and health arenas). People want to be able to tell their lawyers, advisers, therapists, and doctors information that is not shared with others. If one could not talk confidentiality to these people, be the full value of the relationship would not be realized. There needs to be a level of trust where clients can be open up and be fully forthcoming with information so that they can receive the maximum amount of help. Communication between a husband and wife is protected to the extent to where a wife cannot be forced to testify against her husband in the court of law. This norm and legal precedent is in place because society recognizes that privacy is needed to have intimate relationships and conversations. A husband and wife talk to each other in different ways when they are alone. Without privacy, these intimate bonds that are central to the human experience are not possible. If spouses were forced to testify against each other, one's dignity would be violated.

Dignity

Human dignity should not to be reduced to a number and should not be bought and sold in the marketplace. Some of the things we as humans do in life are not secret, but they do require privacy. For example, most people have sex but usually not in public. Other activities, like grooming, would look ridiculous if observed. People would be very vulnerable if this type of information was shared. It is important to have the words that we whisper into our lover's ears not published online and shared publically. Although these words are not unique or have been said before, the fact that they are made public would change their meaning. It would diminish the human experience.

Freedom

Freedom is the ability to live your life the way you want, not being harassed for doing so. When you are being observed and tracked, this freedom is diminished. While government's observation of citizens is certainly a loss of freedom, such losses can also occur in the commercial marketplace. Sometimes consumers give up this freedom for material goods and services willingly, and other times they are duped. For example, when the Angry Birds app was given away, the app maker was able to collect GPS information from consumers, which was then sold to third parties.

Consumers are now constantly observed by video surveillance. Cities have video surveillance, as do most downtown areas and even residential areas. People taking pictures all the time and posting them online is adding to the surveillance. It was such surveillance that identified the suspected Boston Marathon Bombers.

Consumer clickstreams have been collected and observed for years. An emerging trend is that consumers in brick and mortar stores are being tracked in similar ways as they are online. When consumers enter stores, they can be followed around from the signals emitted from their smartphones. Consumers now do not have choices whether they want to participate in market place activities and that compromises their privacy. For many transactions, it is difficult to purchase with cash and not be tracked. At a minimum, it is inconvenient. More importantly, it is very difficult, if impossible to not have cell phone these days. It really is not an option if you want to participate fully in society. However, when the NSA reported that they have be accessing American's phone records, this made consumers realize what it means to have reduced freedom.

Consumer freedom, while diminished in the marketplace, is not dead. In later chapters, we will discuss what consumers can do to regain this freedom. One of the problems with many of the market-based and self-regulatory solutions is that many privacy remedies are disproportionately available to the wealthy. The wealthy can buy privacy. It is the poor that will be forced to give up information and privacy in order to get needed services and products. This, too, will limit the freedom for the society as a whole.

Why Businesses Want/Need Privacy?

Businesses should be concerned about privacy as well. In particular, protecting consumer privacy can affect the outcomes in four broad areas.

1. Maintain customer trust,
2. Avoid media harm,
3. Avoid legal issues (FTC and class action), and
4. Competitive advantage.

Trust is an important currency in the information economy, especially since many actions that companies take with consumer data are not directly observable. Maintaining customer trust is very important to assure that information exchanges will continue to occur in the future. Research has shown that improving trust is more effective than reducing concern (Milne and Boza 1999).

One way that trust can be earned is by making sure the information that is gathered from consumers is secure. Indeed, one of the biggest concerns consumers have regarding privacy and business behavior is the security of their information. In 2013, survey polls (Greenfield 2013) showed that consumers are more concerned about hacking (83 percent) than tracking browsers for targeted advertising (54 percent). Consumers are particularly concerned that the hacking of company databases puts consumers at risk for identity theft.

The other privacy mistake that companies can make is engaging in activities that are seen by the public as being creepy. Google has been flirting with the creepy line for some time (Wolverton 2013). Their new Google Now that anticipates consumers' needs based on contextual information before they even know they need a service is one such item. Another is the photo program that will sort through a user's photos and pick out the good ones.

It is important for businesses to carefully manage consumer data and technologies, because a privacy mishap results in negative press. If a privacy line is crossed that is not acceptable, consumers will reduce their loyalty. During Black Friday of 2013, Target's database that stored credit card information was hacked, which potentially compromised over 40 million consumers' card information. In reaction to this, consumers were furious and frustrated (D'Innocenzo 2014).

When companies fail to protect the privacy of consumers by taking reasonable precautions or misstate their privacy policies, they are subject to investigation by FTC. The FTC began investigating privacy violations online in the late 1990s with spam cases against Nia Cano in 1997 and a privacy case against Geocities in 1999. Since 2010, there have been cases against Lifelock, Google, and Facebook. As of May 1, 2011, there have been 32 legal actions against companies that mislead consumers (Enforcing privacy promises n.d.). FTC judgments can result in large fines (FTC 2012).

The other downside from not paying attention to privacy is the threat to class action suits which are starting to occur with more frequency. For example, a class action suit to be filed in California claimed that Netflix "kept and disclosed information, including records of TV shows and movies viewed by its customers, in violation of the Video Privacy Protection Act and other laws" (Case No. 5:11-CV-00379 EJD; United States District Court, Northern District of California, San Jose Division). A class action settlement against Facebook for $20 million was made because Facebook's sponsored stories product shared users like button data without the ability to opt out.

A positive of taking the lead in privacy protection is that it can be used for a company's competitive advantage. Commentators have noted that if consumers are told what is being done with their data and consumers make market choices based on this information, then business will be forced to compete on the basis of privacy protection (Moorman 2013). In an example of how privacy issues can be used for competitive advantage, Microsoft has been attacking Google's Chrome book with their Scroogle campaign. One of the points is that this laptop is useful only when connected, and Microsoft accused Gmail of invading consumer privacy (Wingfield 2013). In the future, the companies who can offer the best privacy protection will have an upper hand in the market place.

Chapter Summary

This chapter reviewed previous claims that privacy is dead. An argument was put forward for reframing privacy and acceptable behaviors in the marketplace. Because of the benefits of protecting privacy for consumer and marketers, it is important to redefine expectations and undergo procedures to protect privacy in the future. Consumers have a need to control the collection and dissemination of sensitive information. They also require privacy for creativity, protected communications in relationships, maintaining their human dignity, and freedom. Marketers should be concerned about consumers' privacy needs and take proper actions to maintain customer trust, avoid media harm, avoid legal issues, and to gain a competitive advantage.

CHAPTER 3

Perspectives of Privacy: Technology History and Academic Theories

Chapter Overview

Privacy has been a difficult topic to understand given its amorphous nature and changing social and technological context. Previously, it was possible to have solitude in one's home and anonymity in public spaces. Now with the Internet, mobile phones, surveillance cameras, and the "Internet of Things" devices, these privacy states are not as possible as they once were. Indeed, the relationship between technology and privacy is a topic that academics have been wrestling with for years (Milne and Bahl 2010; Smith 2000). In this chapter, you will learn about the history of privacy and technology. In addition, you will be introduced to the major theories of privacy, which inform our understanding of technologically aided information exchanges between marketers and consumers. Lastly, you will learn about research in the marketing and public policy field that shapes our understanding of the contingencies affecting information exchanges.

A Brief History of Privacy and Technology

"Eavesdropper" and "peeping tom" are terms that have been associated with privacy invasion. The dates of their origins suggest privacy has long been a historical concern. Merriam-Webster defines eavesdropping as to listen secretly to what is said in private. Its first use was in 1606 and emanated from people standing inside the drip line of a roof and listening to what was said inside a house. Peeping tom, first used in 1796, is defined as a pruriently prying person. Its origins come from *Peeping Tom*, legendary citizen of Coventry who watched Lady Godiva (2014) riding naked. Other accounts suggest that in the 14th century, there were legal provisions in England calling for the arrests of peeping toms and eavesdroppers (Swire and Bernmann 2007, p. 3).

While the terms eavesdropping and peeping tom were used historically, the rise of technology has made it much more possible to do both so without being caught. Robert Ellis in his historical account of privacy in America (Smith 2000) notes that as soon as new information technologies have been introduced, they were used to invade privacy. For example, soon after the invention of the telegraph in 1938, bugging of conversations started (Huitric, 2008). Privacy invasions were also made possible by invention of the telephone in 1876 and the dictaphone in 1907. However, perhaps the technology that had the biggest initial impact on privacy invasions and thought in the United States was the Kodak camera in 1890.

The invention of the snapshot Kodak camera in 1890 gave the press a new tool to enhance the gossip columns written about celebrities. In reaction to this practice, Samuel D. Warren and Louis D. Brandeis wrote their influential article, “The Right to Privacy,” published in the *Harvard Law Review*. In the introduction of their article, Warren and Brandeis (1890) state:

> The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by intrusion upon the domestic circle.

The purpose of the Warren and Brandeis article was to establish the right to privacy that would not necessarily be limited to a particular context. Indeed, by linking the argument closely to technology and business practices, the article had taken on a quality of timelessness, which is extremely relevant for today. For the following quote, one could easily substitute the word *cell phone* and *social media* for *instantaneous photography* and *newspaper enterprise*, and this quote would be applicable today.

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."

Certainly cell phones (with their cameras) and social media have continued to spread gossip across the Internet (which is the modern equivalent of house-tops). Today people are consistently taking photos during all occasions and sending them to their Facebook or Twitter feeds. So much so, that is difficult to avoid being the subject of uploaded "news."

Do the arguments from Warren and Brandeis hold up today? Jill Lepore (2013) of the New Yorker argues that the privacy debate surrounding new cutting edge technologies is in fact a very old debate. There is a long history of people feeling anxious when new technologies are introduced that make it difficult to keep things private and not publicized to the broader world. She notes that the role of technology historically has been to erase mystery, expose secrets, and deny privacy. Long ago, there was a time when the mysteries of god, science, and state were only known to few. Then with the distribution of books, scientific knowledge was disseminated and erased the mystery. Finally, cameras exposed secrets and smart photos eliminated privacy by disseminating what was once secret. New technologies that are being introduced now and in the future, such as Google Glass, make it even more difficult to keep some activities private (Hoffman n.d.).

Today it is widely accepted that the computer age brought the technology that made information more transparent, accessible, combinable, permanent, and easy to share. This was recognized back in 1973. Horst Feistel (1973) in Scientific American stated, "There is growing concern that computers constitute, or will soon constitute, a dangerous threat to individual privacy." The personal computer in 1975, the World Wide Web in 1989, social media in 2004, and smart phones in the late 2000s, all contributed to this coming to fruition. Through these information technologies, consumers now attack their own privacy by publicizing their own lives.

Concurrently with the introduction of modern information technologies, scholars started theorizing about privacy. In the next section there is a review of the major privacy theories, starting with Alan Westin (1967), who wrote the very influential book *Privacy and Freedom*. Westin's book is one of the first works to address consumer information privacy and protection and offer an academically defensible definition of privacy. More importantly, he was the first to recognize the implications of computers and information technology on privacy before others could see their implications. He espoused that consumers have the right to keep certain information private and the freedom to decide with whom to share it.

Academic Theories

Privacy as Limiting Access to Others

Westin's contribution to the privacy literature centers on why and how consumer seek to control privacy. In particular, Westin's privacy theory articulates the ways that people limit access to themselves by others.

Westin defines privacy as:

> . . . the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small group intimacy or, when among large groups, in a condition of anonymity or reserve. (Westin 1967, p. 7)

Thus, according to Westin, achieving privacy is a dynamic process of readjustment depending on psychological or role-dependent needs. With the adjustment process it is possible to have too much or too little privacy. As noted in his definition, Westin argues that privacy operates at the individual, group, organizational, and institutional levels.

The crux of Westin's theory is his states and functions of privacy. The states are the process of how the functions of privacy are achieved. Put simply, states are how privacy needs are achieved. The functions in Westin's theory are similar to the discussion in the last chapter of why consumers desire privacy. People need privacy, among other reasons, to perform certain functions that are instrumental to their humanity.

The states of privacy articulated by Westin's theory are:

1. Solitude,
2. Intimacy,
3. Anonymity, and
4. Reserve.

Solitude is being separated by others and freed from observation. This separation protects the individual from physical and psychological interruptions Solitude can give the person space to avoid the noises of everyday life. With solitude, one can gain peace of mind. It permits the space to contemplate, be creative, think, and unwind. Westin notes that solitude is the most complete form of privacy. Solitude, which is a chosen aloneness, can be achieved by being in nature, closing doors, and shutting down computer communications. Reading, taking a bath, and any activity that creates space and time for one's opens up the opportunity for solitude.

Intimacy relates to small groups where one can relax and not be guarded. Achieving intimacy requires trust that other will not judge you and use information against you. It allows for frank and honest conversation. This happens with husbands and wives, friend groups, and sometimes in work situations. This can be achieved in both the physical and digital world, by either getting together is small groups in a protected room (from others) or electronically through secure chat rooms such as Google Plus Circles.

Anonymity relates to not being under surveillance in public. The person achieving anonymity is in public is doing public acts, being observed, but not identified. There used to be a time when individuals could find anonymity in a big city. They could walk the streets or ride the subways and not be identified (unless famous). However, with cell phones that emit GPS locations and digital signatures and the increasing prevalence of surveillance cameras, achieving this is very difficult. With the widespread use of personal photo technology (cell phones) and video cameras in public, this privacy state is quickly eroding. Consumers early on felt that the Internet was a public space where they would not be observed. This was not the case. However, in the online space there still are approaches, such as using private browsing modes, which can be used to achieve anonymity (Pinola 2011).

Reserve relates to protecting one's self from unwanted communication and not disclosing information to others. When mental boundaries or social cues are used to create reserve, this can be considered the most subtle of the privacy states. On the other hand, reserve is the primary state in which consumers can protect themselves from unwanted commercial content. This requires consumers to not provide contact information by opting out (or not opting in) to such arrangements with marketers.

The other states not mentioned by Westin include Not Neighboring (Margulis 2003), which is related to solitude.

The why's or functions of privacy according to Westin are:

1. Personal autonomy,
2. Emotional release,
3. Self-evaluation, and
4. Limited and protected communication.

Personal autonomy is the freedom from being manipulated. This is a very fundamental need of individuals and considered a basic freedom by many. This was the basic freedom erased in George Orwell's (1984) famous book. This is also a need that has caused much uproar over the NSA spying situation. When an entity, like a government or a commercial enterprise, controls all information about you, it can manipulate you. A commercial enterprise, for example, can track your movements online and determine the content to show you.

Emotional release is the release from tension of daily life. Irwin Goffman (1959) puts this in terms of wearing a mask in public while on stage and taking the mask off in private when off stage. Being able to unmask is important for one's mental health by reducing stress. When one is in the public, there is effort to keep up appearances. Privacy provides the opportunity to exist without the burden of maintaining this façade.

Self-evaluation is time needed to reflect on one's life. It allows people to integrate information and see patterns that help them establish courses for their life paths. It permits a chance for the self to reflect and adjust. Privacy is needed to establish conditions for these processes to occur. Self-evaluation in a protected environment is the key to one's well-being and growth.

Limited and protected communication is the sharing of personal information with trusted others. It is so important that there are laws in place to guarantee the privacy of one's communication. There are certain situations between spouses, lawyers, and medical personnel where conditions for this communication are well-established for exchanges between consumers and marketers.

Keeping the information between the two parties and not sharing with third parties has become an expectation of consumers under many market conditions where sensitive information is exchanged. Knowing a communication will not be divulged will provide trust and confidence for the parties to exchange sensitive information that will benefit the relationship.

Other functions not mentioned by Westin are providing a space for creativity without judgment, which was mentioned in Chapter 2.

A summary of Westin's states and functions is shown in Figure 3.1.

Privacy Boundary Theories

Westin's theory has been extended by boundary theories that focus on the mechanisms in which privacy is regulated. In this section, there is a review of (1) Altman's (1979), (2) Delerga and Chaikin's (1977), and (3) Petronio's (2002) theories. Diagrams reflecting the discussions of these theories are shown in Figure 3.2.

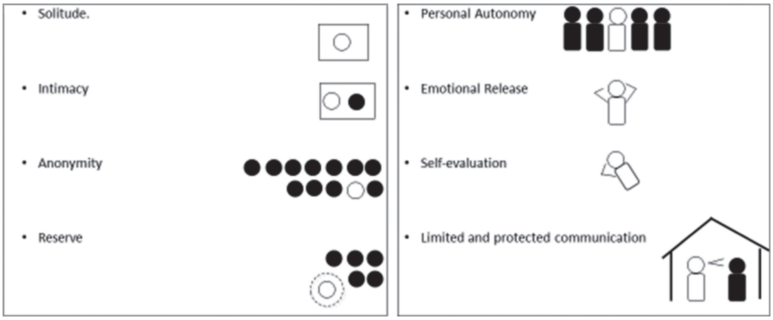

Figure 3.1 Westin's four states and functions of privacy

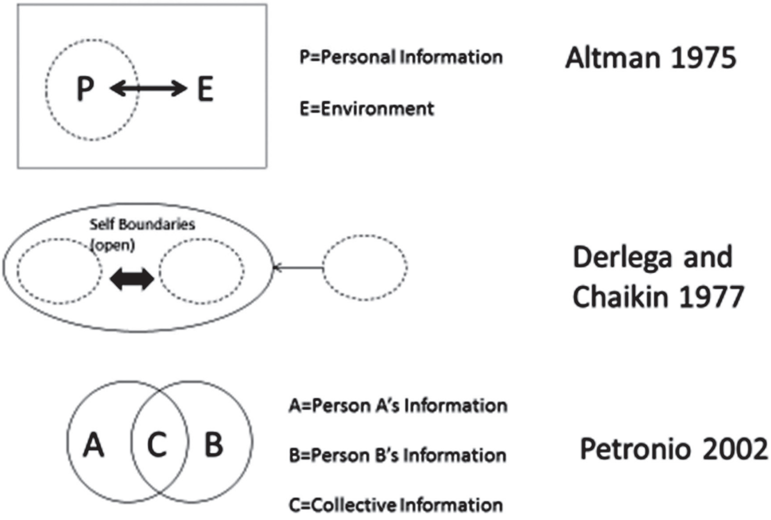

Figure 3.2 Privacy boundary theories

The most influential boundary privacy theory was created by Irwin Altman (1975). Altman's theory of privacy shows a system of regulation. It is an individual and group level model that discusses the processes of opening and closing boundaries and the ramifications of doing so. Altman (1975, p. 24) defines privacy as the "selective control of access to the self." Altman's theory is shown in Figure 3.3 and can be summarized in five points.

1. The privacy process is dynamic. Individuals can regulate their interaction with others by opening and closing boundaries based on the internal needs or external conditions.

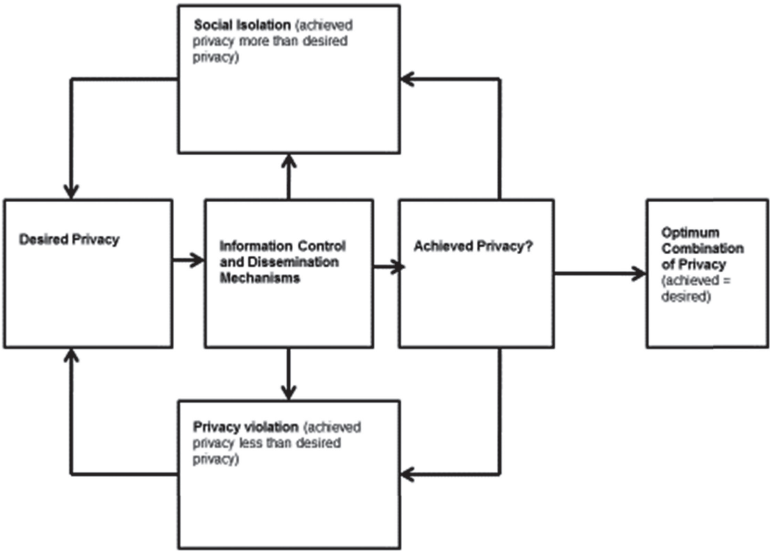
Social Isolation (achieved privacy more than desired privacy)
Desired Privacy
Information Control and Dissemination Mechanisms
Achieved Privacy?
Optimum Combination of Privacy (achieved = desired)
Privacy violation (achieved privacy less than desired privacy)

Figure 3.3 Application of Altman's privacy regulation theory

2. There are differences between actual levels of privacy (that what you currently have) and desired levels of privacy (that what you want).
3. The optimal level of privacy is when desired = actual level. Too much privacy, or isolation, is when desired < actual privacy. Too little privacy, or crowding, is when desired > actual privacy.
4. Two-way communications/interactions affect levels privacy. Thus, privacy regulation is bidirectional.
5. Privacy occurs at both the individual and group levels. Mechanisms include verbal content, territorial behavior, and cultural norms.

An application of Altman's theory is shown in Figure 3.3 where the consequences of self-regulation are illustrated. If the consumer does not regulate stringently enough, he will suffer a privacy violation since he will achieve less privacy than desired. Alternatively, if the consumer regulates too stringently, she may suffer social isolation and have more privacy than desired. The process in the market place is by trial and error, to match privacy control with desired expectations.

An extension to Altman's privacy model is the Delerga and Chaikin (1977) model, which is a dual boundary model. The dual boundary model shows that individuals function and make exchanges within a dyadic safe zone. This safe zone creates a trusted environment. The self-boundary is open if the dyadic boundary is closed, protecting private information from the outside. Individuals regulate these boundaries to create a desired degree of openness and closedness.

This theory has been used in setting up protected shared spaces for groups online with apps. One such app is Couple, which lets two individuals have a protected online network to talk privately. Couple (app) (2014) is similar to other apps such as Whats App, Facebook Messenger, and Kakao Talk. This is very similar to features in Google Plus, which creates circles or groups where information about certain topics can be exchanged.

Another boundary theory that draws from Altman's self-regulation notion of boundary management is Petrino's (2002) theory of communication privacy management. Petrino's theory can be summarized in four points.

1. Private disclosures are dialectical (both risky and beneficial at the same time),
2. People make choices about revealing or concealing and closing or opening access criteria and conditions they perceive as salient,
3. Individuals have desire to regulate access to their private information, and
4. The metaphor of boundary is used to illustrate that consumers are in control of the flow of their information to outside parties. Individuals regulate boundaries through degrees of openness and closedness, where setting boundaries is seen as a communication process. Here, individuals use decision calculus to decide whether to disclose information. If desired privacy is not achieved then turbulence can occur.

Petrino's theory utilizes a rule-based system that draws upon the concept of decision calculus to explain privacy disclosures (Laufer and Wolfe 1977; Milne and Boza 1993). The rules based focus discusses how decisions are made, which is useful for understanding the information exchanges between marketers and consumers. As an example, such decision calculus comes to play for consumers who must tradeoff the benefit of reviewing mobile apps and letting the app market have access to their location data. Likewise, consumers use decision calculus when setting up the privacy controls for Facebook.

Together, the theories of Westin and Altman have been very influential in understanding privacy (Margulis 2003). Westin's theory provides a strong foundation for understanding why consumers need privacy and what states are needed to achieve it. As suggested previously, technology is greatly impacted both solitude and anonymity. Unless there is a lot of trust between people, intimacy is difficult to acquire. However, marketers are attempting to achieve intimacy through customer relationship management programs. As marketing surveillance technologies become more sophisticated, concepts of solitude, anonymity, and intimacy are becoming more germane to public discourse. In today's world of social networks, the reserve state is still being debated and some have argued that consumers are now oversharing and do not use reserve. However, there is a possibility that the development of the social norm of reserve will lead to greater levels of privacy.

Altman's theory provides a strong foundation for understanding the process of regulating privacy boundaries and the disclosure of information. Consumers, through their choices (such as the privacy controls), can regulate the level of privacy they acquire. The bidirectional setting of exchange regulation will determine the extent to which a consumer achieves, overachieves, or underachieves optimum privacy. Marketers in their interactions with consumers are best served by trying to match consumers desired level of optimum privacy. The extensions of Altman by Derlega and Chaitin as well as Petrino theory introduce the important ideas of privacy safe zones and decision calculus. All these concepts are directly applicable to the information privacy exchange perspective discussed next.

The Privacy-Marketing Cost-Benefit Exchange and Contingencies

In addition to the Westin and the boundary theories of privacy, there has been scholarship in the marketing field that has examined privacy regulation by consumers as a cost-benefit analysis. This section of the chapter discusses this perspective and other contingencies that influence the cost-benefit tradeoffs.

Whether or not consumers exchange information with marketers can be viewed through a cost-benefit analysis, where consumers consider the privacy cost and the benefits from providing the information. Milne and Gordon in 1993 viewed such exchanges as implicit social contracts, which were subject to norms in the self-regulatory environment (Laufer, Proshansky, and Wolfe 1976; Laufer and Wolfe 1977). For all cost-benefit tradeoffs, it is ultimately an individual's decision that is subject to many situational factors and contingencies. As such, much of the privacy versus benefit tradeoff have to do with the information attributes and factors surrounding the information disclosure.

The contingencies that have been examined by researchers are:

- the information's relationship to the self-concept,
- the type of information shared,
- the role of exchange partners,
- the role of the technological environment, and
- industry norms.

Protection of the Self-Concept

Privacy and the self-concept are intrinsically connected. As noted previously, Altman defines privacy as selective access to the self. Others note that privacy achieved through solitude is an essential requirement for connecting with, evaluating, and nurturing the self (Altman and Taylor 1973; Milne, Markos, and Bahl 2008; Norberg, Horne, and Horne 2009; Westin 1967). There is also a desire to protect personal information related to the self from unwanted scrutiny and unsolicited input from reference groups (Goodwin 1992). It has been suggested that when dealing with marketers, consumers will consider how information requests could enhance or hurt their self-concept (Milne, Markos, and Bahl 2008).

The self in relation with others has been viewed as a layered amalgamation of various zones around the core -self, where the core-self is the most protected and the surrounding zones gradually open up to more people (Westin 1967, p. 33). As shown in Figure 3.4, the core-self comprises the most intimate elements of the self, while the outer zones contain less sensitive elements of the self. Milne, Markos, and Bahl furthered this understanding of the self with regard to privacy by adopting Belk's (1988) definition of extended self , wherein the inner-self, body-self, group-self,

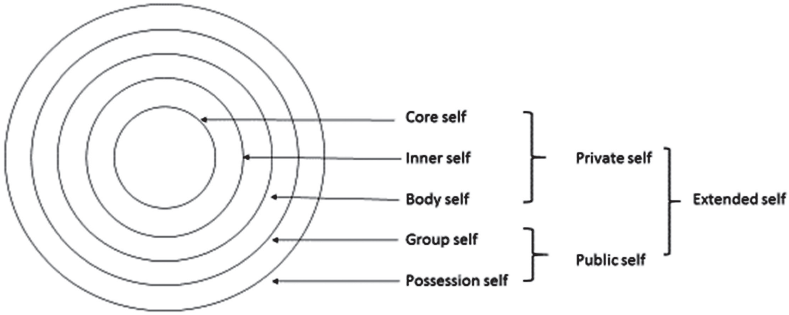

Figure 3.4 The protection of self-concept privacy model

Figure 3.5 Collage on an individual's selves

possessions-self, and environment-self are considered as elements of the extended self that one seeks to protect and enhance.

The extended self can be organized into private self-items that may or may not be shared by consumers depending on the controls that are put in place. The public-self items are more likely to be shared without controls. The inner and body selves are often considered private, and the group and possession selves are often considered public.

An illustration of what the protection of the self-concept means to consumers is shown in Figure 3.5. This figure was created by asking a respondent to gather pictures from magazines that metaphorically reflected what privacy meant to each of these self-aspects: inner-self, body-self, group-self and possession-self. As an illustration, it reflects one person's perspective.

The inner-self to this individual refers to secrets and intimate moments represented by dreams and nightmares. The body-self to this person refers to her sexuality. The group-self represents belonging to nature and like-minded people with similar outlooks. The possession-self was reflected through musical equipment. All these pictures help define the person.

The idea of the self being comprised of different components is consistent with Westin and Altman who define privacy in terms of limiting access to the self. Recognizing the role of the self provides a more dynamic and nuanced representation of the privacy process by allowing different elements of the extended self to form the core-self at different times. Cost-benefit decisions as whether or not to disclose information are purported to be based on the needs of the extended self.

Type of Information Shared

As discussed in Chapter 2, the decision to disclose information is based on protecting what is deemed sensitive and on the consequences of disclosure. Indeed, the type of information request has a direct impact on the outcome of consumers' cost-benefit analysis of deciding whether to disclose. Most consumers agree that highly sensitive information is that information which can directly identify them online or offline (Phelps, Nowak, and Ferrell 2000). The findings from past research indicate that consumers, when deciding whether to disclose information, are generally less concerned with anonymous data being collected compared to personally identifiable information (PII) (Phelps, Nowak, and Ferrell 2000; Sheehan and Hoy 2000). The accepted understanding is that PII is perceived by consumers as sensitive information, denoting a heightened degree of privacy risk (Weible 1993). This concern is shared by the FTC and other public policy advocate and, thus, specific consumer information is protected by law (FTC 2000).

Recent discussion in the privacy law literature, however, highlights the limitations of assuming that only PII information can be considered sensitive (Schwartz and Solove 2011). Non-PII, which is anonymous information that provides personal details such as demographics, group affiliations, online shopping behaviors, and browsing activity, until recently has been considered less sensitive; however, when merged with more data points it can be used for personal identification resulting in unclear situations. Indeed, recent FTC reports have recognized the importance of assessing both PII and non-PII in terms of perceived sensitivity and the potential for privacy harms to consumers (Federal Trade Commission 2009; Federal Trade Commission 2012).

Role of Exchange Partners

Cost-benefit analysis of the decision to disclose information is also driven by the context in which it is viewed or shared with others. The idea is specifically captured in the definition of privacy in the marketing disciple by Goodwin in 1991, which directly links the disclosure decision (control) to those who may view the information:

> The consumer's ability to control (a) the presence of other people in the environment during a market transaction or consumption behavior and (b) dissemination of information related to or provided during such transactions or behaviors to those who were not present (Goodwin 1991).

Consumers will consider the viewer context in evaluating how sensitive information is and whether they will share it with others. However, the when and why of information sharing is much nuanced. The self-disclosure literature notes the importance of both information sensitivity and viewer context in determining the level of information sharing in general (Chelune 1975; Margulis 2003). Research indicates that people disclose and reciprocate more with people with whom they have a close relationships they are less likely to disclose information with strangers and acquaintances (Derlega 1993) and they are more likely to disclose to a single person than to a group (Solano and Dunnam 1985). However, people do not always provide information to those whom they consider close (Barrell and Jourard 1976) and often

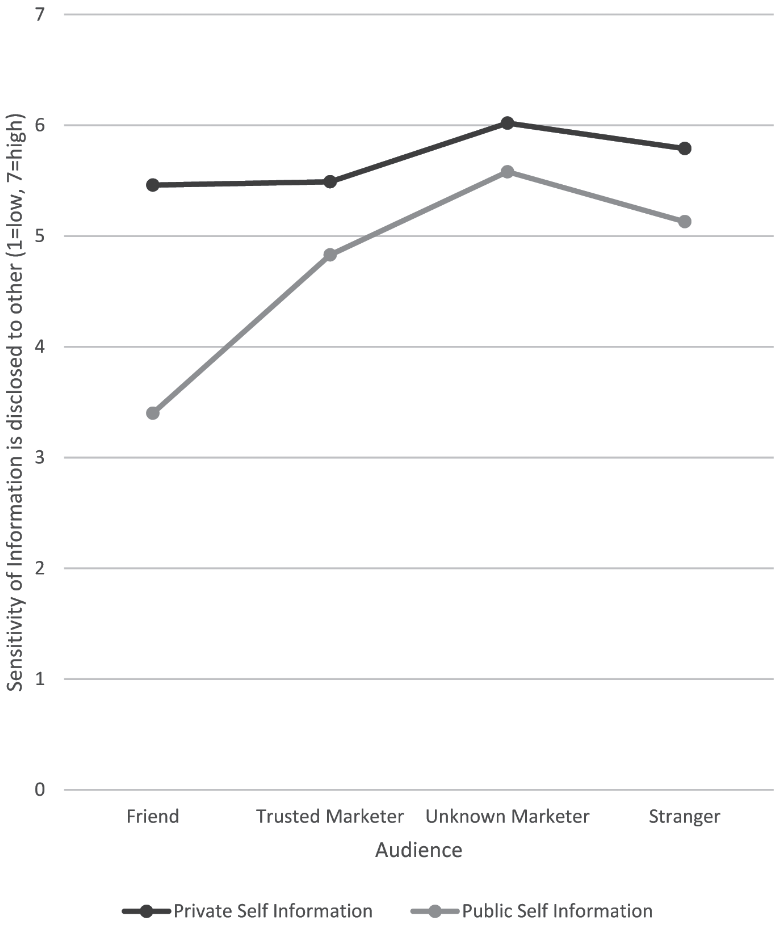

Figure 3.6 Information sensitivity by self and audience

Source: Markos (2010).

act cautiously when the disclosure involves highly sensitive information (Petronio 2002).

Figure 3.6 shows the level of information sensitivity for data that is related to the private-self versus the public-self (see Figure 3.4), and the willingness of consumers to share the information across viewer groups. Data related to the public-self is considered less sensitive regardless of audience, especially if shared with friends. However, for information related to the private-self, this information was considered very sensitive, regardless of the audience (friend, marketer, or stranger).

In a marketing context, consumers sometimes share information and other times do not. For example, consumers are reluctant to share embarrassing information about purchases like contraception, even they are given a customized benefit from a known business (White 2004). For some purchases consumers feel shame due to a perceived social presence that is either real or imagined (Dahl, Manchanda, and Argo 2001). Overall these research findings support the idea that the viewer context influences the perceived sensitivity of information. Perhaps, this is why marketers invest in a quality website (professional appearance) that instills consumer trust in order to create a higher likelihood of consumer purchase (Schlosser et al. 2006).

Technology Environment

The next contingency factor affecting the cost-benefit decision to disclose is the type of technology used to collect information. Research (Markos and Milne 2011) showed that the technology used to share information is important. Researchers found that if another person was on the receiving end as with telephone contacts, consumers were far more likely to provide information than they were through other formats (e-mail, fax, mobile app), especially if they considered the information highly sensitive. Technology offers ever-expanding exchange methods, yet the older methods sometimes offer a stronger sense of security than new technology. In contrast with prior research (Moon 2000), Markos and Milne found that consumers preferred to speak with a live person to communicate sensitive personal information. Across all levels of information sensitivity, the mode of communication that elicited the most disclosure was phone, followed by e-mail, mobile applications, and finally fax.

Other research has shown that consumers desire to remove their name from contact lists varies by communication and technology channel (Milne and Rohm 2000). In this study, consumers were more likely to want to be removed from telephone lists compared to e-mail and mail lists, and lists e-mail compared to mail lists.

The important point here is that preferences regarding information disclosure vary by technology. The above results, however, are time bound and are based on level of experience. Recently, the trust of information on secure websites has increased. For example, consumers are very willing to provide credit card numbers to secure websites. Indeed, in the last few years, there has been an ever increase release of new technologies to gather information.

The use of new information technologies by marketers has caused concern by industry observers as well as by consumers. While new information technologies are beneficial to marketers, some marketers overstep the boundaries of acceptable practice while using them (Holtzman 2006). When information is gathered and used without consumer consent, this results in privacy violations (Goodwin 1991). The asymmetry between marketers' and consumers' acceptance of technologies is what is causing privacy concerns. Often, businesses anxious to utilize the efficiencies from the technologies do not fully understand different consumer segment apprehension of the new approaches for gathering data. Milne and Bahl's (2010) investigation of eight separate marketing technologies showed that there were different expectations for the type of permission needed to collect the information between marketers and consumers.

Consumers' desire to control technologies is not only based on how new the technology is but also how the technology will be used. Based on the same study, Milne and Bahl examined consumer desire to control technologies for marketing communication and information gathering. As the data in Figure 3.7 show, consumers want high levels of control over both

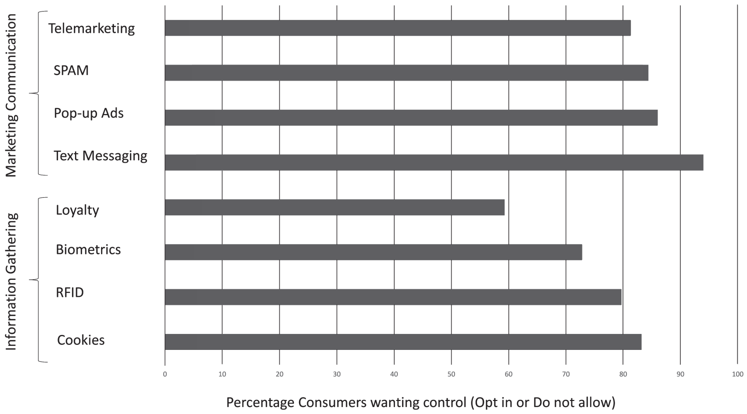

Figure 3.7 Percent consumers wanting control over technologies

information gathering technologies (cookies, biometrics, loyalty cards, RFID tags) and communication technologies (text messages, popup ads, telemarketing, SPAM). Consistently, research has shown that consumers want more control than marketers expect, especially database marketers. Because of the data intensive nature of their business, database marketers expect lower consumer controls than consumers themself. This disparity in expectations creates the conflict between consumers and marketers.

As new technologies are rolled out, new privacy concerns and issues arise. Recent advances in facial recognition technology, for example, have caused concern. One of the reasons is that consumer data can be easily collected and uploaded to online networks. With these capabilities, marketers will have to pay close attention to consumer reactions to the technology, as well as the information acquisitions when using these new technologies.

Industrial Relationships

The last contingency factor affecting cost-benefit decisions about consumers disclosing information is the industry norms where information is being exchanged. Research has shown that consumers concern about privacy and trust of marketers with personal information varies by industry (Milne and Boza 1999). In particular, this research has shown that there is discriminant validity between trust and concern and that both of these constructs are the key to understanding the information practices of firms. As part of this study, industries were grouped into clusters based on scores of trust and concern. In interpreting the data, the researchers inferred that concern was driven by the sensitivity of the information gathered and trust was based on whether the organization was planning to share the information with third parties.

As an update to this study, it was partially replicated in Milne and Ross (2013). The focus of the more recent study, like the original, was to ask consumers to rate 17 industries based on two questions:

1. How much do you trust companies from this industry with your personal information?
2. How concerned would you be if a company from this industry had access to your personal information?

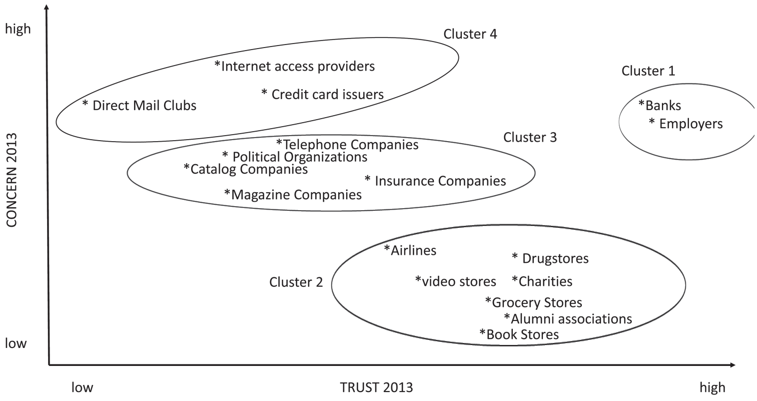

Figure 3.8 Consumer concern and trust of 17 industries in 2013

Figure 3.8 shows the how 17 industries were viewed in 2013 by a sample of online consumers.

The data show that cluster 1, comprised of banks and employers, are the most trusted. Interestingly, despite the sensitive information, there was neutral concern due in part to the heavy regulation of the financial industry. Cluster 2, represented by airlines and retail stores, was the group with positive trust for and the lowest level of concern. This is due to the fact that consumers have a lot of experience sharing information with companies in these industries. Cluster 3 is represented by more digitally based industries such as telephone companies. There is moderate concern but less trust due to the prevalence of information sharing in these industries. Cluster 4 comprised of Internet providers, credit card companies, and direct mail clubs, has the same trust level as cluster 3. However, the history of these industries and the sensitive information gathered led to the high concern levels.

Chapter Summary

This chapter illustrated the relationship between privacy and technology. It pointed out that privacy invasion has historical roots and there is a pattern of new information technologies when they first were introduced being used to violate consumer privacy. The famous law review article by Warren and Brandeis, “The Right to Privacy,” was in reaction to technologies being used for privacy invasions. It was noted that principles in this article hold true today.

Four academic privacy theories were presented: Westin, Altman, Derlega and Chaikin, and Petrino's. Of great importance is Westin's 1967 theory of privacy. Westin noted four states of privacy: solitude, intimacy, anonymity, and reserve. The functions, or why people need privacy, were for personal autonomy, emotional release, self-evaluation, and limited and protected communication.

Next boundary theories, which focus on the mechanisms for regulating privacy were discussed. Altman's theory presented a system for regulation that relies upon the selective control of access to the self. Altman's theory showed the implication of having too much or not enough privacy. Delerga and Chaikin extended Altman's theory by introducing a dual boundary and the idea of a safe zone. Petrino, drawing upon other boundary theories, created a theory of communication privacy management. This rules-based approach relies upon decision calculus.

In the last part of the chapter, cost-benefit tradeoffs of privacy management were discussed. The contingencies that affect these tradeoffs include the information's relationship to the self-concept, the type of information shared, the role of exchange partners, the role of the technological environment, and industry norms. The next chapter further examines information exchange in the marketplace.

CHAPTER 4

Information Exchange and Privacy in the Marketplace

Chapter Overview

This chapter examines information exchange and privacy in the marketplace. Information exchange, which is central to the modern economy, presents many benefits to consumers and society at large, as well as associated privacy risks. Consumers are faced with the difficult decision of determining how to participate in the market while gaining some control over their own privacy. Marketers are trying to benefit from the information exchange but also not wanting to violate the trust of consumers.

In this chapter you will learn about the theory of marketing exchange and the antecedent factors that influence marketers and consumers information exchanges with each other. The factors include:

1. The role of social contracts,
2. Market influences (marketing concept, policy and ethics, regulation and social media), and
3. Consumer influences (perceptions, demographic background, risk and technology tolerance).

Conceptual Model of Factors Affecting Information Exchange

The chapter is organized around an information exchange model shown in Figure 4.1. This model depicts the market and consumer background

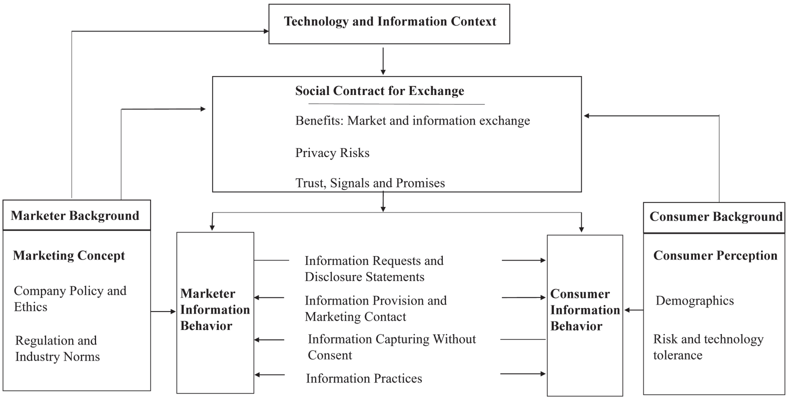
Technology and Information Context
Social Contract for Exchange
Benefits: Market and information exchange
Privacy Risks
Trust, Signals and Promises
Marketer Background
Marketing Concept
Company Policy and Ethics
Regulation and Industry Norms
Marketer Information Behavior
Information Requests and Disclosure Statements
Information Provision and Marketing Contact
Information Capturing Without Consent
Information Practices
Consumer Information Behavior
Consumer Background
Consumer Perception
Demographics
Risk and technology tolerance

Figure 4.1 Model of factors affecting information exchange

factors and decision processes affecting the information exchange behavior between marketers and consumers. It is important to note that while relationship marketing is the goal and focus of marketers, the long run relationships can be severely affected by mishandling a single information exchange. Consumers, who have a long trusted relationship with a marketer, may, upon noticing a privacy or security breach, reassess each and every information exchange. Given the risk surrounding information exchanges, this is the reason the focus here is on the fundamental exchange, while realizing that a single exchange may evolve to relationship status in the future.

The information exchange model shows the various types of information exchanges that are directly affected by social contracts and marketer and consumer background factors. Social contracts are influenced by marketers and consumer background factors and the technological and informational context. The technological and information context is determined by the marketer background.

The model shows that information exchange between marketers and consumers consists of four types of information behaviors.

1. Information requests made by marketers and disclosure statements delivered from marketers to consumers,
2. Information provision by consumers and marketers and the marketing contact between marketers and consumers,

3. Consumer information capturing by marketers without consent, and
4. Information practices.

As shown in the model, the decision by both consumers and marketers to engage in an information exchange is based on a social contract for exchange. For marketers entering into a social contract, this entails deciding what types of market and information benefits are being offered, determining how privacy risks are going to be managed, and assessing the level of trust with regard to commanded and specific promises made. For consumers entering into a social contract, this entails assessing the value of the market and information benefits determining the technology and information context privacy risks surrounding the exchange, and assessing the credibility of the marketer's reputational trust and promises.

The technology and information context has direct influence on the social contract. Marketers, for example, dictate the technological platforms and the type of information that is to be exchanged. Such decisions are directly affected by the marketing concept tactics employed by the firm, as well as by the company policies and ethics and the regulatory and industry norms. For consumers, the technological platform and information context affects the consumer information exchange directly in terms of the benefits and privacy risks associated. Consumer perceptions of the information sensitivities and control and risk of using these technologies affect the ultimate exchange decision. Here consumer background factors such as their demographics and risk and technological tolerances come to play.

Marketing and Exchange Theory

Marketing has been referred to as the discipline of exchange, and exchange is fundamental to the theory and practice of marketing (Alderson 1965; Bagozzi 1975; Houston and Gassenheimer 1987). At its most basic and narrow perspective, exchange can be viewed as "the direct transfer of tangible entities between two parties," (Bagozzi 1975) yet it has also been recognized that exchange entails the transfer of intangibles, both actual and symbolic (Bagozzi 1975). Thus, in marketing, exchanges encompass situations where goods and services are exchanged for money, as well as where messages are communicated from marketers to consumers and information is exchanged between the parties. Further, exchanges in terms of the parties involved (for instance, parties A, B, and C) range from simple to complicated configurations. Exchanges can be classified as restricted (A↔B), generalized (A→B→C→A), or complex (A↔B↔C). The restricted case represents a marketer and consumer interaction, and the generalized case can represent marketer A's use of a third party B to communicate to customer C. Complex exchange represents a marketing channels situation where the marketer (A) works through an intermediary (B) to reach its consumers (C).

The economic-based laws of exchange state that the exchange between two parties occurs if each party's utilities increase as a result of the exchange. Alderson's law of exchanges (Alderson's 1965) is described in terms of shifts of assortments. Consider that x is in A's assortment and y is in B's assortment. An exchange will take place if:

1. x is different than y,
2. the potency of assortment A is increased by dropping x and adding y, and
3. the potency of assortment B is increased by dropping y and adding x.

Further, Houston and Gassenheimer (1987) note that potency enhancement is the motivating force behind exchange. In other words, for both consumers and marketers, the driving force is *need satisfaction*. Parties enter into mutual exchanges with the thought that they will improve their assortment and are better able to satisfy their needs.

Sometimes, under various market conditions, entities enter into exchange knowing they will have to delay their gains (or need satisfaction) until the future. Such behavior requires trust that the other party will deliver on their promises in the future. However, it is possible that the value generated from the exchange for one party can be diminished when the value is realized only after the transaction has taken place. Under these circumstances, exchanges will not strictly follow the laws proposed by Alderson. The deviation from theory is explained by the fact that exchange is not an isolated action; rather, exchanges are part of a pattern comprising a longer-term relationship. When examining exchange over time, it is possible that *y* can be added to assortment A and then may later be deemed unsatisfactory, thus causing the holder of assortment A to see its value diminished. The question that arises is what will the holder of A do at this point upon realizing that the exchange was not beneficial.

A fair exchange occurs when the elements of the exchange are specified at the time of the transaction with no deception. However, deception can occur when consumers are not aware of the activities of the marketer or the specific terms of the exchange. This can occur because the marketer is either not forthcoming or that the consumer does not have enough experience with a particular marketer. Deception is most likely when there exists a social distance between exchange parties (Houston and Gassenheimer 1987). Social distance can also create lower levels of awareness. To overcome the negative aspect of social distance, marketers have turned to relationship marketing, which is a managerial tool that can diminish the social distance and give consumers greater trust in the actions of the business in fulfilling the specifics of the given exchange. By establishing relationships, the focus moves away from isolated exchanges that need to be negotiated on an as-needed basis to a relationship framework where there are well-agreed upon expectations about the behaviors of the parties involved.

Information Exchange

Some of the exchanges that we have discussed so far are when a consumer discloses personal information to a marketer. Consumers enter into information exchanges and relationships with marketers with the expectations of receiving benefits, such as better targeting, customization, improved customer service, and so forth. With respect to information exchanges, there are four types of information exchanges between marketers and consumers (Milne 2000). These exchanges between marketers and consumers, facilitated by technology, are enumerated and discussed below.

1. Information requests made by marketers and disclosure statements delivered from marketers to consumers.

One way to get information from consumers is to ask for it directly. Historically, database marketers have accessed information through surveys, product registrations, and warranty cards. Often times this information is filled out online, for example, when a consumer joins a website community and fills out a profile. The other type of information conveyed from marketers to consumers is disclosure statements. These are usually listed on marketer's websites as privacy notices. Consumers are often directed toward them at the time of registration. Some companies will notify consumers when the disclosures changes. The effectiveness of privacy notices has been criticized, citing the notices for being too long, full of legalese, and difficult to comprehend (Milne, Culnan, and Greene 2006).

2. Information provision by consumers and marketers and the marketing contact between marketers and consumers.

To conduct commerce online, marketers need information and consumers need to participate and provide information. For example, purchasing with credit cards using frequent shopping cards, while disclosing information to marketers, also affords the consumer convenience and benefits. To utilize apps on one's phone also requires providing information to the marketers. However, providing information to marketers imposes costs on consumers in terms of privacy risk and unforeseen transaction costs in the future. As a consequence, some consumers will only provide information in situations where there are strongly implied benefits or direct benefits such as compensation (Gabisch and Milne 2014).

3. Consumer information capturing by marketers without consent.

The online environment permits marketers many ways to efficiently gather data on consumers in a covert manner without their knowledge. In the online environment, it is possible for marketers to capture consumer click stream data and movements on websites and to keep track of them over time by placing cookies on the consumer computers and mobile devices. Consumer movements are also tracked as they go from website to website where the machines also send cookies about the consumer visit to advertising networks. While online activities are the most frequently tracked, consumers in the physical space are also being covertly tracked. For example, through their phones, consumers unassumingly provide information to marketers in the physical world. Some stores have set up devices to use information and track consumers' paths through stores.

4. Information practices.
   Consumers and marketers often share information to make the online experience seamless. Many apps are set up so that information can be obtained from consumer accounts and automatically update. For example some apps, such as Spotify or Insight Timer, will automatically post on a person's social network when an activity on the app was completed such as listening to a song or meditating. Thus in the case of digital apps, the digital content of what song was listened to goes directly from Spotify to Facebook.

Social Contracts for Information Exchanges

Information exchanges in the marketplace generally take place in the absence of a legal contract but rely upon social and reputational mechanisms to enforce them, which are referred to as social contracts. Social contract theory (Macneil 1980) recognizes that, due to shared interests, tradeoffs are made by each party to arrive at acceptable exchanges. Norms guide the behavior of both exchange parties by setting the minimum standards for exchange. From this perspective, businesses should avoid fraud and deception and show respect for their customers. In marketing, social contract theory has been used to explain the importance of norms in exchanges (Heide and John 1992) and trust in inter firm relationships (Gundlach and Murphy 1993). At a more macro level, others have conceptualized social contracts as an approach to balance the interests of different constituencies in society (Culnan 1991; Laufer, Proshansky, and Wolfe 1976; Laufer and Wolfe 1977). Dunfee, Smith, and Ross (1999) noted that the social contract, with its tie into fundamental principles of exchange, provides a moral compass to marketing. Not only do social contracts provide positive influences, but market forces also regulate poor business behavior and will undermine their long-term success. Such points provide the underlying logic for self-regulation.

With regard to understanding information exchanges, social contract theory has been used to examine privacy requirements for name removal

(Culnan 1995) and the privacy-benefit tradeoffs that consumers make with direct marketers (Milne and Gordon 1993). Information exchanges are relational because they are generally noncommercial because money was not exchanged, and they are long-term with implicit terms. They differ from discrete contracts, characterized in microeconomics, where single exchanges between unrelated parties take place. With information exchanges, there are many relational components with multiple exchanges taking place over time and implicit terms which are governed in part by social norms.

Prior to entering a social contract for an information exchange, both parties must make a cost/benefit tradeoff. Consumers need to perceive whether the benefits of entering into the contract outweigh the costs (Culnan 1991). Consumers may benefit from the personalized offers they receive from the marketer or other economic incentives such as coupons and rewards (Gabisch and Milne 2014). At the same time, consumers are weighing possible privacy risks that are present by providing personal information. These risks can occur when the information is transferred to unintended parties. For example, a consumer could suffer damage if a marketer transfers data to an undisclosed third party or does not give the consumers the opportunities to remove the information from a database (Culnan 1995). If the benefits outweigh the risks, they will enter the social contract; otherwise, they will not. Likewise, marketers must consider what promises and provisions they are providing to get consumers to comply with information requests. They must also consider whether they have the resources and commitment to follow through on their promises. If they do not and a privacy breach occurs, damage can be done to the marketer's reputation in the market place. On the other hand, putting the provisions in place can pay off as gaining access to consumer personal information has tremendous economic benefit.

Benefits: Market and Information Exchange

Both marketers and consumers benefit from the exchange of information. For marketers, consumer information allows for better targeting, customization of offers, and overall improvement in marketing ability. It is an essential element for companies to follow the marketing concept.

For consumers there are many benefits. Oftentimes, consumers provide information because it improves the marketing done to them. It may result in more relevant and better targeted ads and reduce the quantity of undesired communications. Indeed, several sites such as Google and Yahoo ask consumers to reveal preferences for the type of communications to receive. Information exchanges often offer some type of compensation such as access to a website or e-book content, an app, or free access to information-based products such as music. Marketers can use the information provided or acquire behavior-based information that is gathered from consumers' interactions with the online exchange platform (i.e., listening to internet radio for "free"). Consumers also exchange information for monetary rewards such as coupons or cash awards (Milne and Gabisch 2014). In addition, consumers provide information because it is convenient to have the information stored on various platforms.

Privacy Risks

Privacy risks occur when sensitive information is exchanged with marketers. Consumers can perceive many types of risks, such as monetary, physical, social, or psychological. Different types of information requested or acquired from consumers have different levels of perceived risk and thus are perceived to be more or less sensitive. For the most sensitive type of information, such as financial and medical information, there are some laws in place. However, for the rest of information that is provided or acquired, social contracts are relied upon. Consumers assess the risk by considering the reputation and trust of the company to follow through on promises for use and protection.

Privacy risks are considerable when marketers and consumers have countervailing expectations for handling exchanges and the transferred information. Privacy risk is heightened when information is transferred to third parties (Cranor, Reagle, and Aakerman 2000; Culnan 1993; Culnan and Armstrong 1999; Turow 2003), information is used for inappropriate or intrusive communications with consumers (Petty 2000; Slane 2005), and there are security issues (Hoy and Phelps 2003; Miyazaki and Fernandez 2000, 2001).

Protection of Information

Consumers have continued to express a high level concern over information collection by marketers (Cranor et al. 2000; Turow 2003). The challenge for consumers is that consumer information is subject to collection across multiple channels (in store, mail order, telemarketing, mobile devices, and online). To protect information, consumers need to be aware of data collection, provide consent for the collection of information, and have the ability to control the reuse of the information collected through a permission mechanism (Caudill and Murphy 2000; Culnan 1995; Foxman and Kilcoyne 1993). Consumers will achieve privacy when they can control the access and transfer of the information. Another concern is how to protect personal identity and safeguard their financial assets (Milne, Rohm, and Bahl 2004). To protect financial and other information, consumers need to be aware of data collection and have the ability to control the reuse of the information collected through a consent mechanism (Caudill and Murphy 2000; Culnan 1995; Foxman and Kilcoyne 1993).

Trust, Policies, and Signals

Trust

Trust has emerged as a central concept in the marketing literature as it underlies the study of relationship marketing (Dwyer, Schurr, and Oh 1987; Morgan and Hunt 1994). Trust is important for relational exchange because it permits exchange partners to look beyond short-term risks or possible inequities and focus instead on long-term gains. The crux of trust is to facilitate cooperation (Moorman et al. 1992; Morgan and Hunt 1994). There are many definitions of trust. Researchers in the marketing literature define trust as the willingness to rely on an exchange partner in whom one has confidence (Moorman et al. 1992). In another marketing definition, Doney and Cannon define trust as the perceived credibility and benevolence of a target of trust (Doney and Cannon 1997).

These definitions inform the context of consumers and marketers exchanging information. While consumers are offered the promise of benefits that may be realized later on when a relationship evolves, trust is important for starting and continuing with relationships. Trust in this context is the expectancy of a customer to rely upon marketers to keep their promises and treat consumers' personal information fairly. In an empirical research study that investigated trust levels of database marketers, Milne and Boza argued that creating trust is more effective than reducing concern (Milne and Boza 1999). They noted that both trust and concern can affect the probability of purchase in opposite directions, regardless of whether the consumer has done or not done business with the marketer previously. Concern lowers the probability of purchase and trust increases the probability. For existing customers, trust also strengthens the relationship. Milne and Boza's research found trust to be a strong positive influence and concern a strong negative influence of purchase behavior. Moreover, concern is driven more by the level of information sensitivity and trust is driven by whether or not information is shared with third parties.

As discussed next, privacy policies and signaling mechanisms have been attempted by marketers to increase the trust of consumers.

Policies

Controlling access to one's information requires setting boundaries (Altman 1975). One accepted formal approach to establish boundaries in marketer–consumer interactions is the use of privacy policies (Milne and Culnan 2004). With respect to marketer–consumer interactions, fair information practices (FIP) dictate that marketers should provide privacy notices that give consumers a choice in the type of relationship desired with a marketer. From a consumer's perspective, there is a range of boundaries that can be set. At the one extreme, consumers can gain complete control over information collection and intrusion by not allowing any contact by an organization—as can be done through do not call lists. This situation would eliminate a marketer's access to that particular consumer. On the other extreme, consumers can allow all types of intrusions if they fail to implement any control—as in the case of a computer user that has no firewall and does not restrict contact in. Here, marketers are given full access.

Between the extremes of total control and no control are selective control mechanisms, which have come to be known as opt-in and opt-out, opt-in refers to the case when a consumer explicitly gives consent to receive contact and share information ahead of time. Opt-in, which is referred to as permission marketing (Godin 1999; Krishnamurthy 2001), is often touted as central to good marketing practices since it reduces clutter, search costs, and improves targeting precision for marketers. Milne and Boza suggest that opt-in marketing is a trust building form of choice (Milne and Boza 1999). Opt-out refers to the case when a marketer initiates the contact and then provides consumers the option of not receiving future messages or engaging in further data collection. The burden for both situations is on the consumer to take action and decide whether to allow subsequent contact by the marketer. This form of choice favors the marketer in the sense that consumers may be too distracted or lazy to control the access to their information. Research has shown that the format of privacy questions can influence consumer agreement. Opt-in and opt-out are not equivalent and will generate different levels of answers (Bellman, Johnson, and Lohse 2001).

A study conducted by Johnson, Bellman and Lohsein 2002 shows that opt-in and opt-out matter due to the defaults (Johnson et al. 2002). Table 4.1 shows the differences between opt-in and opt-out forms for situations where a box is blank and when it is pre-checked. The ultimate object was to get individual's permission to receive notifications about health surveys.

When the box is blank, the opt-out option resulted in 96.3 percent agreeing to receive notices about health surveys compared to the opt-in option. This is because the opt-in took some type of action beyond the default state. In the opt-out situation, the default was favorable to the objective. However, when the box is already filled in, and the default of the opt-in is more aligned with the objectives than the opt-out, there is

Table 4.1 The role of defaults and framing on privacy

	Opt-in	Opt-out
Box Blank	□ Notify me about more health surveys	□ Do *not* notify me about more health surveys
	48.2%	96.3%
Filled in Box	■ Notify me about more health surveys	■ Do *not* notify me about more health surveys
	73.8%	69.2%

a reversal of the percentages allowing notification. For this situation, the opt-in resulted in 73.8 percent and the opt-out in 69.2 percent. Thus, the results of this research show that consumer privacy can be influenced by the defaults and framing. Unfortunately, some companies try to confuse consumers with tricky language and a pre-ticked box as demonstrated by the following: “Please do not untick this box if you do not wish to not receive no further correspondence.” (New 2013)

The choice of form depends on the purpose of the marketer. Professor Dan Ariely (n.d.) notes the percentage of consumers in European countries who indicate they are willing to donate their organs after they pass away varies considerably by the way the question is asked or framed. For countries whose form utilizes an opt-in format and individuals are required to check a box if they want to donate, the average donations are 15 percent. For countries whose form utilizes an opt-out format, and individuals have to check a box if they do not want to donate, the average donations are 95 percent. The point is that people are cognitive misers and do not check boxes, so setting the default has a big impact on the outcome. Based on established norms for online marketing, the choice of opt-in is considered the best for privacy since the consumer has to make an active decision, which will engender trust.

In the future, it is important to choose the best format when marketers are trying to gather permission while using emerging technologies. Some technologies may not be able to use traditional a priori permission. For example, with ubiquitous technologies such as RFID and motion detected cameras that have or will be used in retail outlets, there is the potential that a great deal of information is collected, some of which may or may not be relevant to the marketing purpose. Further, it is very likely that multiple events, from multiple consumers might be captured, making it hard or difficult to protect consumer privacy. Indeed, retail outlets are becoming very much like websites, where customer movements and actions are tracked. Since consumers are used to anonymity in public spaces, this may be problematic at first. Following current FIP, it might follow that consumers need to be notified that such tracking devices are used in the store with signs at the entrance and throughout the store. Consumers at check-out stands, or through signing up for frequent shopping cards, may also have to give permission for the marketer to use the information being collected with the new technologies. Other researchers have suggested that a priori permission may not be possible and that post hoc log analysis through a privacy audit is the appropriate way to regulate privacy practices with these technologies (Sackmann, Strucker, and Accorsi 2006). Establishing an efficient and effective means to notify consumers of marketer practices and give them choice to opt-in or opt-out continues to be a challenge that needs to be addressed.

The practice of providing online privacy notices online began to be widely practiced at the end of the 1990s. However, the usefulness of online privacy notices has come under fire since they are found to be too lengthy and hard to read due to excessive legal jargon (Milne, Culnan and Greene 2006). Consequently, many consumers are not reading the notices. In a national study, research found that 53.8 percent of the notices are written at a level above a high school education. It also showed that 47.9 percent of Americans over 25 years of age, based on their education levels, could not understand what was written in the notice.

To improve, notices will require a multi-faceted approach (Milne, Culnan, and Greene 2006).

1. Provide incentives for accountability,
2. Develop standards for notices,
3. Use alternative formats such as layered short notices,
4. Focus on comprehension as opposed to readability, and
5. Motivate consumers to read the notices.

Given that consumers are not reading notices, this makes it difficult to provide protection to consumers from more complicated scenarios such as advertising network use of cookies. While consumers have voiced a strong reaction to the use of cookies (Milne and Bahl 2010), it remains to be seen whether they will partake in the protection procedures offered by the Network Advertising Initiative and others.

Providing notices for mobile platforms is important as there is the potential to further invade consumers' sense of privacy as they navigate through public spaces. It is important to track what type of interactions between marketers and consumers need permission and which do not. While the importance of privacy and location privacy issues, in particular, is often voiced by the public, there is always a tension that new products will be introduced that ignore the need to have basic privacy safe guards. The challenge with mobile marketing is that notices are difficult to read on mobile devices with small screens. It is likely that new formats and shorter notices will need to be implemented to improve the situation.

Signals

Getting consumers to visit and engage with a website requires establishing trust. In situations where a reputation is not established, consumers look for signals. This is especially important if they are going to provide information to the marketer through the website or make a purchase. Indeed, the website signals are important for improving buying intentions and have been shown to be relatively more important than privacy/security statements (Belanger et al. 2002). One signal that has shown to be effective is the quality of the website. Websites that are perceived to be of higher quality evoke more trust. However, signals have been shown to be interpreted by in different ways by consumers (Prabhu and Stewart 2001). For example, searchers and browsers perceiving high versus low risk pay different level of attention to website signals (Schlosser et al. 2006).

Another signal that has been offered to consumers is the website seal of trust. The biggest trust seal program is offered by TRUSTe. The services of TRUSTe include assessing, monitoring, and certifying the privacy practices of websites and other devices such as mobile apps, clouds, and advertising channels. TRUSTe assures consumers that the marketer can safely collect information. As of 2012, TRUSTe had certified more than 5000 businesses (TRUSTe 2014). The certification process makes sure that the marketer is in compliance with its own privacy statements and those of the TRUSTe program (www.truste.org).

Research on the effectiveness of a seal program suggests that participation in a seal program is not related to what is reflected in the stated privacy policies. Moreover, when there were seals, consumers were more likely to shop online in highly risky situations. Consumers are more likely to believe that a site has higher privacy standards when there is a seal displayed, although in reality there are no differences in terms of the marketers' policies (Miyazaki and Krisnamurthy 2002).

Ultimately, however, before a consumer shops at a site it is important to make sure their information, especially financial information, is secure. Consumers will likely examine: (1) third party privacy seals, (2) privacy statements, (3) third party security seals, and (4) security features. Of these, Belanger et al. found that consumers valued security more than third party seals, privacy statements, and third party security seals (Belanger et al. 2002). Still, all features should be displayed as consumer reactions to privacy concern are very heterogeneous.

Technology and Information Context

Technology Advances

The technology employed in data collection and marketing efforts will affect the type of boundaries requested by consumers and marketers. The boundary decision is based on a benefit and risk analysis as well as relational needs. In periods of rapid technological change, there are conflicts over the protection of privacy since the perspectives of marketers and consumers differ in the appropriate use of information technology (Bloom, Milne, and Adler 1994). Supporting this assertion is a long history where dating back to photography in the 1890s the introduction of technologies created privacy concerns (Smith 2000). Today, use of cameras, mobile phones, facial recognition, and GPS tracking devices raise questions about the capture and use of information.

Establishing norms between consumers and marketers has focused on the expectation for privacy boundaries (Culnan 1993; Milne 1997; Phelps et al. 2000). These expectations are summarized as:

1. Whether consumer have no boundaries,
2. Whether access by marketers requires the gaining of permission (either through an opt-out or opt-in mechanism), and
3. Whether no permission is given by consumers.

While laws such as the Telephone Protection Act (1991), CanSpam Act (2003), and the Children's Online Privacy Protection Act (2000) help establish some boundaries, privacy policies are the primary means used to establish boundaries for the opt-in and opt-out choices that consumers make. For exchange to be optimized, there is a need for both marketers and consumers to agree on the boundary settings. With new technologies, the boundary setting involves a back and forth process. In the end, these are shaped by discourse through the press, consumer complaint behavior, and in some cases Federal Trade Commission (FTC) review.

A national survey by Milne and Bahl (2010) directly compared consumer segments' and marketer expectations for privacy boundaries associated with the use of eight standard marketing technologies (cookies, biometrics, loyalty cards, RFID, text messaging, pop up ads, telemarketing, and SPAM). In addition, data were collected from marketing vendors and marketing managers using the same set of questions. Comparing the results shows the areas where consumer segments and technologies differ between the groups. The eight technologies examined had different levels of regulation at the time the survey was conducted. For example, telemarketing, text messaging, and spam had some legislative control. Other technologies such as cookies, pop up ads, and loyalty cards were not regulated at a national level, although there was concern about the covert nature of cookies, pop up ads (McCoy et al. 2007; Miyazaki 2008), and loyalty cards (Spychips. http://www.spychips.com/). Some of the new technologies such as RFID tags and biometrics were less known by consumers (Langenderfer and Linnoff 2005; Peslak 2005Tsang, Ho, and Liang 2004).

Table 4.2 groups the technologies as relatively older or newer as perceived by consumers. The technologies are further subdivided by whether the technologies are used primarily for information collection or information communication (delivery or pushing messages to consumers). Within this group of technologies, it turns out that marketers are going to want to use information gathering technologies more than consumers are willing to permit. Interestingly, for the new information gathering technologies, marketers want access but at a reduced level and consumers want control but also at a reduced level. Marketers are either cautious or not as innovative, and consumers are not aware. For technologies that are used to communicate to consumers and push information, consumers want a lot of control and marketers have lower expectations of access. Also regulation with the do not call and CanSpam acts control the older technologies.

Table 4.2 Technology classification

	Older technologies	Newer technologies
Information Gathering	Cookies Loyalty cards	Biometrics RFID tags
Communications	Telemarketing Spam	Text messaging Pop up ads

Details about the percentage of consumers who want to have controls for using a particular technology and the percentage of database marketing vendors and marketing managers who want access to the technologies are shown in Table 4.3. In Table 4.3, control is measured as the sum of not allow and opt-in category percentages. Access is measured as the sum of the opt-out and allow category percentages. The pattern suggests that marketers want more access to technologies that are primarily used for information gathering as opposed to invading consumer environments. Consumers, who prefer control over all technologies, were more protective against technologies that invaded their environment as opposed to those that acquired their information.

When looking at consumer reactions, it is also important to recognize that there are a wide set of opinions regarding desired privacy control. Indeed, the literature also shows that consumers have different concern levels (Dolnicar and Jordaan 2007; Kumaraguru and Cranor 2005; Milne and Gordon 1994). The Harris Polls privacy segmentation scheme consisted of three segments: privacy fundamentalist, privacy pragmatists, and privacy unconcerned (Kumaraguru and Cranor 2005). These range from very concerned to unconcerned.

A segmentation study of consumers in the study of the eight different technologies showed substantial variation of privacy attitudes. Females, older and less educated, wanted more stringent privacy control, while more educated and less time constrained consumers prefer more relaxed privacy controls with opt-in. Similar to the Harris Study, there was a three cluster solution found: restricted, balanced, and receptive, which ranged from very concerned to unconcerned. Their relative size in the population were 42 percent, 40 percent, and 18 percent, respectively.

In Figure 4.2 the comparison of the different segments' preferences for closed, permission based (opt-out or opt-in), and open boundaries shows

Table 4.3 Percent consumers wanting control and marketer wanting access by technology

	Consumer control	Marketing manager access	Database marketer access
Information Gathering			
Loyalty cards	59.3	58.6	84.4
Cookies	83.2	16.8	79.9
Biometrics	72.8	27.2	59.7
RFID	79.7	20.3	61.0
Communication			
Telemarketing	81.3	18.7	51.9
Spam	84.4	15.6	24.9
Pop up advertising	86.0	35.0	46.8
Text messages	94.0	5.0	23.0

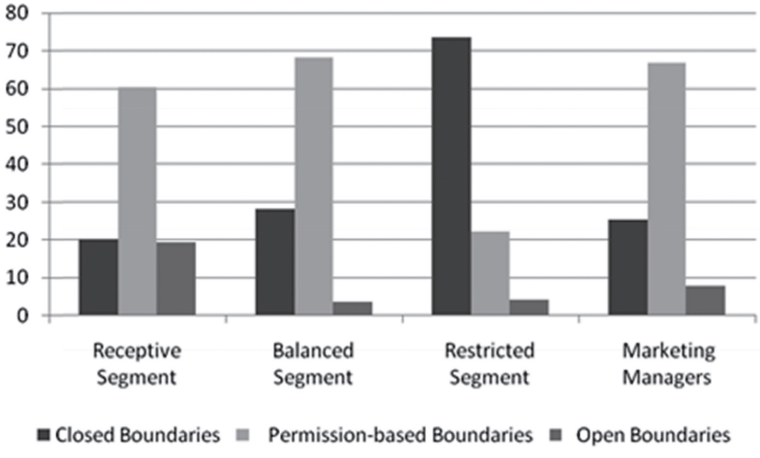

Figure 4.2 Percentage of boundary preferences for consumer segments and marketing managers

the variation within consumers and where similarities exist with managers. The receptive and balanced segments are very similar to the marketing managers. The restricted segment differs and contributes to the dialogue that challenges what marketers are doing. In other words, the restricted segment is most sensitive to open boundaries. It is interesting to note that the restricted segment, while oppositional to marketer desires, represents only 18 percent of the population. Still their voice must be listened to as they affect public opinion through the press and lobbying efforts.

Information Context

In addition to the technology used to collect and communicate information and the role of consumer segments, the type of information request affects consumer willingness to provide that information. Table 4.4 shows consumer willingness to share various types of information with marketers. For example, consumers are least likely to provide social security

Table 4.4 Consumers' willingness to provide information

Least likely to provide	Somewhat likely to provide	Likely to provide
Social security number	Cell phone number	Income level
Security/access codes, passwords	Handwriting sample	Hometown
Financial account numbers	IP address	Shopping behavior
DNA profile	Documentation of grievances	Number of children
Health insurance ID	Home address	Sexual preference
Credit card number	Mother's maiden name	Job title
Passport number	Home phone number	Weight
Finger print	Work contact information	Political affiliation
Driver's license number	Work phone number	Occupation
Family/friend's contact information	Work address	Religion
Law enforcement files	Social network profile	Height
Vehicle registration number	Signed petitions	Marital status
Digital signature	Online screen name	Country of citizenship
GPS location	Birth date	Race
Credit score	Email address	Gender
Medical history	Surveys answers provided to companies	
License plate number	Zip code +4	
Voice print	Place of birth	
Picture face		

number, somewhat likely to provide cell phone number, and likely to provide income level. Underlying the level of willingness is the risk of the information getting in the wrong hands. These harms are discussed in the next chapter.

Marketer Background Factors

Implementing the Marketing Concept

A fundamental principal of marketing is that marketers need information about consumers. As such, information acquisition is tantamount to being a good marketer. Indeed, a fundamental principle of marketing is the marketing concept—which requires the marketer to find out what the consumers want and desire and then configure a product, price, promotion, and place (or distribution) strategy that best suits the customer so that the marketer can gain competitive advantage over other marketers. Having information is said to improve the efficiency of market exchange. The challenge for marketers is how to get information from consumers without violating consumer's sense of privacy.

Technology as a Double Edge Sword

Complicating the process of information acquisition by marketers today is the digital platform upon which most exchanges are made. Now, on Internet enabled platforms, it is easier than ever to collect information on consumers. However, the digital interactions that consumers have with marketers are a double edged sword since the benefits provided consumers may heighten their privacy concerns. The digital benefits offered to consumers include customized product offering, personalized messages, flexible pricing, and shop anywhere convenience on the mobile devices. At the same time, there are costs since the information acquisition activities are not visible. These include transmission of information to third parties, covert web tracking, behavioral advertising, and predictive algorithmic offerings.

Figure 4.3 shows the marketer's offering, in terms of the 4Ps, as exchanged for information. When consumers receive the offering mix, they receive benefits but also face privacy concerns when they provide personal

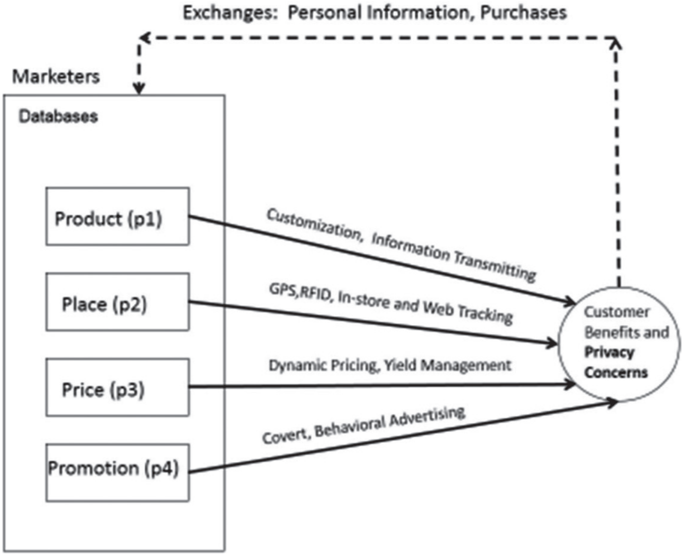
Exchanges: Personal Information, Purchases
Marketers
Databases
Product (p1)
Place (p2)
Price (p3)
Promotion (p4)
Customization, Information Transmitting
GPS,RFID, In-store and Web Tracking
Dynamic Pricing, Yield Management
Covert, Behavioral Advertising
Customer Benefits and Privacy Concerns

Figure 4.3 Technological aspects of four Ps model

information. The figure also show how each of the four Ps has digitally enabled features. The four Ps act as a double edge sword, complicating the cost/benefit tradeoff for information exchanges.

Product. Consumers are able to customize their products online. Whether buying a new pair of tennis shoes from Nike or buying a BMW car, it is possible to select an array of options online and see your product configuration. Nike ID allows consumers to put their name on their shoes, the ultimate in customization on the screen. Market level customization is done by another company named Threadless, an online retailer of T-shirts. Threadless turns to its online community to create and pick the best designs. In addition to giving consumers choice in the product designs across an array of product classes, products themselves will become information transmission devices. For example, cars with tracking devices can send insurance companies information about speed levels. Smart electric grids are reporting consumer usage levels. Health monitors are now being sold that capture and transmit health information to providers. Scoble and Israel (2013) report that many new products will have sensors that capture information about the consumer. While they offer benefits, they also invade one's solitude.

Place. The Internet and mobile devices have had a large impact on the where commerce can take place. Technology has empowered consumers to buy online wherever they may be. Also, GPS devices in the phone help consumers keep in touch with their social network in the physical world. Apps like four square are used to meet up with friends. However, the same technology also has the potential to invade consumer privacy. Consumers are now aware that their movements across the Internet are being tracked. Now technologies such as geofencing are tracking their movement in real space. Like most technologies, geofencing has both benefits and costs to consumers. Geofencing occurs when a physical retailer puts a mileage geographical boundary around the establishment. When a consumer enters the boundary, the retailer can send offers to the consumer via the mobile device. While this sounds desirable at first, if all retailers start this practice one becomes bombarded with messages, further eroding whatever little anonymity a consumer has in public.

Price. Consumers benefit in the online world by having more information about pricing options. For example, consumers can quickly compare prices between competitors by going online. They can also make price comparisons between different channels of distribution and decide if they want to buy in a physical store or online. Pricing online, however, gives marketers many competitive tools. First, it is easy for marketers to gauge demand for a product and for those products in high demand, increase the price. Dynamic pricing and yield management programs have long been used by airlines to extract profits from under-utilized seats. There are new pricing formats also available, including an array of actions, which may or may not benefit consumers. The *Wall Street Journal* reports that Staples online store changed its prices after it determined where the shopper was physically located and determined whether they were within 20 minutes of their competitors—Office Max or Office Depot—brick and mortar stores (Valentino-Devries, Singer-Vine, and Soltan 2012). Digital information also helps set prices in the real world.

There are soda machines that alter prices based on the outside temperature (Hays 1999).

Promotions. Consumers have long responded to advertising and promotions. The Internet and mobile devices have provided consumers a way of easily accessing and storing coupon deals. There is the convenience of having the barcodes for coupons on smart phones read at checkout stands. One type of promotion device that has caused some concern is the marketer's use of behavioral advertising. This is when a marketer is able to send tailored advertising based on information from previous sites visited online. Marketers get this information from ad networks of participating sites. For example, suppose that a salesperson was reading the Boston Globe online newspaper about a ball game to between New York and Boston. Then he booked a flight from Boston to New York for the week. Then for the next website he visited, an ad was served up that advertised the ball game between Boston at New York that week. Some might consider such advertising informative and useful. Others find it creepy.

The previous discussion highlights that online marketing is driven from a database. The strategic interactions around the four Ps with consumers will result in information exchange. However, as a result of these interactions, consumers will receive benefits and also possibly have privacy concerns. Given that information exchange is so fundamental to conducting business today, information flows need to be managed by business.

Privacy: The Fifth P

One solution for managing information flows and improving exchanges between marketers and consumers is to consider privacy as the fifth P. Privacy can directly affect consumer reactions and, through incorporating privacy considerations in the other parts of the marketing mix (four Ps), can improve trust and lower concern. The schematic in Figure 4.4 shows that when managers elevate privacy considerations to the level of the four Ps, the level of trust is improved. Consistent with the FTC's privacy by design recommendation, the fifth P privacy is shown to impact the considerations of the other four Ps. This is done through enhancing transparency and moving away from covert operations that have been

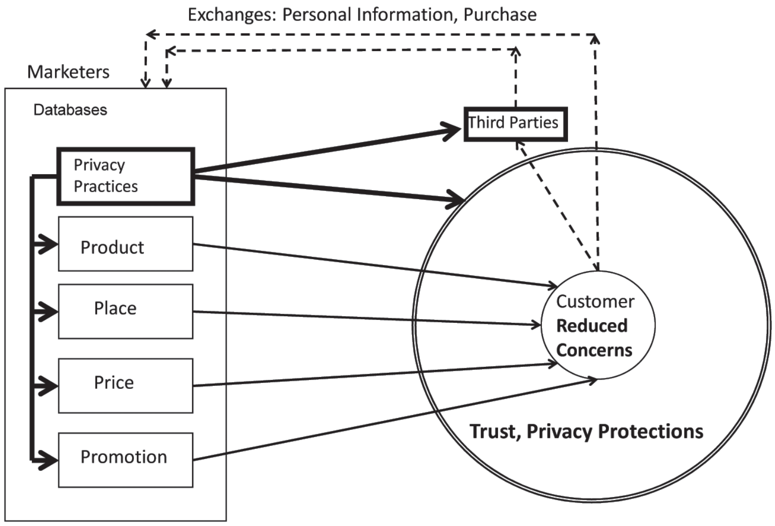

Figure 4.4 Privacy as the fifth P model

demonstrated to cause distrust (Milne, Rohm, and Bahl 2009). Thus, all the data collecting activities associated with the implementation of any of the four Ps should be transparent to consumers. In addition, the fifth P considerations should be present in the management of third party relationships so that they are also transparent to consumers.

As has been discussed, improving trust is an effective approach for reducing privacy concern in database marketing situations (Milne and Boza 1998). Trust in marketing is defined as the "willingness to rely on an exchange partner in whom one has confidence" (Moorman et al. 1992) and "as the perceived credibility and benevolence of a target of trust." (Doney and Cannon 1997) The first definition suggests that the consumer must have beliefs based on past experience that it is OK to rely on the marketer even under conditions of uncertainty. The second definition suggests that the consumer must trust the marketer's credibility. For the marketer, it is more effective to promote trust activities rather than trying to reduce concern. Thus, transparent communication through clear disclosure of policies is better than trying to cover up and obfuscate privacy practices or even engage in covert practices.

To improve trust online, suggestions have ranged from improving security of online sites, being transparent about data collection and relationships with third parties, being authentic in communications, using appropriate opt-in and opt-out mechanisms when necessary, and displaying third party trust certifications. With these improvements, consumers should be more willing to exchange information and conduct commerce online.

Company Policy and Ethics

When it comes to creating a privacy and ethical conduct policies, most companies are guided by the FIP. These principles, discussed at more length in Chapter 6, provide guidelines for companies to create policies around. In brief the principles call for:

1. Consumers to be given notice of and have awareness of data collection practices,
2. Consumers to be given choice of and to provide consent to the collection of the data and its use,
3. Consumers to be given access rights to review their personal information stored on databases, and
4. Consumers to be given assurance backed up with action that their data is secured.

Over time, there has been constant pressure put on companies to be compliant with FIP. In 1998, a survey of 365 organizations (Milne and Boza 1998) belonging to the Direct Marketing Association (DMA) showed limited following of the fair information principles: 38 percent notified consumers about the gathering of personal information, 33 percent indicated the use of the information, and only 26 percent asked permission to use the information. Moreover, studies at the time found that only 10 percent of 361 organizations' websites reviewed practiced all four FIP of notice, choice, access, and security (Culnan 2000). With the FTC putting companies on notice to be accurate with their notifications and recommending that notices follow FIP, there was some improvement at this time. A longitudinal study at the time showed that from 1998 to 2001 the percentage of popular websites posting privacy notices increased from 44.8 percent to 98.6 percent (Milne and Culnan 2002). The compliance rate for all websites was not as high with only 76.7 percent posting notices. In general, the popular websites were found to be more likely to have FIP elements in the website. Today, posting privacy notices that follow FIP is the norm and is expected for all sites.

Given the industry changes, self-regulation has continued to be the lever for industry ethical compliance. Among the biggest proponents and lobbyists of self-regulation is the DMA. In their association guidelines for ethical business practices, they suggest that companies follow compliance best practices which are over and above baseline principles. They also ask its members to review the Fair Information Practices and Principles.

Examples of the DMA's best principles are found in their "Do the Right Thing" document. The principle suggestion is for companies to do the right thing, not just what is legal. For example, the DMA asks that its members abide by consumer choices for offers regardless of the channel used. They offer mail preference services, increased do not contact lists, telephone preference services, and the DMA e-mail preference services. They also encourage companies to make sure third party vendors are compliant as shown by this following best practice statement (Do the right thing 2009).

> **Best Practice**
>
> You should use and/or inform all DMA member clients that they should use e-MPS when processing third party e-mail lists, and require all non-member clients who refuse to use e-MPS in connection with third party e-mail lists to sign an appropriate waiver acknowledging their refusal to use e-MPS as requested.

In all, the DMA document is 97 pages long and contains 54 articles of instruction to the marketers.

In addition to the self-regulatory efforts, privacy groups have created services for consumers to check on individual company policies. One such organization is PrivacyChoice, which was started in 2009 to help facilitate privacy among websites and apps and help inform consumers. Their product, Privacyscore, is a tool that consumers can use to assess the privacy risk of using a website with respect to both personal and anonymous data. According to the website http://privacyscore.com/faq a privacyscore of 100 would indicate:

- The site's policies expressly limit the sharing and use of personally identifiable data in these ways:
    - Personal data (like name, phone number, and e-mail address) should not be provided to marketers without permission and should be deleted on request.
    - A user's request to delete personal data should be honored.
    - Notice should be provided in the case of disclosure of personal data pursuant to legal process or government requests, where legally allowed.
    - If service providers have access to personal data, their use of it should be restricted by contract.
- All trackers seen on the site pledge to respect anonymity, choice, and boundaries, and should be subject to industry accountability.
    - Personal data should not be collected or used, or should be separated from behavioral data.
    - Boundaries should be recognized in areas like health conditions and financial data.
    - Choice should be provided as to whether data will be collected or applied for the purpose of ad targeting.
    - Accountability should be provided through both regular compliance reviews of internal processes by industry organizations (such as the Network Advertising Initiative) or independent auditors, as well as ongoing external monitoring of practices by industry organizations.

Table 4.5 shows the privacy scores for six popular websites.

These numbers were generated from the program on the privacyscore.com website. Wikipedia has a perfect score of 100 that puts it in the comfort range, Microsoft and Facebook scores are in the caution range, and Yahoo, Google, and Amazon scores are in the concern range. All the sites with concern levels do poorly in informing consumers about tracking. In particular, they do not confirm user anonymity. They also retain the

Table 4.5 PrivacyScore.com ratings for six popular websites

	Yahoo	Google	Microsoft	Facebook	Amazon	Wikipedia
Overall score	68	65	89	89	65	100
Rating	Concern	Concern	Caution	Caution	Concern	Comfort
Site's policies	45	45	45	45	30	50
Personal data generally not shared	30	30	30	30	30	30
Deletion request are honored	10	10	10	10	0	10
No assurance of notice if data are requested	0	0	0	0	0	5
Vendor confidentiality is confirmed	5	5	5	5	5	5
Tracking	23	20	44	44	30	50
Do they confirm user anonymity	No	No	Yes		No	
Do they observe sensitive boundaries	Yes	Yes	Yes		No	
Do they provide an opt-out choice	Yes	Yes	Yes		Yes	
How many months do you collect data	48+	18	48		48	
Who provides industry over site	NAI	No	NAI		No	
	DAA	DAA	No		No	
Number tracking companies	6	Just Google	2	4	1	0

information collected about consumers for 48+ months. While Yahoo has six additional tracking companies accessing the sites, Google and Amazon do not as they do most of the tracking themselves.

With the revelation that the National Security Agency (NSA) has been monitoring U.S. citizen's phone records, there has been greater concern over whether particular websites will share information with government agencies. To this effect, the Electronic Frontier Foundation examined whether certain companies' policies would provide the government personal data upon demand. Consumers, when providing this information to companies, are entrusting that this information will not be transferred. There are sensitive conversations, thoughts, photos, and so on loaded and stored upon company web servers. According to the 2013 survey, Yahoo does not do a good job standing up for the consumer. Yahoo does not (1) require a warrant for content, (2) tell users about government data requests, (3) publish law enforcement guidelines, or (4) fight for users' privacy rights in Congress. Table 4.6 shows the results of the who has your back survey?

Regulation and Industry Norms

Both industry regulation and industry norms affect consumer relationships with companies. As discussed earlier, companies in the direct marketing industry have certain ethical guidelines that they are supposed to follow if they are part of a trade association. Related to the norms that have evolved is the type of information that is stored and transferred within the industry. For example, the financial industry, which deals with very sensitive financial information, has the highest level of consumer concern. Not surprisingly, the industries with the highest level of sensitive information are more likely to be regulated.

A 2013 survey measured consumer concern about handing over personal identifying as well as the level of trust for companies across 17 different industries (Milne and Ross 2013). Table 4.7 organizes these industries showing high/low concern industries crossed by high/low trust industries. A star indicates if there are specific laws applicable to data handling in these industries. The industries in the high concern and low trust sector tend not to be highly regulated, with the exception of credit

Table 4.6 Who has your back survey

	Yahoo	Google	Microsoft	Facebook	Amazon	Wikipedia
Requires a warrant for content	No	Yes	Yes	Yes	No	*
Tells users about government data requests	No	No	No	No	No	*
Publishes transparency reports	No	Yes	Yes	No	No	*
Publishes law enforcement guidelines	No	Yes	Yes	Yes	No	*
Fights for users rights in courts	Yes	Yes	No	No	Yes	*
Fights for users' privacy rights in congress	No	Yes	Yes	Yes	Yes	*

www.eff.org/who-has-your-back-2013
*Not in survey

Table 4.7 Trust and concern levels for 17 industries

		Trust	
		Low	High
Concern	High	Insurance companies Magazine publishers Catalog companies Political organizations Telephone companies Direct marketing clubs Credit card issuers* Internet providers™	Employers* Banks that process checks*
	Low		Book stores Alumni associations Grocery stores Charities Video stores* Drug stores* Airlines

card issuers. The data suggest that regulation does have the effect of improving trust.

Consumer Background Factors

Consumer Perceptions

Consumer perceptions are heterogeneous and affect information behavior and, ultimately, decisions to exchange information. Consumer perceptions vary based on need for marketing and information benefits, their desired level of convenience, level of knowledge, and information sensitivity. In conjunction, demographic background affects these perceptions and the risk tolerance.

Demographics

There is a long tradition in understanding how demographics affects consumer willingness to provide information. A very influential article by Phelps et al. examined consumer willingness to provide (Phelps et al. 2000). They found that the background variable of education was influential in predicting privacy concerns. Consumers with more education tended to be more concerns. Other research has found females to take more effort in protecting their information (Hoy and Milne 2010; Milne, Labrecque, Cromer 2009).

Risk and Technology Tolerance

Consumers vary in terms of risk and technology tolerance. Much of what underlies this perception is self-efficacy in being able to use technology and engage in online risky behaviors. Research has found high self-efficacious individuals are less likely to take high risk actions (those that are unprotected) and more likely to engage in risk reducing behaviors, such as those that protect information (Milne, Labrecque, and Cromer 2009). Thus, when consumers face risk and also have the skills to handle the risk, they are more active in controlling their online environment. The confidence in their own ability reduces the perceived risk through being able to undertake protective actions.

Summary

This chapter examined information exchange and privacy in the marketplace. it presented an information exchange model that depicts the market and consumer background factors and decision processes affecting the information exchange behavior between marketers and consumers. The chapter began by reviewing marketing and exchange theory. Then it reviewed the four types of information exchanges that occur between marketers and consumers:

1. Information requests and disclosure statements made by marketers,
2. Information provision and marketing contact: volunteered information exchange by consumers with subsequent contact by marketers,
3. Information capturing without consent: observed information gathered by marketers that is not volunteered by consumers, and
4. Information sharing.

These information changes were then viewed as social contracts, and the benefits and risks from the exchange were articulated. Trust, privacy policies, and signals were then discussed as mechanisms for facilitating exchanges. Also discussed was the role that technology has in deciding the boundaries of protection for information exchange and the different perspectives shared by consumers and marketers. Next, company and consumer factors affecting exchange were examined. For companies, the role of technology was shown to influence the implication of the marketing concept, affecting each of the four Ps. A model was presented that suggests that privacy can serve as the fifth P to improve exchange. Next, for companies, policies, ethics, regulations, and industry norms were discussed. Lastly, the consumer perceptions were briefly covered, focusing on the role of demographic background and technological self-efficacy.

CHAPTER 5

Information Based Privacy Harms

Chapter Overview

The last chapter examined the role of information exchange in the marketplace and its implications for privacy. In this chapter, you will learn about the information sensitivities and perceived risks related to different types of information. In the second part of the chapter, you will learn about a range of exchange harms including intrusion, data collection, share, and data processing harms. There is also a discussion of the harms emanating from the applications of specific technologies.

Information Sensitivities and Perceived Risks

Consumer willingness to disclose information is dependent on the perceived risk of doing so and the associated harm if others use the information. The higher the risk, the more sensitive the information is considered and the less likely consumers are to disclose. As discussed in Chapter 2, personal identifying information (PII) is considered very sensitive since it can be used to identify people. If this information is in the wrong hands, one's identity (and money) could be stolen or, at a minimum, their privacy invaded. Thus, information such as credit card number, social security number, finger prints, medical history, IP address, cell phone number, and GPS location are considered PII and sensitive. In addition to PII, other types of information are considered sensitive. With predictive modeling techniques, all types of data can be combined and put into models to identify consumers and their particular market behaviors. One way to examine the sensitivity data is to assess the level of risk associated with the data being shared.

Examining consumer-perceived risk through a multidimensional lens captures a more complete picture of what and why consumers consider different types of information sensitive. Researchers have suggested that the following four risk dimensions are useful for understanding disclosure behavior and privacy concern (Jacoby and Kaplan 1972; Milne, Hajjat, and Markos 2014).

- Monetary,
- Physical,
- Psychological, and
- Social.

Focusing on how risk affects consumer decisions provides a more accurate understanding of consumer concerns rather than viewing them simply in terms of information sensitivity. By understanding the particular risk underlying behavior, managers can focus on consumer objections that inhibit them from providing information.

Monetary Risk

Monetary risk is one of the most protected. The threat of monetary risk affects actions consumers take to keep information secure, whether to share information with third parties, and the steps taken to block hackers (Berghel 2000; Collier and Bienstock 2006; Gross and Acquisti 2005; Weiss 2008). In addition, when financial information is combined with other database activities of information matching and aggregation of data, this leads to more monetary risk exposure.

Identify theft occurs when a thief steals personal information and uses it without permission of the owner. The most sought after information is one's name, address, social security number, credit cards, and bank account information. This information can get in the wrong hands when one shares or posts on the Internet or stores information in an unsecured manner on a computer. It also happens from mail theft, stolen wallets and purses, and from dumpster diving—when one rummages through the trash for documents. Indeed, while online identity theft is most feared, many overlook non-online protection activities (Milne 2003).

Monetary risk can also occur when a marketer's computer files are compromised. In December of 2013, a cyber-attack breached Target and several other retailers. The stolen information included addresses, e-mails, and phone numbers of 70 through 110 million customers. Other breaches included credit card numbers and verification codes (Yang and Jayakumar 2014). This was the biggest known breach at the time the theft was discovered. It is unsettling to note that within the last decade there has been an increase of security breaches (Haley 2014; Kelly 2013). The year 2013 saw an increased attack on medium sized businesses, more mobile malware that invaded consumers' privacy, a growth of ransomsomeware, and security breaches occurring through the Internet of things platforms.

Social Risk

Social risk is an important consideration since consumers are conscious of their online reputations and identities. Thus, in disclosing information consumers are likely to weigh the impact of the disclosure on their digital reputation, online ratings, recommendations, and credibility in online communities and social networks (Dellarocas 2010; Hogg and Adamic 2004; Peters and Stelter 2010;). With social risk, consumers will pay attention to what is put in user profiles (and who has access), the period and time that information is stored online, and the control they have to delete information from postings.

The story of the dog poop girl illustrates the power of the Internet to shape reputation. In South Korea, a young girl's dog pooped on the train and she refused to pick it up. Another passenger took a picture of her and posted it online where it got picked up by a popular blogger. The story went viral and was picked up by the South Korea mainstream media. The girl was recognized, harassed, and shamed. As a result, she dropped out of the university she was attending.

Whether or not the girl deserved such harsh treatment is up for debate. However, in other cases, people's reputations can be harmed without proper justification. It might be that an embarrassing picture from college days posted by someone else is on the Internet, a person's medical past that could damage their careers, or a small business that had some bad reviews from an embittered customer. Research has shown that it is difficult to manage information online and, in many cases, people may forget that some less favorable information is on the web. This is why setting up procedures such as a Google Alerts is a good idea to guard against reputation damaging postings. In situations where it is hard to remove reputation damaging information, individuals and companies are turning to companies such as Reputation.com to help manage their reputation.

Psychological Risk

Psychological harms can occur when disclosures are made that make people feel uncomfortable or regretful. Psychological harm can occur when privacy is not afforded for normal psychological functions. Online environments such as Facebook are ripe for psychological risk (Youn 2005, 86–110). This is because the environment is used for identity development at the expense of privacy. While there are protections available for individuals to remain anonymous, it requires individuals to show reserve when links to one's real world identity are provided. This proves to be difficult. Often much is shared that can cause psychological harm after the fact.

Psychological harm can also occur from cyber stalking and cyber harassment. Cyber stalking is when there is a specific threat or pattern toward malicious behavior. Cyber harassment usually does not involve a credible threat. Online bullying is quite prevalent with malicious comments (threats, distress, slander, taunting, hate speech, physical danger), unwanted exposure, badmouthing, discrimination, and insults leading to a negative social impact on self-esteem, embarrassment, or even physical harm (Adam 2002; Gross and Acquisti 2005; Salter and Bryden 2009). A report on high school Facebook users included the story of a girl being bullied by another girl who was trying to get others to post comments that suggested the victim commit suicide. Fortunately the victim's friends stood up for her and the bully apologized (Christofides, Muise, and Desmarais 2010).

Physical Risk

Online behaviors can have real world consequences. Facebook, for example, has been blamed for harming marriages (Toor 2010) as old flames are reunited online and harmful to one's health by diminishing the levels of face-to-face encounters which are essential for health (Stolze 2009). The other physical risk happens when online information provides bullies or stalkers with a victim's real space location, which leads to physical harm; Or when the bullying, harassment, physical-stalking, and physical threats lead to self-destructive behavior, social influence, and suicide (Eckholm and Zezima 2010; Hoffman 2010; Salter and Bryden 2009). To protect from physical risk, it is important to protect information that can be used to identify the whereabouts of a person in a physical space.

The Perceived Risk of Different Information Types

A study was conducted to understand how 52 specific types of information relate to monetary, social, psychological, and physical risks (Milne, Hajjat, and Markos 2014). Some of the information types were classified as PII and other types were not. A sample of 400 adults was asked to identify the type of risk that each of the information items represented. For each information choice an individual could choose none, some, or all of the risks. Respondents also reported how sensitive each source of information was and whether they were willing to disclose the information. A summation of the percentage of respondents who felt there was a risk was calculated for each information type.

To better understand the multivariate structure of the data, a principal component analysis was run on the average risk percentages for the 52 information types. A two-dimensional solution was found. The technologies were then clustered into six segments. A map showing the two-dimensional positions of the information types is presented in Figure 5.1. Figure 5.2 overlays the cluster boundaries and plots vectors that help describe the two-dimensional space. The numbers reflecting information sensitivity, the four risk scores, and willingness to provide information, for each information type, grouped by cluster is shown in Table 5.1.

The table shows the average scores for the information types. Information sensitivity and willingness to provide are 10 point scales, with 1 = low and 10 = high. The four risk items are scored from 0 to 1 where 0 indicates 0 percent of the sample felt this was a risk and 1 indicates 100 percent felt this was a risk. Overall information sensitivity for the

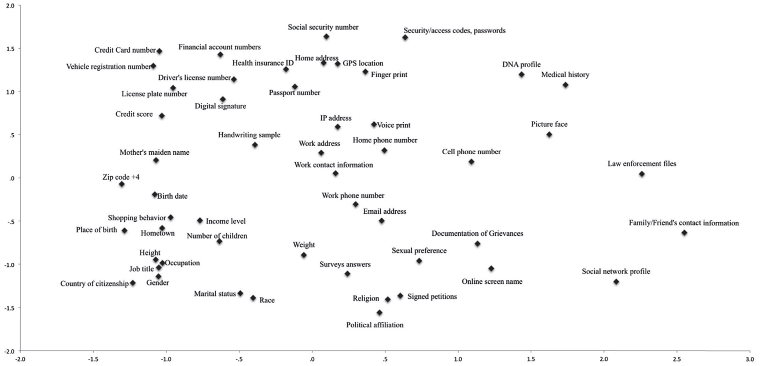

Figure 5.1 Risk similarity of 52 types of information along two dimensions

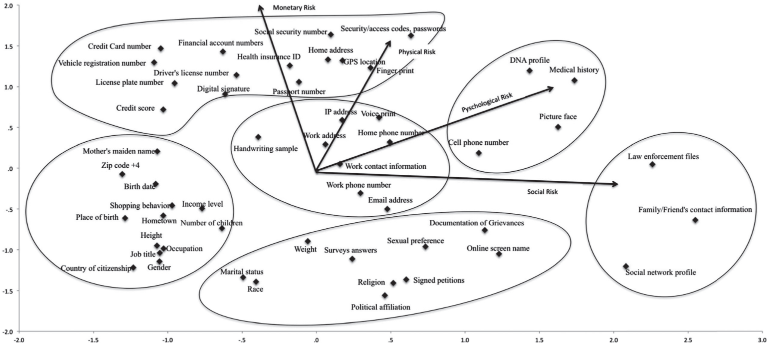

Figure 5.2 Relationship of six information clusters with four risk vectors

52 items was 6.82 out of 10 and the willingness to provide had an average score of 3.45 out of 10. Thus, in general, people are sensitive about sharing information publically and are not much willing to share. On average 42 percent and 39 percent of the sample felt the technologies exhibited social and monetary risks, and 31 percent and 27 percent felt the items exhibited psychological and physical risks. For each information type in the table, the score for each variable is highlighted if it was above the average.

- Cluster 1 represents 15 demographic items: mother's maiden name, birth date, income level, place of birth, zip code +4, hometown, number of children, shopping behavior, job title,

Table 5.1 Information sensitivity, risks, and willingness to provide information for 52 information types

Information Type	Information Sensitivity	Psychological Risk	Social Risk	Monetary Risk	Physical Risk	Willingness to Provide	Cluster
All types of information	**6.82**	**0.31**	**0.42**	**0.39**	**0.27**	**3.45**	
Mother's maiden name	7.39	0.24	0.32	0.60	0.16	2.55	1
Birth date	7.14	0.25	0.29	0.46	0.11	3.83	1
Income level	6.21	0.23	0.36	0.42	0.10	4.58	1
Place of birth	5.88	0.16	0.30	0.33	0.15	4.51	1
Zip code +4	5.67	0.18	0.24	0.21	0.39	4.47	1
Hometown	5.54	0.19	0.29	0.18	0.26	4.74	1
Number of children	5.27	0.24	0.32	0.14	0.22	5.31	1
Shopping behavior	5.09	0.22	0.33	0.42	0.10	5.23	1
Job title	4.91	0.18	0.31	0.20	0.10	5.45	1
Occupation	4.59	0.18	0.32	0.23	0.10	5.93	1
Marital status	4.22	0.22	0.37	0.11	0.08	6.55	1
Country of citizenship	3.89	0.13	0.31	0.16	0.11	6.80	1
Height	3.84	0.23	0.24	0.08	0.15	6.30	1
Race	3.70	0.21	0.39	0.09	0.10	7.02	1
Gender	3.42	0.19	0.28	0.09	0.13	7.07	1
Cluster 1 Average	**5.11**	**0.20**	**0.31**	**0.25**	**0.15**	**5.33**	
Documentation of grievances	7.08	0.41	0.54	0.24	0.14	2.52	2
Surveys answers provided to companies	5.85	0.32	0.44	0.18	0.07	4.41	2
Signed petitions	5.84	0.27	0.54	0.14	0.12	3.26	2
Online screen name	5.82	0.32	0.64	0.28	0.14	3.82	2
Sexual preference	5.35	0.36	0.48	0.11	0.18	5.36	2
Weight	4.78	0.36	0.33	0.09	0.12	5.52	2
Political affiliation	4.63	0.24	0.53	0.09	0.11	5.86	2
Religion	4.19	0.30	0.49	0.08	0.10	6.22	2

(contiued)

Table 5.1 (continued)

Information Type	Information Sensitivity	Psychological Risk	Social Risk	Monetary Risk	Physical Risk	Willingness to Provide	Cluster
Cluster 2 Average	**5.44**	**0.32**	™	**0.15**	**0.12**	**4.62**	
IP address	7.87	0.33	0.44	0.47	0.42	2.49	3
Home phone number	7.70	0.39	0.43	0.33	0.39	2.55	3
Voice print	7.27	0.42	0.43	0.52	0.31	2.27	3
Work address	7.13	0.27	0.44	0.33	0.48	2.91	3
Work contact information	7.09	0.30	0.44	0.32	0.38	2.67	3
Work phone number	6.89	0.30	0.47	0.30	0.29	2.70	3
E-mail address	6.72	0.34	0.49	0.35	0.16	4.04	3
Handwriting sample	6.67	0.30	0.39	0.58	0.24	2.45	3
Cluster 3 Average	**7.17**	**0.33**	**0.44**	**0.40**	**0.33**	**2.78**	
Social security number	9.55	0.43	0.42	0.89	0.34	1.39	4
Security/ access codes, passwords	9.45	0.47	0.48	0.85	0.38	1.40	4
Financial account numbers	9.41	0.37	0.34	0.90	0.25	1.42	4
Credit card number	9.40	0.35	0.28	0.91	0.23	1.52	4
Passport number	9.06	0.33	0.42	0.67	0.40	1.58	4
Health insurance ID	8.90	0.37	0.39	0.74	0.36	1.50	4
Finger print	8.68	0.39	0.45	0.63	0.47	1.63	4
Driver's license number	8.40	0.29	0.38	0.71	0.40	1.81	4
Digital signature	8.35	0.33	0.35	0.74	0.24	1.99	4
GPS location	8.32	0.36	0.36	0.30	0.75	1.99	4
Credit score	8.31	0.29	0.32	0.79	0.14	2.12	4
Home address	7.97	0.35	0.37	0.39	0.69	2.54	4
Vehicle registration number	7.80	0.25	0.30	0.69	0.45	1.93	4

Table 5.1 (continued)

Information Type	Information Sensitivity	Psychological Risk	Social Risk	Monetary Risk	Physical Risk	Willingness to Provide	Cluster
License plate number	7.03	0.25	0.30	0.55	0.48	2.16	4
Cluster 4 Average	**8.62**	**0.35**	**0.37**	**0.70**	**0.40**	**1.78**	
DNA profile	9.22	0.54	0.49	0.43	0.54	1.49	5
Medical history	8.79	0.58	0.53	0.48	0.45	2.15	5
Cell phone number	8.04	0.44	0.51	0.35	0.34	2.44	5
Picture face	7.33	0.48	0.56	0.31	0.49	2.32	5
Cluster 5 Average	**8.35**	**0.51**	**0.52**	**0.39**	**0.46**	**2.10**	
Law enforcement files	8.33	0.51	0.67	0.33	0.36	1.92	6
Family/Friend's contact information	8.28	0.42	0.80	0.30	0.30	1.84	6
Social network profile	6.62	0.37	0.74	0.18	0.20	2.97	6
Cluster 6 Average	7.74	0.43	0.74	0.27	0.29	2.24	

occupation, marital status, country of citizenship, height, race, and gender. Consumers are more likely than average to share this information. The one exception is mother's maiden name, which is sensitive due to a high monetary risk. (It is often a security question for banks). The rest of the information is not found by the consumers to contain much risk.

- Cluster 2 contains eight information types that contain more social and psychological risk than general demographics in cluster 1. The items include documentation of grievances, survey answers provided to companies, signed petitions, online screen name, sexual preference, weight, political affiliation, and religion. Consumers are still willing to provide this information, with the exception of the items documentation of grievances and signed petitions.

- Cluster 3 contains work-related information that consumers are not willing to provide. Items include IP address, home phone number, voice print, work address, work contact number, work phone number, e-mail address, handwriting sample. Across most items there is a physical risk element. Interestingly, the more biometrically related data of voice prints and writing samples had some monetary risk. E-mail was the only type of information from this group that consumers were more willing than average to provide.
- Cluster 4 represents the high monetary risk information, and not surprisingly has the lowest willingness to provide. The items include social security number, security/access codes/passwords, financial account numbers, credit card number, passport number, health insurance ID, finger print, driver's license number, digital signature, GPS location, credit score, home address, vehicle registration number, license plate number. The top monetary risk items out of the 14 items in this cluster were social security number, passwords, financial code numbers, and credit card numbers.
- Cluster 5 has four items: DNA profile, medical history, cell phone number, and picture face. They are all considerably highly sensitive and each has psychological, social, and physical risk.
- Cluster 6 has three items distinguished by the highest average social risk: law enforcement files, family/friend's contact information, and social network profile. It is interesting that social network profile information was seen as a social risk by 70 percent of respondents. However, the average rating for information sensitivity was below the sample means.

As shown in the previous section, there are varying levels of risk attributed to different types of information. Consumers can be harmed when information is mishandled. The next section describes four classes of harm that can occur from information exchanges between a marketer and consumer.

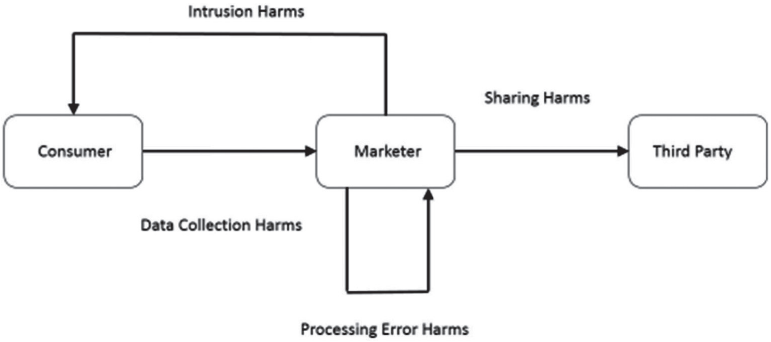

Figure 5.3 A model of information harms in marketing

Information Harms in Exchange

Information exchanges present situations where different processes lead to consumers having various types of information harms, which are possible with a marketer's interaction with consumers (Solove 2008). These four harms shown in Figure 5.3 are:

- *Data collection harms*, when data are collected both with and without the consumer's permission,
- *Processing errors harms*, which occur when this information is manipulated and combined with other information which may vary in levels of accuracy,
- *Intrusion harms*, which occur as a result of the information collected or in the effort to collect more information, and
- *Information sharing harms*, which occur when information is shared with third parties.

Harms from Information Collection

The manner in which a marketer collects information can harm consumers. Much of the harm comes from unauthorized data collection or intrusions into a consumer private space. The two types of information collection that lead to harms are:

- Surveillance and
- Interrogation.

In the marketing context, surveillance is capturing information by listening or recording. Harm can occur from the marketers installing online cookies and storing records on electronic devices. The recording of a consumer's clickstream is a form of surveillance. The practice of behavioral advertising, which relies upon networks of sites tracking sites a consumer visits and what contact they click on while at the site, is also a form of surveillance. So are video cameras in retail stores and the use of phone signatures to track consumer paths through the store. Another form of surveillance is frequent shopper cards and credit cards, where all one's purchases are captured. The harm that comes from surveillance occurs when consumers find out that covert data collection had been taking place or when this information is used in ways not specified by the consumer. This is what makes these practices different than traditional market research.

Interrogation occurs when consumers are asked questions during a survey or interview. Sometimes the information provided by consumers is completely voluntarily, other times consumers are required to provide the information as part of an exchange, for example, to get a "free" e-book. Harm can come when consumers are sent surveys they do not want, when their survey responses are not secure, or if there are continued requests for information after the initial exchange of data. The intrusions are a harm since consumers consider their time a scarce resource and often make decisions to avoid data collection interrogations.

Harms from Information Processing

The manner in which databases are built, maintained, and secured creates potential harms for consumers. The specific information process harms come from:

- Aggregation and
- Security.

Aggregation is the combining of data from disparate sources. In building databases, companies are now combining different types of information, which as stand-alone pieces of information are harmless. However, the aggregation of different pieces of information can potentially create harm when a full profile of a person if formed, which was not intended by the individual. Identification can be a problem when information is linked to a specific individual. This is indeed the greatest harms from information processing can occur.

Security refers to keeping information safe and not falling into unauthorized uses. A major harm to information processing is when the keeper of the information does not keep the information secure. Consumers are exposed to identity theft risks when careless leaks and improper access occurs. The threat of identity theft is real, with 13.1 million Americans victims of this crime in 2013 (Rogers 2014). When consumers are notified of the security breaches, they often have to cancel credit cards and endure the transaction costs for the new card acquisitions. In general, fraud raises the costs that all consumers have to pay.

Harms from Intrusions

Marketers in their communication efforts are pushing information to consumers in the form of e-mail, texts, phone calls, and online ads. The specific harms from intrusions include:

- Invasion and
- Decisional interference.

Invasion is the interruption into one's private life. It usually invades one's solitude and is not appreciated by consumers. Historically, direct mail and telemarketing have been sources of intrusion. Through grass root consumer movements and legislative action, the flood of junk mail and telephone calls at dinner time has been thwarted with do not mail (Direct Marketing Association n.d.) and do not call lists (Shookman 2013). Now, with e-mail, there is the potential harm from unwanted spam. While the definitions of spam vary widely, spam is simply unwanted e-mail from many consumers' perspectives. Similarly, unwanted advertising online is also considered harmful from some consumers' perspectives.

Decisional interference occurs when a person's decisions about private affairs are affected by others or the presentation of information. Augmented reality has been argued to interfere with decisions, and opens up the possibility of consumer harms when displays are distorted through optical illusions (Brinkman 2011).

Harms from Information Sharing

Marketers need to pay attention to whether they have permission from consumers to share information, especially when it is considered sensitive or is considered risky by consumers. The specific harms from information sharing include:

- Breach of confidentiality,
- Disclosure,
- Exposure,
- Blackmail,
- Appropriation, and
- Distortion.

Breach of confidentiality occurs when one does not keep one's promise and information is not kept confidential. This typically pertains to relationships where privacy is implied such as with a lawyer, psychologist, or other medical professional. However, breaches can also occur when a privacy agreement was made and then actions were taken to break the agreement. For example, in 2013, there was an investigation into whether Facebook's new privacy policy broke older agreements that were mandated by a FTC settlement (Sasso 2013).

Disclosure is when a person's reputation is affected by revealing truthful information about them. Social networks have been a source of harm to consumers either by posts and tagged pictures by others or self-disclosures that were passed on to unattended others. For example, there have been many cases of where self-disclosures on Facebook have gotten individuals fired. These include a bank intern who went to a party instead of a family emergency, a new employee who called her job boring, a teacher fired for drinking on vacation, and a waitress who insulted her customers (Bracetti 2012).

Exposure occurs when a person's privacy is exposed to others. Social media do this by displaying one's friend behavior to all of those who are connected to the individual. While some actions are not considered private, others might be. The other type of exposure is when an individual's pictures are posted that they do not want posted. Although pictures from public events do not need permission, caution should be used where there are expectations of privacy.

Blackmail is when one threatens to disclose information unless something is exchanged. There are scams on Skype that lure users to expose themselves on camera by making them believe they are chatting with an attractive man or woman. With the image captured, the person is blackmailed for money with the threat of telling family or friends or publically posting the pictures (Wright 2013).

Appropriation is when someone's identity is taken to serve another's aims or purposes. There is the interesting case of Doug Rickard who takes pictures from screen shots of Google's street view. While this work has been displayed at the San Francisco Museum of Modern Art, there are critics who say he has misappropriated the images (Zhang 2013). In social media, misappropriation can also occur. The term catfishing refers to someone who steals images and uses them to represent their online image and then makes up details to attract romantic interests on social media sites.

Distortion is when one discloses misleading or false information about another. Consumers can be harmed if the distortion is about them. Consumers can also be harmed if they make decisions based on distorted information, which has been reported to occur with consumer reviews of products (Besbes and Scarsini 2013). Distortion can also occur from companies. Recent fake reviews on Yelp have led the state of New York to levy fines against companies (Masnick 2013).

Overall, the increased accessibility of information is leading to more harm. Information that is put online can spread quickly and is not constrained locally, it goes global. Moreover, the information does not go away as it is stored indefinitely (Mayer-Schonberger 2009). All these factors increase the possibility of harm.

Harms from Specific Technologies

The last section reviewed the types of harms that occurred between interactions between marketers and consumers. In this section the focus is on five specific harms that are tied to specific information technologies:

- Spam,
- Covert marketing,
- Stalking,
- Geofencing, and
- Facial recognition.

Spam

Getting too much e-mail is a common consumer complaint. It clogs up electronic mailboxes with communications that are generally not of interest to consumers. Disposing of the mail wastes consumer time and makes it more difficult to spot the mail that consumers want to read. Spam, the name for unwanted e-mail, is defined as unsolicited (usually) commercial e-mail sent to a large number of addresses (Spam 2014). Electronic spamming usually is thought to occur through e-mail, but it occurs through other media. These include instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions spam, and social networking spam.

The origins of the term *spam* come from a 1970 Monte Python skit where the only food on the menu is different combinations of spam. As the waitress recites the menu to a prospective customer, Viking customers are singing a chorus of Spam, Spam, Spam . . . wonderful spam! They are making fun of the propensity for England to serve this canned meat product after World War II. This cheap and plentiful product was applied to unsolicited; e-mails thus the name stuck (Spam (Monty Python) 2014).

Because there are virtually no operating costs and the difficulty of tracking senders, spamming continues today. E-mail spam has been estimated to cost American firms and consumers $20 billion. These numbers would be much higher if it were not for the wide spread use of spam filters.

With the spam filters, it is estimated that only 1.2 percent to 1.8 percent of spam gets through to mail boxes. Furthermore, it has been estimated that the benefits to spammers (gross revenues from sales) is $200 million per year. Thus, the ratio of costs to society versus the benefits to spammers is 100:1 (Rao and Reiley 2012, 87–110). It is this imbalance that makes it a considerable consumer harm.

The direct costs of spam include the consumption of computer and network resources. The harm to businesses and consumer is also the time and attention of dismissing unwanted messages. Spam by its nature demands attention but does not offer a choice in the way one has to deal with it. However, when consumers respond to spam they can fall prey to messages with criminal intent. Consumers by answering spam also fall prey to phishing schemes and identity theft. The other harms to consumers include the spreading of computer viruses and other malicious software.

Covert Marketing

Marketers have long used surreptitious methods of information collection and subtly communicating to consumers. The term covert marketing refers to marketing efforts where the consumer (the recipient) does not link the marketing effort to a particular marketer. It can be a form of deceptive advertising, such as including product placements in various media outlets. It now is being used in the online context (Kaikati and Kaikati 2004).

Online covert marketing takes place both for information gathering and for marketing communications and promotions. Both are intertwined. Information collection helps marketers with their targeting and message formation. Covert information collection includes cookie collection as part of a behavioral advertising program (Miyazaki 2008). In addition, blogs and chat rooms have been used by marketers to surreptitiously collect information. In some cases, marketers hire individuals to infiltrate chat rooms to solicit and monitor consumer feedback, while not informing others they are associated with the sponsoring company.

Consumers can be harmed from covert communications in that their guard may be down if they are not aware a commercial message is being offered. Consumers are harmed from covert data collection because neither they do not have an option to protect sensitive information from being transferred nor a say in how it used or to whom it may be transferred. Empirical research suggests that when consumers find out about the covert activities of marketers, they are more concerned about the information gathering aspects rather than the promotion activities. Moreover, consumers tend to be more forgiving of covert activities if they had a positive relationship with the company prior to learning about their covert activities (Milne, Bahl, and Rohm 2009).

Stalking

Stalking from social media can be a great harm. The nature of social media makes it relatively easy for a stalker to gather and use information against a victim. Partly because the Internet offers a false sense of anonymity, because there is no physical interaction there is a perception of security, and in an environment where friends of friends exist, content that was tailored for a close group of friends often gets transmitted to a much wider audience than intended.

Stalkers can use profile information to learn a lot about a person's interests, habits, friends, routines, and whereabouts. With this background information, stalkers can also have a better guess at consumer passwords, especially if one uses pet names or birthdates. Taken together, this information can be used for mild forms of over contact to potentially deadly encounters.

The five types of stalkers include:

- Intimacy seekers,
- Incompetent suitors,
- Rejected stalkers,
- Resentful stalkers, and
- Predatory stalkers.

About 60 percent of stalkers are from ex-partners. Research has shown that stalking or checking out an ex's profile is linked to more distress about the break-up, more sexual desire for the ex-partner, and lower personal growth (Marshall 2012).

A new trend in stalking is when information is misappropriated. One such case is that of a young woman who learned that she had had someone stalking her for over five years. The individual who was stalking her was stealing pictures from her Facebook and other social media and using them to catfish. She also learned that this same person had previously sent her lewd texts. Although she confronted this person and took her concern to the police, there was nothing that could be done because she had given the stalker permission to access her photos on Facebook (Shookman 2013). In another case, a Virginia woman was harassed by an ex-boyfriend who had assumed the women's identify and announced to crowd that she wanted to have sex with men. Soon men started showing up at the real woman's door. This is a case where social media is being used as a weapon to harass another (Jouvenal 2013).

Geofencing

Consumers can face harm when their geographical location is known to marketers. Since cell phones transmit locational information, this becomes data that marketers want to use to their advantage. To track consumers some marketers use geofencing, which is a location-based software program that uses radio frequency identification to define geographical boundaries. This virtual barrier enables the marketer to take an action once a consumer's phone enters or leaves a pre-specified geographical area. Geofencing programs enable the delivery of advertising or coupons to an individual once they enter a geographical region. For example, a person who opted in to a loyalty program at the local coffee shop could be the recipient of a coupon for a cappuccino when in the neighborhood. Or, a to-do-list app could notify a consumer to pick up eggs at a store or when a favorite clothing store was having a sale if they were in the vicinity. The advantages are that apps can run automatically based on geographical context and not have to be dependent on consumer input.

The harms from this technology lie in others' access and use to the information. A survey of 587 respondents by researchers in Carnegie Mellon revealed the top 10 concerns (Tsai, Kelley, Cranor, and Sadeh 2010).

1. Revealing the location of your home to people you do not want to give your address to,
2. Being stalked,
3. Having people intrude on your private space,
4. Being found by someone you don't want to see,
5. Being found when you want to be alone,
6. Having the government track you,
7. Being bothered by ads that use your location,
8. Having your boss spy on you,
9. Revealing activities you are participating in, and
10. Being judged based on your location.

As technology advances and becomes more networked, individual users have less control of their personal devices and others in the network will gain more control and cause potential harm. One example of this is a patent that Apple was granted in August 2012. The patent, U.S. Patent No. 8,254,902, is otherwise known as "Apparatus and methods for enforcement of policies upon a wireless device." This patent allows the functionality of the phone to change based upon the occurrence of a certain sensitive event. Thus, if a phone is within a range of a sensitive event, it may be forced to be put in sleep mode and thus lose all functionality. While it may be useful for turning off cell phones in movie theaters and in classroom, it may also be used to limit the civil liberties of protesters or those seeing the police make a brutal arrest (Whittaker 2012).

Facial Recognition

Back when the movie the Minority Report showed facial recognition being used by stores, it was thought to be science fiction. Now, facial recognition technology is available. Government, marketers, and now individuals can have software on their mobile devices that can be used to recognize faces in a crowd. The CDT in their report on face recognition's impact on privacy (Geiger 2011) recognizes three levels of risk:

1. Individual counting,
2. Individual targeting, and
3. Individual identification.

Individual counting is when individual data are gathered on an aggregate basis and not used for individual communications. For example, software could record passer-byers demographics as part of a marketing research study. *Individual targeting* is when consumer facial information is captured on an aggregate basis and used to tailor advertisements to individals. An example would be the data from passer byers could be used to tailor individual ads. *Individual identification* is when consumer facial information is collected on an individual and aggregate basis and is used to tailor advertisements to the individual. The facial information is linked to the individual's identity and location. One possibility is that biometric data could be used to identify individuals online first and then offline (Singer 2014).

The biggest privacy issue here is the occurrence of an individual being identified based on facial features alone. What this means is the loss of anonymity in public. Where most people can still blend into the crowd and not be recognized without third parties being able to link their face with a name, this is not the case when facial recognition software is being used.

The power of facial recognition was shown by Professor Acquisti who conducted a facial recognition experiment on the Carnegie Mellon campus. As part of this experiment he would stop students, take a picture of the person, and then asked them to fill out a questionnaire on a laptop. While student was doing this, he would upload the picture to a facial recognition software program where it matched the photo with a database of identified photos scrapped from campus Facebook accounts. Before the student finished the survey, the survey was dynamically updated with 10 photos that had the closest match to the student's photo. The student was asked to identify him or herself in the pictures. One in three subjects was identified through this method. Acqusiti's proof of concept experiment suggests that when photos can be linked to a name, and coupled then with other research that shows name and secondary information that can be linked to a social security number, an anonymous face could identity a person's personal identifying information.

Chapter Summary

This chapter examined consumer harms that occur from information exchanges. It began by reporting a study that measured consumer perceived sensitivity and risks associated with different types of information. Next the discussion focused on harms that are present in different stages and process of information exchanges. The last section examined specific risks occurring from new information technology.

The next chapter addresses forms of protection available to consumers and can help guide businesses in facilitating fair and trustworthy information exchanges.

CHAPTER 6

Forms of Protection

Chapter Overview

The focus and mechanisms of privacy protection are historically and culturally based. In the United States, the focus has been to regulate information use by government, while permitting information use by private companies unless it specifically harmed consumers as dictated by sector-based law. Much of the privacy control of businesses is reliant upon self-regulation, with the oversight of the Federal Trade Commission (FTC). Increasingly, consumers have been educated and encouraged to take protection matters in their own hands through formation of more safeguarded norms and by employing technological solutions to create privacy. In other parts of the world, such as Europe, the development of privacy protection was impacted by shared cultural experience. Shaped by World War II, the Holocaust, and Soviet control of the Eastern Block, privacy protection emerged into something that is much stricter than in the United States, where no one collects or uses personal information unless they have prior permission to do so. The approaches in other parts of the world vary by their specific historical and cultural experiences.

In this chapter you will learn about the forms of privacy protection in the United States (and the European Union) that can protect consumers and regulate and guide businesses in the handling of personal information. In particular, the focus of this chapter is to present a review of Privacy Protection mechanisms. There are two sections:

- The first section examines externally focused legal and suggested self-regulatory approaches.
- The second section looks at specific actions that businesses and consumers can take to protect consumer information privacy.

The first section begins by examining both legal and the FTC proposed self-regulatory mechanisms to control U.S. business behavior. In the review of privacy legislation in the United States, the focus is on national level laws, highlighting a few that have had a big impact on marketers. Similarly for the self-regulatory efforts, there is a discussion of Fair Information Practices and Privacy by Design principles that have been articulated by the FTC. As part of this section, there is a review of certain key actions taken by the FTC against companies that violated privacy laws. The section concludes by contrasting the U.S. system with that of the European Union.

In the second section there is a review of business actions to promote privacy that have not been externally dictated. This includes suggested privacy practices and technological solutions. Following this, there is a discussion of what consumers can do to promote their privacy in the market place. These include following many of the educational programs put forth by privacy advocates and the FTC.

Externally Focused Legal and Suggested Self-regulatory Approaches

U.S. Privacy Legislation

The roots of privacy thought were shaped in the 1890 Harvard Law publication, *The Right to Privacy*, written by Louis Brandeis and Samuel Warren. Since this initial public discussion, federal and state legislation has been relatively scarce until the 1960s. As technological advances occurred, however, there was an increase of privacy legislation as shown in Table 6.1.

In the next section, six of the major privacy legal acts and laws from this list are discussed:

1. Fair Credit Reporting Act (FCRA)
2. Communication Laws
3. Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)
4. Children's Online Privacy Protection Act (COPPA)
5. Gramm Leach Bliley Act and Privacy Notices (GLB)
6. Health Insurance Portability and Accountability Act (HIPAA)

Table 6.1 US privacy legislation

US Law	Description
Freedom of Information Act (1966)	Permits third part access to federal records. Access to personal information held by Federal Agencies.
Fair Credit Reporting Act (1970)	Promotes accuracy, fairness, and privacy of credit files. Regulates credit bureaus that gather and sell consumer information.
Federal Privacy Act (1974)	Requires Federal Agencies to apply fair information practices while handing records with personal information.
Electronic Communications Privacy Act (1986), amended 1986	Prohibits tampering with stored communications on computers. Amends federal wiretap law to cover e-mails, cell, and other electronic communications.
Computer Matching and Privacy Act (1988)	Amends privacy act and provides guidelines to follow when matching information held on government databases.
Telephone Consumer Protection Act (1992) [TCPA]	Requires telephone solicitors to provide consumers option to not receive future contact.
Federal Identity Theft Assumption and Deterrence Act (1998)	Makes it a national crime to steal someone else's identity.
Driver's Privacy Protection Act (1994), effective 1997	DMV's are prohibited from releasing personal information from driver licenses records.
Financial Services Modernization Act (1999) [Gramm-Leach-Bliley Act]	Financial institutions required to provide consumers a privacy notices and chance to opt out.
Children's Online Privacy Protection Act (2000) [COPPA]	Makes it illegal to contact children 12 and under online without parental permission.
Health Insurance Portability and Accountability Act (1996), effective 2001	Health professionals required to protect the privacy of health records.
Do Not Call Registry Act (2003)	The Federal Trade Commission operates a do not call registry.
Fair and Accurate Credit Transactions Act (2003) [FACTA]	Consumers provided with new tools to review credit records and protect against identity theft.
CAN-SPAM Act (2003), amended 2004	Creates standards for those using commercial e-mail to stop spam.
Identity Theft Penalty Enhancement Act (2004)	A law that sets rules and penalties for identity theft.

The Fair Credit Reporting Act

FCRA was enacted in 1970 to make sure companies properly collected, maintained, and used personal information pertaining to credit worthiness, standing, capacity, character, reputation, and mode of living. The law regulates those who create consumer reports and those who use them. It has provisions to maintain accuracy of the reports by giving consumers the rights to review the information in the reports. It also limits report use to a set of permissible purposes, such as a credit application.

FCRA regulates consumer reporting agencies (CRA), creditors, and information users. CRA collect and disseminate consumer information. The big three CRAs are:

1. Experian,
2. TransUnion, and
3. Equifax.

There are also many other national specialty CRA that gather and disseminate information pertaining to medical records and payments, tenant history, employment history, check writing history, and insurance claims. Creditors, such as credit card companies, mortgage and auto financing entities, are companies that furnish information to the CRAs. Users of information can be credit, insurance, and employment background checks.

Communication Laws

The communication-based laws and regulations are a good example of law being enacted to keep up with technology. Three of these notable laws are:

- Telephone Consumer Protection Act (TCPA),
- Do Not Call Legislation, and
- Telemarketer Sales Rules.

In the late 1980s, unsolicited faxes were a problem. Thus, the TCPA was implemented, which provides provisions for consumer to file lawsuits and collect damages for receiving unsolicited phone, fax, and auto dialed prerecorded calls. The flood of calls continued, however, and consumers felt it was tough to stop them. Thus the Do Not Call registry, which helps enforce TCPA, was formulated in 2003 and implemented in 2004. The registry made it possible for consumers to register their phone number and greatly limit the number of telemarketing calls. Some exceptions were that consumers could still receive calls from not-for-profit organizations, companies conducting surveys, and from companies where they had an existing business relationship within the last 18 months.

The Telemarketer Sales Rules (TSR), first enacted in 1995, was updated in 2003 by FTC to help implement the Do Not Call legislation. The purpose of TSRs is to regulate for-profit organizations and for-profit telefunders who are seeking charity donations. The rules require covered organizations to follow rules such as call only between 8 a.m. and 9 p.m.; screen names against the do not all lists, display caller ID information; identify themselves and what they are selling and disclose all material information and terms.

A 2013 rule change to the TCPA requires written permission from consumers for a marketer to use an automated phone dialing system or to leave prerecorded voice message. The new rule cannot rely on do not call lists. Each violation has a fine ranging from $500 to $1500. Because of robot calling technologies, there is risk that TCPA settlements could be quite large (The U.S. Chamber Institute for Legal Reform 2013).

CAN-SPAM ACT

The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM) covered entities in the United States sending e-mail messages. The CAN-SPAM act, in an effort to reduce unsolicited e-mail, regulates marketers in the following ways:

- Requires a functioning return e-mail address,
- Prohibits false headers and deceptive subject lines,
- Prohibits follow-up mail within 10 days of when an individual indicates they do not want to receive future mail,

- Requires clearly labeling whether the mail is an advertisement unless prior consent was given, and
- And requires sexually oriented material to have a warning label.

The CAN-SPAM act is enforced by FTC and has fines up to $11,000 per violation. Interestingly, in 2008, Facebook was awarded a $837 million judgment against a spammer who sent over 4 million e-mails to Facebook site users containing offers for marijuana, male enhancement, and assorted sexual propositions (Facebook spammer slapped 2008).

Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA) was put in place to protect children under 13 that are online. It requires website operators to provide detailed privacy notices that state what type of information is being collected from children, how it is used, and whether it is disclosed to third parties. It requires the website operator to get verifiable consent from the parent prior to collecting information from children. It gives parents the opportunity to review information collected on their children. It prohibits website operators from requiring personal information disclosure as part of games and contests and requires the website to secure the information once obtained. The rule was updated in 2013 to provide more precision on the definitions. The new provision creates additional parental and notice requirements. COPPA's coverage has also been extended to include ad networks and plug-ins that interact with websites targeted to children. Over the years, the FTC has been very actively enforcing COPPA. One of the most notable enforcement was when the FTC fined Zanga $1 million for violating kids' privacy (Xanga.com to Pay 2006).

Gramm Leach Bliley Act and Privacy Notices

The Gramm Leach Bliley Act (GLBA) known as the Financial Services Modernization Act was a broad sweeping legislation allowing for financial holding companies to offer a wide range of services and financial products. The GLBA also required financial institutions to safeguard consumer privacy. Specifically, financial institutions are required to:

- protect the security of stored consumer information,
- provide annual notices of the gathering, sharing, and use of consumer information, and
- permit consumer opt-out choices regarding the sharing of consumer information to third parties.

After its implementation, there was concern over whether the privacy notices were understandable by consumers. A big concern was whether the notices were written in language at the proper grade level and without excessive legalese.

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) was implemented to improve the efficiency of health services. The creators of the act realized that with the trend toward electronic exchange of records, there were possible privacy issue that were raised. HIPAA applies to health care providers (hospitals), health plans, and health care clearing houses (third parties). The privacy rule within HIPAA regulates when privacy notices need to be presented to patients and what type of information requires consumer consent and what does not. For example, personal health information does not require consumer approval if it is used for treatment. However, if personal health information is used for other purposes, then it would require an opt-in authorization.

The second largest HIPAA violation to date was in 2013 when over four million records were stolen from four laptops and the responsible party, Advocate Medical Group, took over a month to inform the affected patients (Ouellette 2013).

The FTC and U.S. Regulatory Enforcement

While limited legislation to protect consumers exists, the majority of privacy protection is self-regulation. To this end, the fair information practices guide this behavior. The FTC regulates to see that businesses live up to their promises.

Fair Information Practices

In 1973, the U.S. Department of Health, Education, and Welfare Advisory Committee on Automated Data Systems developed the code of fair information principles. The code included:

- Openness—record keeping systems and databanks must be publically known,
- Individual participation—individuals have right to review, correct, and remove information,
- Collection limitation—there should be limits to what information is collected,
- Data quality—data must be accurate and collected for a relevant purpose,
- Finality—there should be limits to the use and disclosure of information,
- Security—data should be protected against loss, destruction, and unauthorized access, and
- Accountability—record keepers should be accountable for the fair information principles.

There was increased regulatory attention in the 2000s as to whether businesses were following fair information practices and whether consumers were given ample opportunity to control their personal information. The FTC, responsible for handling violations of the Federal Privacy Act of 1974, has relied upon four fair information practices, which have been modified over time.

- *Notice/Awareness*—This principle states consumers should be made aware of an organization's information practices through notices. Such notices should identify the data being collected, how used—especially if transferred to third parties, and the steps taken to protect the data. The notice historically has been considered the most important Fair Information Practice (FIP) by the FTC. Issues exist how notices will transfer to new mobile devices.

- *Choice/consent*—Consumer want to control how their information will be used and have the choice whether they choose to participate or not. Consumer choice also extends not only to data collection but whether the data are transferred to third parties. While historically opt-out was used by the direct marketing industry, there has been a shift in norms for opt-in being used online. In addition, Internet marketers, such as Google, have been creating preference centers that provide consumers choice in the type of data that is used and the type of communications they want to receive.
- *Access*—Consumers have the right to view their personal information and make any corrections necessary if there are inaccuracies. Access is to be provided in a convenient, timely, and relatively inexpensive manner to consumers.
- *Integrity/security*—Data that are collected should be protected by unauthorized access. This means companies must use appropriate collection and storage procedures that protect the data from hackers and other unwanted viewer. Security of data remains a top concern as marketers have continued to be hack and consumers have their personal information stolen.

Privacy by Design

In 2012, the FTC introduced the concept of Privacy by Design in their report "Protecting Consumer Privacy in an Era of Rapid Change" (Federal Trade Commission 2012). The baseline principle for privacy by design stated that companies should promote consumer privacy throughout their organizations and at every state of the development of their products and services. Substantively this means that companies need to incorporate privacy into all their practices. This includes data security, reasonable collection limits, sound retention and disposal practices, and data accuracy. In terms of procedural practices, companies are to maintain comprehensive data management procedures throughout the life cycle of their products and services. With privacy by design, privacy is thought of at the beginning and all stages of a business or services development and execution. This is in contrast to treating it as an afterthought or something to tack on after the product and service has been in the market place.

The motivation for privacy by design was to augment the fair information practices that many companies were practicing. Thus, the overall privacy framework included privacy by design and two FIPs:

The overall Privacy Framework proposed by the FTC was:

- Privacy by design,
- Simplified choice for businesses and consumers, and
- Greater transparency.

While self-regulation has been in place for some time, there was criticism that the pace of change was not fast enough. Thus, the FTC stated it was going to work with Congress and other stakeholders to form legislation. Simultaneously, the FTC was strongly encouraging industry to adopt self-regulation principles. At this time, there continues to be much industry support for self-regulation and FIP. However, with the challenges of big data, less attention will be given to the collection of data and more on the use.

Enforcement

The FTC enforcement efforts have centered on whether companies keep the privacy promises they make. Often these promises are stated in privacy policies or communications. For example, a case brought against Epic Marketplace, Inc. in 2012 focused on a violation of the FIP of notice/awareness. Epic marketplace is an online advertising company that used history sniffing to secretly and illegally gather information (FTC Settlement 2012). Its privacy policy said it would only collect information from consumer visits to its network. Similarly, a case was brought against Myspace in 2012 because its privacy policy stated that it would not share personally identifying information without giving notice and getting permission to do so. The FTC charged them of breaking their promises (Myspace settles FTC 2012). Similarly, Google was charged with deceptive tactics that were in violation of their privacy policies in their launch of Google Buzz. In this situation, consumers were enrolled in the program when they thought they were opting out. In this case, the FTC proposed that privacy audits be conducted for the next 20 years (FTC charges deceptive 2011).

An interesting case of deceptive communication was brought against the company Lifelock that sold a service of protecting consumer information for a $10/month fee. Lifelock also offered a $1 million guarantee to compensate customer for losses they might have become a victims of identity theft while using Lifelock services. The CEO Todd Davis was so confident that he publicized his Social Security Number (457-55-5462) in magazines and TV. After he did so, his identity was stolen 13 times. These bogus claims by Lifelock resulted in a $12 million fine from the FTC for deceptive advertising. Davis' history as an identity theft victim made Lifelock's claims less credible (Nearly one million lifelock 2010).

The other FIP that companies are failing on is integrity and security. There continue to be many cases where companies did not provide adequate security to protect consumer information. A case in 2008 against TJX charged the company with compromising consumer data due to poor security. Consumer data was stolen by hackers who sat in parking lots of stores with unsecured wireless networks and weak encryption practices. Around the same time, CVS was charged with improper disposal of pill bottles and medical records—they were discarded unshredded into company dumpsters. The type of information that was placed unsecured into open dumpsters included "pill bottles with patient names, addresses, prescribing physicians' names, medication and dosages; medication instruction sheets with personal information; computer order information from the pharmacies, including consumers' personal information; employment applications, including social security numbers; payroll information; and credit card and insurance card information, including, in some cases, account numbers and driver's license numbers" (CVS caremark settles 2009). In 2014, the FTC filed a case against GMR Transcription Services, a company that provides medical transcription services, for exposing thousands of consumer records on the open Internet (Provider of medical transcript 2014).

Interestingly, even companies that guarantee the security of websites to consumers have had cases brought against them by the FTC. ControlScan, a company that assures consumers and visitors that a website is secure, was guilty of offering bogus seals of approval. Their seal of approval offered a date stamp, suggesting the site security was being checked daily, which it was not. In reality, their websites were only being reviewed weekly (Online privacy and security 2010).

Overall, the FTC has continued to enforce privacy violations in the marketplace and is increasing the number of cases brought against companies (Enforcing privacy promises n.d.). In the next section, there is a discussion of the European Union's privacy protection perspective, which differs from the U.S. self-regulatory approach.

EU Directive and Global Perspective

In Europe the protection of privacy is considered a fundamental right. The primary focus is not to allow the collection or use of any personal information unless permitted by the law. The right to privacy is articulated in Article 8 of the *European Convention on Human Rights* (ECHR) (2014). It provides a right to respect for one's *private and family life, his home and his correspondence*, subject to certain restrictions. The European Directive is part of the European data protection framework. It incorporates several FIPs. Thus, data must be:

1. Fairly and lawfully processed,
2. Processed for limited purposes,
3. Adequate, relevant, and not excessive,
4. Accurate,
5. Kept no longer than necessary,
6. Processed in accordance with the data subject's rights,
7. Secure, and
8. Transferred only to countries with adequate protection.

It is important for U.S. companies to note that data from the European Union cannot be transferred to a non-EU country unless adequate data protections are guaranteed. This is usually accomplished through safe harbor provisions where the U.S. firms agree to the above terms. In addition, the EU model is very stringent about choice. An opt-in mechanism is required for the processing and use of sensitive data. Thus, all direct marketing activities require opt-in permission to use consumer data.

Businesses and Consumers Actions to Protect Consumer Information Privacy

Steps Business Can Take to Protect Privacy

In reaction to the complexity of the data environment, many companies have created a position of a chief privacy officer. This senior level executive is responsible for managing the risks and business implications of privacy laws and industry policies. In the United States, the privacy officer was first created in 1999. It was notable when IBM hired a Chief Privacy Officer in 2000, signifying the importance of such an administrative position. In 2002, the International Association of Privacy Professionals (IAPP) was formed from the merger of the Privacy Officers Association and the Association of Corporate Privacy officers (Chief privacy officer 2014). The IAPP has since offered certifications such as the Certified Information Privacy Professional (CIPP), which is one of the leading global certifications. The certification prepares the individual to help companies with data protection, information auditing, information security, legal compliance, and risk management (About the IAPP n.d.).

Building trust through the promotion of signals is essential for businesses to earn the confidence of consumers. One signal that is effective is the posting of a Certified Privacy Seal on a website or an app. Companies like Truste offer services to see that companies are with the requirements established by Truste. Given the multichannel nature of information privacy, Truste assesses and certifies websites, clouds, apps, data, downloads, and smartgrids (About TRUSTe n.d.).

Companies can take many steps to protect consumer information. Truste, which certifies websites are in compliance with best privacy policies, suggests the following (Protecting Customer Information n.d.):

1. Review your privacy statement to make sure it's easy to read and understand.
2. Make sure your privacy statement aligns with your terms-of-service statement.

3. When establishing your company's privacy program, build internal documents with an eye to your public privacy statement.
4. Review your privacy policy regularly to make sure it accurately reflects your current data collection and handling practices.
5. When writing or revising your privacy statement, use may or might statements sparingly.
6. Add ad effective date to your privacy statements.
7. Make sure EU certifications are seamless.
8. Comply with privacy laws such as COPPA.
9. Treat testimonial PII respectfully.
10. Notify customers if you are about to transfer their personally identifiable information elsewhere.
11. Determine whether changes you make to your website require you to notify all site users.
12. Consider synching up your privacy and security teams.
13. Use SSL (Secure Sockets Layer) encryption when it's important.
14. Prepare for a case of data breach.
15. Minimize data collection on your website.
16. When you collect data on your site, take extra steps to inform users how their information will be used.
17. Retain customer data for the shortest time possible.
18. If your organization shares personal information with third parties for marketing purposes, comply with all laws (i.e., California's Shine the Light Law).
19. If you use user-profiling technologies like cookies, log files, web beacons notify users about it in your privacy statement.

Many of these recommendations are being adapted by privacy officers in companies.

Deidre Rodriquez (CIPP/US), while Director of the Corporate Privacy Office and Regulatory Oversight for Wellpoint, Inc., suggested 10 basic steps for creating a Quality Privacy Program. While developed for healthcare, they have applicability elsewhere (Rodriguez 2013).

1. Understand the compliance requirements that affect the organization and create a set of policies and procedure to comply with these.

It is important to create a document that articulates compliance requirements and matches these up with the procedure are to meet these requirements.

2. Look at privacy from all angles and see how it relates to the organization as a whole. This involves conducting a comprehensive risk analysis.
3. Implements the privacy by design principles suggested by the FTC. Thus, when creating tools it is important that they address all the privacy issues facing the organization and industry.
4. Translate the privacy by design statements into privacy impact assessments. Appropriate controls and plans for improving should be put in place.
5. Anticipate which type of data is likely to be audited and have systems to get the requested data quickly.
6. Make sure to test the process of responding to privacy inquiries. This will require testing by different user groups.
7. Identify the root cause of any actions requiring sanctions.
8. Learn from the mistakes of others in the industry.
9. Have a written plan to deal with known issues.
10. Monitor and track your process of protecting privacy with data.

The previous points that suggest what it takes to build a quality privacy program highlight the complexity for businesses in protecting consumer privacy. While privacy officers may lead the charge, responsible information management is ultimately the responsibility of every individual in an organization.

Advice for Consumer Actions to Protect their Privacy

In the self-regulatory environment of the United States, consumers are ultimately responsible for their own privacy. Indeed, much of the discourse on privacy protection centers consumer education. A recent study by the Pew Internet & American Life Project found that 86 percent of internet users took steps to protect their privacy. These activities ranged from clearing cookies to encrypting their mail. Fifty-five percent have taken action to avoid being observed by specific people (Rainie et al. 2013).

Consumers do not have to look far for educational material. Sources of educational material come from the government, privacy advocacy organizations, and news-based websites.

The FTC, for example, has education material on:

- Limiting unwanted calls and e-mails,
- Computer security,
- Kids' online safety,
- Protecting your identity, and
- Repairing identity theft.

As an example of the steps that consumers can take to protect themselves against identity theft, the FTC recommends the following (Federal Trade Commission n.d.; National Science Foundation n.d.):

1. Use passwords on all your card, bank, and phone accounts,
2. Don't keep passwords or PINs with wallet,
3. Never give information without knowing the other party,
4. Read credit card statements carefully and often,
5. Know your payment due dates,
6. Read your health insurance plan statements,
7. Shred documents with personal information, and
8. Review your credit reports at least once a year.

Other organizations such as StaySafeOnline.org offer general tips on how to stay safe online and across social networks. Indeed, there are many groups and organizations whose mission is to inform the public about the risks of online and offer protective actions. Table 6.2 provides a list of some privacy advocacy groups that offer privacy advice and education.

It is interesting to recognize that these organizations have been educating consumers for some time but many of the points of advice remain the same. However, as the technologies become more advanced, new advice is added in. Back in 2002, the Electronic Frontier published a list of 12 tips of protection that are still relevant today (EFF's top 12 ways to protect your online privacy 2002).

Table 6.2 List of privacy advocacy groups

Electronic Privacy Information Center (EPIC)	http://epic.org/	A public interest research center that focuses public attention on emerging privacy issues.
American Civil Liberties Union (ACLU)	https://www.aclu.org/	Defends and preserves the right to privacy (among others).
Consumers Against Supermarket Privacy Invasion and Numbering (Caspian)	www.nocards.org	A grass roots consumer group dedicated to fighting supermarket loyalty or frequent shopper cards.
Coalition Against Unsolicited Commercial Email (CAUCE)	http://www.cauce.org/	Organization originally advocating for antispam laws. Now it also defends privacy rights
Center for Digital Democracy	http://www.democraticmedia.org/	Consumer protection and privacy organization.
Computer Professionals for Social Responsibility	http://cpsr.org/	Alliance of computer scientists and others concerned about the impact of computer technology on society.
Electronic Frontier Foundation	https://www.eff.org/	Confronts cutting edge issues defending free speech, privacy, innovation, and consumer rights.
Privacy Coalition	http://privacycoalition.org/	A nonpartisan coalition of individuals and organizations that have agreed to a privacy pledge.
Privacy International	https://www.privacyinternational.org/	Privacy International defends the right to privacy across the world and fights surveillance and other intrusions into private life by governments and corporations.
Privacy Rights Clearinghouse	https://www.privacyrights.org/	A nonprofit consumer education and advocacy project whose purpose is to advocate for consumers' privacy rights in public policy proceedings.
US Public Interest Research Group (PIRG)	www.uspirg.org/	*U.S. PIRG* stands up to powerful *interests* whenever they threaten our health, our financial security, or our right to fully participate in our democracy.

Top 12 ways to protect your online privacy
https://www.eff.org/wp/effs-top-12-ways-protect-your-online-privacy
Note: list from 2002

1. Do not reveal personal information inadvertently.
2. Turn on cookie notices in your Web browser and/or use cookie management software or infomediaries.
3. Keep a clean e-mail address.
4. Don't reveal personal details to strangers or just-met "friends".
5. Realize you may be monitored at work, avoid sending highly personal e-mail to mailing lists, and keep sensitive files on your home computer.
6. Beware of sites that offer some sort of reward or prize in exchange for your contact information or other personal details.
7. Do not reply to spammers, for any reason.
8. Be conscious of web security.
9. Be conscious of home computer security.
10. Examine privacy policies and seals.
11. Remember that *you* decide what information about yourself to reveal, when, why, and to whom.
12. Use encryption!

An updated online protection list was updated in 2010 by Michael Fertik, founder of Reputation Defender. (The mission of Reputation Defender is to help improve individuals and businesses reputations. They do this by suppressing search results, help protect personal data, and manage reputations through the review process (Fertik 2010).)

1. Block cookies on your Web browser,
2. Don't put your full birth date on your social-networking profiles,
3. Don't download Facebook apps from outside the United States,
4. Use multiple user names and passwords,
5. Know how much private data are out there about you,
6. Be really cautious about geolocation services,
7. Shred,
8. Opt out of "people search" sites,

9. Max out your privacy settings on social networks, and
10. Close old accounts.

Recent updated advice has come from PC World that recommends consumers use technological solutions for ensuring privacy (Paul 2013).

1. Secure the line with a Virtual Protected Network (VPN) when connected to an e-mail, bank, or other sensitive account over public WiFi.
2. Stop leaving private data in the cloud. Use encrypted cloud storage devices such as Truecrypt.
3. Secure your online services with two-factor authentication. Two-factor authentication requires you to enter a short numeric code in addition to your password before you can gain access to your account.

Indeed, the Internet is replete with advice to consumers on how to protect their privacy. Many organizations offer safety checklists. Some sites provide specific advice on how to travel safe or how to prevent cybercrime, the age graded advice on how to stay safe online.

In the future, technological solutions will be used more frequently to protect consumer privacy. This will be driven by the improved usability of the solutions and the increased technical competence and awareness of consumers. In the next section, privacy technology tools that can help consumers keep their information private are discussed.

Technologies (EPIC Online Guide to Practical Privacy Tools n.d.)

Privacy protection through the use of technology has been available for many years, but its use by the public at large is not yet widespread. There are many software programs that can protect privacy and these are often free open source programs. Some of these programs are discussed next.

Internet Anonymizers, VPNs, and Proxy Servers

It is possible for a user to surf the web and visit websites without anyone being able to gather information about the sites the user visited.

Anonymizer services do this by disabling pop-up windows and cookies. They also conceal the user's IP address. Typically proxy services are used to provide information for HTTP requests from the website visited instead of retrieving it from user website. Thus, when a user clicks on a link of a website (or types a URL into a browser), the anonymizer service retrieves and displays the information from its in own server. The visited website then receives information from the anonymizer's server instead of the users. The privacy advantage is that the user information is protected and the user is not identified as having visited a website. The disadvantage of such services is that the user cannot take advantage of any personalization. The programs below are examples of such services:

- Anonymizer (https://www.anonymizer.com), Encrypts, and anonymizes Internet communications.
- Cyberghost VPN (https://cyberghostvpn.com), Hides your IP address and allows you to surf anonymously.
- Proxy.org (https://proxy.org/cgi_proxies.shtml), Lists proxy websites
- Tor (https://www.torproject.org), Free software that protects against network surveillance. Sends communications over a distributed network.
- Orbit (https://guardianproject.info/apps/orbot/), An Adroid based Tor system

Web Browser Ad-Ons (Ortega n.d.)

One approach for protecting privacy is to use browser ad-ons. These are designed to protect users from browser flaws and privacy violations. For example, Ad-on plus stops banners and certain types of advertisements from being downloaded and displayed. The website is customizable to the users' preferences. Another program such as Netcraft toolbar protects the user from phishing attacks by blocking access to suspicious looking URLs. The site maintains a database of such URLs and relies on the community to constantly update.

- Adblock Plus (https://adblockplus.org/en/internet-explorer), Blocks banners, pop-ups and video ads.

- Netcraft Toolbar (http://toolbar.netcraft.com/), Protects against Phishing attacks.
- HTTPs Everywhere (https://www.eff.org/https-everywhere), Forces servers to present HTTPS websites where they are available.
- Disconnect (https://disconnect.me/), Allows you to block the invisible websites that track you.
- Better privacy (https://addons.mozilla.org/en-US/firefox/addon/betterprivacy/), Helps remove or manage flash cookies.

Search Engines (5 Alternative Search Engines n.d.)

The major search engines such as Google, Bing, and Yahoo track your searches and build dossiers about your preferences so they can serve up results based on your history. The serving up of search information based on your history is referred to as a filter bubble, which limits the type of information to which you have access. It is very likely that different people will be shown different information when typing in the same search term. To combat, the search engine DuckDuckGo does not collect information about you nor allows third parties to do so. It does this by discarding user agents and IP addresses from its server logs. Also, it does not impose filter bubbles on a search.

Maintaining privacy and not having filter bubbles on searches is important because it allows individuals the freedom to research and learn about new areas without observation and being judged. The lack of filter bubble allows the searcher to receive new information outside of their original circle of content so that they can grow and learn new things. Also, since saved searches can be requested legally, privacy on such services is important so that the search does not come back to harm an individual.

The following are examples of two privacy based search engines.

- DuckDuckGo (https://duckduckgo.com), Allows one to search anonymously and does not filter bubble anyone.
- Ixquick (https://ixquick.com), Does not record IP address from a search.

E-mail/Communication Encryption

E-mail communication can be protected from unintended viewing through e-mail encryption. The encryption process usually relies upon public-key cryptography, also referred to as public/private key encryption. With such a system, users publish a public key that others can use to encrypt messages sent to them. A private key is used to decrypt the messages sent to them. Two such programs are listed next:

- GPG (http://www.gnupg.org/), Free software for OpenPGP e-mail encryption.
- Mailvelope (http://www.mailvelope.com/), OpenPGP Encryption for Webmail. Integrate directly into the webmail user interface.

Alternative E-mail Accounts (Nosowits 2013)

With the NSA spying, there has been more interest in secure e-mail accounts. Having a secure password no longer protects ones privacy. One question for users is whether the company turns over e-mails to government requests. Interestingly, Swiss accounts advertise being out of range of the NSA. Some examples of alternative e-mails that are secure and not easily accessible by government requests are:

- Guerrillamail (https://www.guerrillamail.com/inbox), Disposable temporary e-mail address. Addresses for inboxes last forever, but e-mail is deleted within one hour.
- Tor Mail (http://tormail.org), A free anonymous e-mail service provider that requires uses to have Tor on their computer.
- Countermail, Secure e-mail provider. Has a USB key option that requires key to be put in USB port to access e-mail.
- Hushmail (www. Hushmail.com), A free service with open PGP encryption housed in Vancouver CA.
- MyKolab (https://mykolab.com/), Swiss company that offers secure e-mail accounts including calendars and address books. Stored in secure Swiss data center. Data will not be crawled.

- Neomailbox (https://www.neomailbox.com/), Secure e-mail with IP anonymity. Has spam and virus protection. Hosted in Switzerland.

Anonymous Remailers

Another way to protect privacy is to use an anonymous remailer. This process relies on a server that receives messages with embedded instructions on where to send the information without revealing where the information came from. Depending on the type of remailer, the receiver of the mail can or cannot respond to the remailer. The anonymity afforded to the sender should be used responsibly. QuickSilver is an example of an Anonymous remailer.

- QuickSilver, The outgoing message is multi-encrypted and sent through a series of remailers. The remailer strips information about where email was from. Privacy is achieved through encrypting and remailing.

Disk/File Encryption

With laptops being stolen and the security of data compromised it is important to secure disks and files. Disk file encryption is a technology that protects privacy by converting information on a disk unreadable unless accessed by a code that can be used to decipher the information. This is useful because it protects against unauthorized access to stored data. One example is TrueCrypt:

- TrueCrypt (http://www.truecrypt.org/), Encrypts files or portions of a storage disk.

Secure Instant Messaging (Bahny 2013)

Instant messages often use the public Internet and thus are subject to potential loss or theft of personal information or loss. For business using these services, privacy of information transferred must be maintained. Five Apps that can be used within a private corporate network include:

1. BigAnt Instant Messenger
2. Bopup Communication server
3. DBabble
4. Openfire
5. Winpopup LAN messengers

For consumers using instant messaging, there are several options of encryption based programs listed below:

- Cryptocat (https://crypto.cat/), Encrypts instant messages. Not even readable by network.
- Off-the-record messaging (https://otr.cypherpunks.ca/), Offers encryption, authentication, and deniability.
- Tor chat (https://github.com/prof7bit/TorChat/wiki), Peer to peer instant messenger. Requires tor.

Disk/File Erasing Programs

When people throw away old hard drives, simply erasing or reformatting the drive is not enough to protect someone from lifting information from the drive. When a file is deleted the operating system does not delete the file but rather only deletes the reference to the file. Thus, it is possible for others who acquire the discarded hard drive to access the information and steal one's identity. Below are a couple of programs that securely erase hard drives.

- Darik's Boot and Nuke (http://www.dban.org/), A free erasure program for consumer to use. It's a self-contained boot disk that deletes hard drive contents. Good for erasing hard disk before recycling.
- Ccleaner (http://www.piriform.com/ccleaner), Cleans internet history, temporary files, makes computer run faster

- Eraser (http://eraser.heidi.ie/), A free utility for securely erasing data from a hard drive. It provides multiple methods to overwrite data. Can be specific to subdirectories.

Password Managers

Individuals are encouraged to use different hard passwords but often do not because of the difficulty remembering and the hassle. Password mangers are software programs that organize password and pins. A password manager program stores the encrypted passwords for secure logins. These can be accessed through master passwords, USB keys, and smart cards. Some programs use auto fill features where the machine will write in the passwords in the required fields. Privacy is protected from phasing and pharming scams and keystroke logging. The vulnerability of writing down passwords is minimized. Two such programs are as follows:

- Password Safe (http://passwordsafe.sourceforge.net/), Creates a secured and encrypted user name/password list. To unlock list you must remember a master password.
- LastPass (https://lastpass.com/how-it-works/), Creates secure passwords and has vault. Features autofill feature

Firewalls (Tyson n.d)

A basic but important protection for businesses and home networks is a firewall. Firewalls protect networks from offensive websites and potential hackers. A firewall is a barrier to keep unwanted sites away from your property. It filters information coming through the Internet and non-desirable information is flagged by a filter, and not let through. Two programs that establish firewalls for consumers are:

- ZoneAlarm (http://www.zonealarm.com/security//en-us/home.htm).
- Comodo (http://personalfirewall.comodo.com/).

Antivirus Software (Antivirus Software 2014)

Computers are always at risk of viruses that come through e-mails and downloaded files. Antivirus software prevents, detects, and removes malicious computer viruses. Two popular programs are:

- Norton Antivirus (http://us.norton.com/antivirus/), Actively protects against viruses, identity theft, and social media scams.
- Ad-Aware (http://www.lavasoft.com/products/), Anti-spyware and antivirus software.

Mobile Privacy

With more and more information exchange happening on a mobile platform, there are also particular apps that are useful for protecting the privacy of mobile based communications.

- SilentCircle, Encrypted voice, video, text, and file communications
- Wickr, Encrypted self-destructing text, picture, audio and video messages
- Redphone/TextSecure, Open source application for encrypted voice and text communications
- K-9 Mail, Open source mail app for android that supports PGP
- iPGMail, App to send and decrypt PGP-encoded messages
- DuckDuckGo Search and Stories, Secure anonymous searches with Tor/Orbot integration

VoIP/Video Messaging

A specific privacy issue within the mobile space is how to protect Internet voice communications from eavesdropping through the use of encrypted programs. Two programs that protect privacy are:

- Jitsi (https://jitsi.org/), Secure and encrypted video and audio calls. Open source program.

- Silent Circle (https://silentcircle.com/), Subscribers transmission are private and encrypted end-to-end over their mobile devices. Services are downloadable from an App.

Temporary Cell Phones

For individuals wanting the highest degree of privacy protection in the mobile environment, there is the Burner cell phone which is disposable. The Burner cell phone can be bought with credit, debit, or bit coin. After packaged and shipped, the company destroys all the transaction records of the purchase in their system.

- Burner Phone (https://www.burnerphone.us/), A 30-day disposable phone. Unlimited talk and text for 30 days. Nationwide coverage, completely anonymous.

Private Social Networking

Keeping information private in social networks is nearly impossible given complex computer settings, data arrangements with third parties, and user agreements where the company owns consumer data. In reaction to Facebook and the issues mentioned, some net users are turning to alternative social networks where individuals own their data and it is not centrally held by the company. Two of these networks are:

- Diaspora (https://joindiaspora.com/), An alternative social network that is based on the principles of privacy, decentralization, and freedom. Members own their data, can house it on the servers of their choice, and you have freedom of not using real identity.
- Buddycloud (http://buddycloud.com/), Open source Code for creating decentralized social networks.

Alternative Currencies

Cash has historically been used as the only non-traceable currency. Now bitcoins are available that are non-traceable and are not regulated by banks. They have advantage of being transferred over the internet quickly with no or low fees.

- Bit Coin (https://bitcoin.org/en/), A digital P2P digital currencies. It is open sourced.

New technologies and programs continue to be developed. For more in-depth information on how to protection your privacy, check out the ultimate privacy guide (Crawford n.d.).

Chapter Summary

This chapter reviewed forms of privacy protection available to consumers:

- Laws,
- Self-regulatory action,
- FTC compliance,
- Educational efforts, and
- Technological solutions.

In the near term, self-regulation and FTC monitoring and educational efforts will continue to be relied upon. With advances in technology and consumers improving technological self-efficacy, there will be more wide spread use of privacy enhancing technologies.

CHAPTER 7

The Future of Privacy

Chapter Overview

The future of privacy is inextricably tied to the progression of information technology. As discussed throughout this book, technology is a double edged sword that creates benefits to both consumers and marketers, yet at the same time puts consumer personal information at risk and the ability of marketers to secure information at risk as well. When new technologies are introduced before consumers are aware or ready for them, the creepy factor becomes very relevant. For marketers, this is something that must be managed.

It is likely the future of privacy will need new approaches to regulate privacy. However, if the past is a predictor of the future, privacy protection will continue to be some combination of self-regulation, legislation, and technological solutions. With new contexts like big data, the weights given to and specifics of these three solutions will need to be adjusted. In this chapter, the focus pertaining to privacy protection will be on self-regulation, specifically on managing the creepy factor that continues to be present with the emergence of new technologies. With this change, norms for both marketers and consumers will need to be adjusted through changes in business practices and education to handle the increased pace of new technological advancement. The self-regulation aspect of norms is emphasized because this is perhaps the only protection element that can keep up with the rapid changes ahead.

In this chapter you will learn about a possible future for privacy based on current trends and trajectories. The future discussed is one of an evolving world of big data, where online technology advances will allow marketers to extend into previously public spaces where anonymity was assumed and also into previously private areas of our cars and homes. The invasions of technology into our life will challenge privacy behaviors of solitude, intimacy, and reserve. It is quite possible that regulation and protection in this new environment will need to change because data from the Internet of Things often contains non-identifiable data that is combined to make personal inferences. Given complexities of the environment, privacy protection is likely to move toward issues of use and away from permission to collect. One approach for garnering change is to use a self-regulation lever and established norms of use that are agreed upon by both marketers and consumers.

The next section will discuss how the rise of new technologies, including the Internet of Things, will affect privacy in public and privacy spaces. The benefits from the technologies and the myriad of privacy challenges they have associated with will be discussed. This is followed by a summary discussion of how these technologies impinge on the privacy strategies of achieving anonymity, solitude, intimacy, and reserve. The last section discusses the theory of creepy and the future of resolving the creepy factor by transforming norms through generational shifts, reformed privacy practices by businesses, and privacy education.

The Technological Future

By most accounts, technological change is accelerating. As an illustration, consider the graphs of the number of times GPS, biometrics, and facial recognition were mentioned concurrently with the term privacy over the past decade in the *New York Times*. All three technologies in Figure 7.1 have started to be discussed in the press in conjunction with privacy starting in the 2000s. These technologies are all similar in that they are used to identify the individual.

The future of information technology has been aptly named the age of context by Scoble and Isreal. Indeed, in their book, these authors outline a future where a connected world brings information to consumers when and where they want it, in some ways before consumers realize they need the information. This drive toward this technological future is composed of five forces (Scoble and Isreal 2013):

1. Mobile devices,
2. Social media,

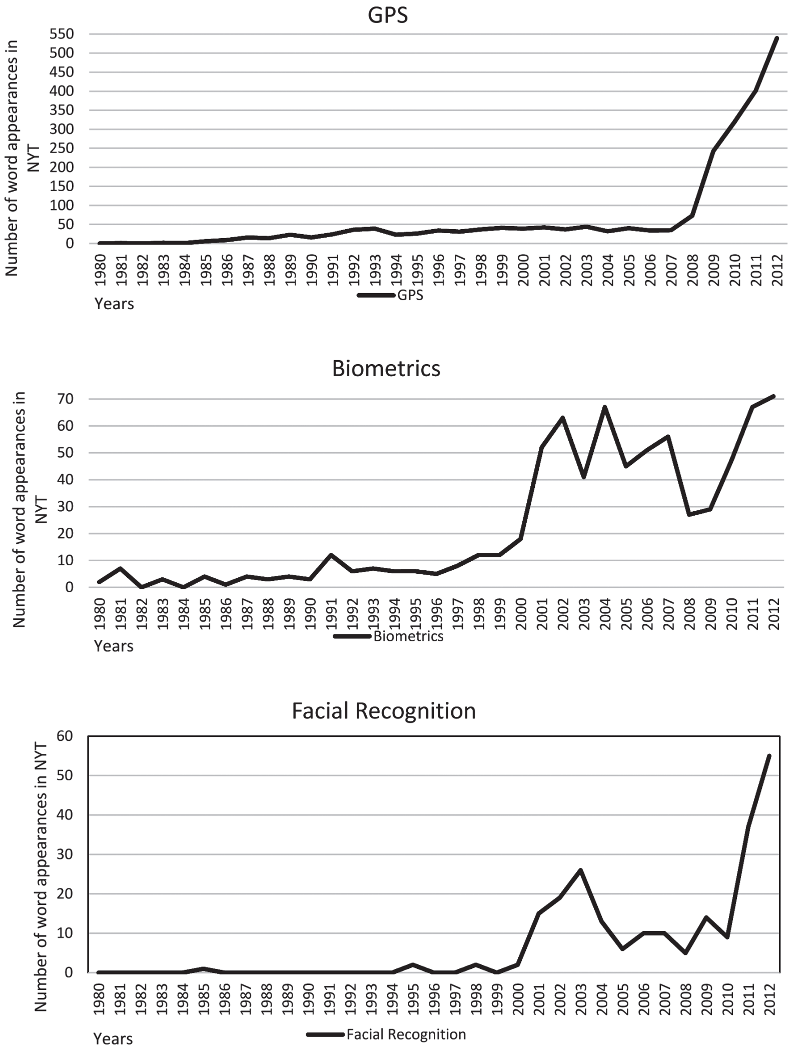

Figure 7.1 Mentions of technologies in the New York Times

3. Big data,
4. Sensors, and
5. Location-based services.

These forces all contribute to the practice of marketers gathering and storing of data in the cloud and giving real time access to consumers on the go.

Google Glass is perhaps the poster child for future technologies. It is a pair of eyeglasses with a mini android computer sitting on the side frame and on the top of one eye socket. It is placed on the glass frame so that one can view a screen prism in the upper right part of the eye socket frame and still have a view through the glasses. The screen can be controlled via voice commands. One can say, OK Glass, "take a picture," "record a video," engage in a Google Hangout, ask Google a question, get directions, or send a message. The advantage of Google Glass is that it is hands free and can provide the consumer with information while they are mobile. The camera app has been reported to be a key feature because it takes pictures much faster than a mobile phone. The other feature that will increasingly become important is the personal assistant feature. Over time, Glass will be acquainted with your personal patterns and will anticipate what you need at the moment or the particular context. Equipped with Google Now, the app will get you information when you need it. The Google Now websites states, "From knowing the weather before you start your day, to planning the best route to avoid traffic, or even checking your favorite team's score while they're playing, Google Now brings you the information you want, when you need it." When you are always wearing your computer with Google Glass, this will become a reality.

Health sensors and monitors are another technology that is starting to be used. According to Rockhealth, a health product seed accelerator, there will be 400 million such products worn by consumers in 2014. The features of health sensors are that they capture information about an individual's health and then store it on a cloud system for further analysis by the user at a later date. This quantification of self is said to help promote better health. Some of the examples of products coming out in the marketing in 2014 include the following (8 New Health-tracking Sensors n.d.):

- *Jawbone Up*, a flexible wrist bank that has vibration and motion sensors to capture the wearer's heart rate, sleep patterns, exercise patterns, and calories burned.
- *Withings*, a WiFi Body scale that automatically sends body metrics to the Internet for personal tracking,
- *Novarti's smart pill system*, which includes microchipped medication tables to track consumer compliance, and

- *AgaMatrix*, a device that tracks carbs and glucose to control diabetes.

This quantification of self, defined as self-knowledge through self-tracking, is said to help promote better health. People have been noted to cure themselves from disease and vastly improve physical performance (Moschel n.d.). The quantification of data permits individuals to spot trends and alter their behaviors to optimize their quality of life.

Perhaps the product that might best represent this self-quantification trend is the Wello. The technology resides in a cell phone case and allows the collection of blood pressure, heart rate, blood oxygen, temperature, and lung function (Ganapati 2014). The thinking is that over time an individual can see patterns of their health and take better care of themselves.

Cars

One of the first Internet of Things applications have been with cars. The toll pass using RFID technologies has made it easier for drivers to go through tolls. It also contributes data that can be used for monitoring drivers. In addition, systems such as Onstar and GPS systems have provided consumers with security and direction for years. Increasingly, cars are coming with technologies that send trip information such as speed traveled and sudden braking to third parties for monitoring. It is expected that more than 60% of new cars will have connected monitoring capabilities by 2017. Included in such devices are electronic data reorders or EDRs. These black boxes snap into action if the air bags deploy. They will record the speed, braking, acceleration, and seatbelt usage (Woodyard and O'Donnel 2013).

In England speeding tickets are mailed to consumers who have been viewed speeding through a series of 1,000 surveillance cameras. Instead of cameras, RFID technology could be used to measure speed between tollbooths (Urken 2011).

Currently, U.S. auto insurance companies such as Progressive and State Farm offer discounts (10 percent to 15 percent) for good driving determined from car sensors. Progressive installs a small digital device that plugs into the car's diagnostic port. The device provides a chirp if the car is driven outside of Progressive's set safe driving parameters (speed, length of time at certain speeds, etc.). At the times when the rates are set, the information is sent to Progressive. State Farm gets permission to install devices that pick up data from onboard GPS devices such as Onstar (Vogel 2012). This is a good example where consumers will trade their privacy for monetary compensation.

GPS Tracking

Just as consumers have been tracked online, new technology solutions are emerging to track consumers offline in retail stores. To do this, cellphones are now being used to track consumers through malls and stores. The MAC number, which is unique to each phone, can be captured by marketers and used to track a person through the WiFi and bluetooth. Retailers claim it is anonymous because the number is not tied to personal identifying numbers. However, such information is useful to marketers to understand traffic issues and backups at the checkout counter (Kerr 2014).While marketers at first thought this technology was benign, consumers think otherwise. Initial tests of this technology at Nordstroms in 2013 resulted in consumer back lash and claims of creepy, prompting Nordstroms to cancel the program (Clifford and Hardy 2013). The FTC has started investigating the use of these technologies, and retail analytic firms have put forward a set of privacy guidelines including notification and the chance to opt-out. Nonetheless, there is a trend toward retailers offering apps to consumers that permit the stores to track their progress through the stores. Some companies are matching videos of people entering and leaving stores with data from the person's cell phone. For those consumers who have downloaded the app, the retailers have information about who they are (Clifford and Hardy 2013). What was once done online is now possible offline in the real world.

One such app is Shopkick, which allows retailers to track and learn how consumers shop. As an incentive, the app alerts consumers to discounts and rewards that are connected to the app. Thus, if consumers walk by the jeans rack in American Eagle they can receive messages about the jeans. Consumers who have the app are alerted that the retailer has it when they walk through the door (McFarland 2014). In turn, retailers are able to learn about traffic patterns and reach the right consumers when they are physically near merchandise they are likely to purchase.

In addition to GPS tracking, RFID tags are being placed in numerous clothing items and products we buy. These tags enable marketers and anyone with a RFID reader to access the information from the tags from a distance away. Current uses of the RFID technology include the mobile fast pass, some credit cards, and toll passes. But with the prospect of all products being tagged, the future of retail where there are no checkout lines is a real possibility. Indeed, this glimpse of the future was first shown in 1992 in an ad by IBM. The ad portrays a single man picking up some steaks and placing them inside a coat pocket and then picking up a newspaper before walking through sensors (IBM RFID Commercial 2006). The future also offers the possibility of ads being shown in retail establishment displays prompted by RFID chips on the clothing you wear (Albrecht and McIntyre 2005).

RFID tags are not without their downsides. One such concern was raised by parents of an Atlanta school that was going to use RFID bands to keep track of students on school busses. The concern was that the bands could be used by others who had RFID readers for stalking. Further, and perhaps more disturbing, is that it conditioned the children to be fine with being tracked (Zara 2013, January 8). In a similar fashion, Disney is planning to implement a Magicband, a bracelet that serves as a ticket, room key, and payment account. Such uses were criticized by Albrecht, who noted that this helps normalize RFID technology and moves us toward a surveillance society (Zara 2013, April 20).

Critics claim that the problem with the RFID technology is that it reduces the transaction costs to protect privacy. In the physical world, there is a transaction cost for a person who must cross fences and physical barriers to get information. Online, with RFID technology, it is much easier to get information. For example, it is easy for someone to scan one's garbage. Such a scenario could provide a boss, if she was suspecting her employee was becoming an alcoholic, the ability to unobtrusively scan the garbage to find out how many alcohol bottles were being disposed (Selinger 2012).

A person's house is considered his castle. Indeed, the last barrier to protect from privacy invasions has been the house. To maintain barriers, for example, do not call laws were enacted to keep privacy invasions to a minimum. However, with smart technologies now and in the future controlling electricity, heating, and refrigerators, this is coming to an end. Much attention has been given to Google's purchase of Nest, a product that regulates the temperature in the house. The product learns the patterns of the household and can be trained to take over to maximize comfort and minimize cost. There are concerns about Google and others having access to all this information (Brady 2014). For example, if one analyzed a household's power usage, more detail would be gained about a family's schedule and habits. In the future with smart refrigerators, those with access to the data could examine the power usage and see when the refrigerator was opened and how much food was in it. As this data are accumulated, it provides a digital trail for subpoenas, law requests, and hackers. When home devices are tied to a mobile device, there is added vulnerability if the phone is hacked or stolen as the mobile device serves as a remote control for the house functions (Titlow 2013).

Benefits of Future Technologies

The technologies of the future are beneficial because of the access to more information. For individuals practicing the quantification of self, this can provide data patterns to improve their health and lives. When data systems are applied to household maintenance and controlled with a mobile device, this provides the consumer with much convenience and savings. One can turn appliances on and off remotely. As these systems become more automated as with Google Nest, it removes the consumer from routine tasks and free them up cognitively. There are benefits of big data when used by the public sector at a societal level. It can improve health care delivery, education, energy usage, and homeland security. For the private sector, it helps companies know their consumers better and brings more complex products to the market.

Risks of Future Technologies

The risks in the new technologies lie in the automaticity of actions that the programs may take. The algorithms used with big data are made from a sequence of steps. Data are filtered into groups and help users see patterns and relationships. However, it is possible that the algorithms make decisions for efficiency sake that we do not necessarily want. Already Google's use of a filter bubble affects many consumers by providing a more narrow set of returned recommended links which is narrower, or different, than what may be desired by some. The use of the filter bubble limits one's freedom and choice. Another risk of the big data world is the increasing dependency on machinery and the problems that can occur when they break down.

The other risks pertinent to this book are privacy and security. First of all, with these new technologies is the threat of government requests for information. There have been accounts that government requests for personal data have been on the rise (Lightblau 2012). When the information requested comes from inside the home, this crosses a barrier of reasonableness. The second risk is the third party sharing or access to information. Currently for example, smart meters do not always send information directly to the internet cloud. Rather they store the information on local data hubs (other smart meters). This data is not necessarily secure (Rose n.d.).

With respect to security, hacking is a continued problem. Already there has been a widespread hacking of smart homes. A virus named the "Thingbot" contributed to more than 100,000 internet connected smart home devices being hacked and programmed to form a network that spammed consumers with phishing e-mails for a couple of weeks. As the number of devices grows over time, this is another area of computing that will need to be protected by strong passwords and updating software (Davis 2014).

The Theory of Creepy

New technologies are challenging social norms to break down and contributing to situations where consumers feel that the actions of marketers are creepy. The term creepy usually refers to a legal activity and not necessarily an unethical activity, but an activity that is not accepted by social norms. Creepiness also consists of a certainty level of ambiguity that causes people stress. For example, when Facebook first introduced the beacon advertising system, bloggers questioned if this was creepy (Nathan 2007).

The Beacon program was an advertising system that sent advertising data from external websites to Facebook. The purpose was to allow for targeted advertisements. Also, it allowed users to share their activities with their friends. This was done as activities on Facebook partner sites were published to a user's newsfeed. Due to a class action lawsuit this program was shut down in 2009. Other bloggers felt that it was creepy when Facebook first introduced the timeline feature (Kirkpatrick 2011).

Reviewing the introductions of new technologies shows that many of the features, which were at first deemed creepy, are now accepted. Creepy seems to be a time bound concept perhaps affecting different groups differentially.

The rapid deployment of technology is making it hard for marketers and consumers to understand what is ethical and socially acceptable. This, along with the fact that technology is eliminating transaction costs of finding out information, is inviting parties to engage in activities that would have never been considered previously. In this contextual background, Tene and Polonetsky (2013) have articulated a theory of creepy. Their argument is that creepy does not necessarily breach recognized principles of privacy or data protection law, but rather crosses traditional social norms. The claims to creepiness occur because of the differences between marketers and the consumers who are affected by the new technologies. Technological usage situations where creepiness is most prominent are:

- Ambient social apps,
- Social listening,
- Personalized analytics,
- Data driven marketing, and
- New product launches.

Examples of each of these cases are discussed next.

Ambient Social Apps

Technologies that use GPS information to identify individuals nearby have been considered creepy by many industry observers and consumers. Most notable was the app Girls Around Me. This app mapped the location of girls who checked into social networks in an app user's geographical area. The app took publically available information from Foursquare and Facebook to generate the map and provided pictures of the girls. Supporters of the app argued it was the responsibility of social media users to protect privacy and not make profiles public. It was eventually shut down due to social pressure. Nonetheless, there are other apps that have not been targeted as creepy but still have the potential to be creepy. The app Highlight shows if another network user is within 100 yards and brings up the target users profile. The app advertises itself as giving users a sixth sense (Burns 2012). At the very minimum, it can help users remember people's names.

Social Listening

It is common practice for marketers to engage in social listening, which is the analyzing of social media content for sentiment analysis and market research to help provide better service by better understanding consumer needs. Several airline companies have seemed to cross the line from using clever marketing research to being creepy. The British Airways' "Know Me" program had airline personnel googling passengers' names to learn more about them (Hume 2012).

In another program, airline KLM has a meet and seat program where passengers pick seats and seatmates based on Facebook and linked in profiles (Lubin 2012; Tzeng n.d). Some individuals might welcome the opportunity to spend time with people they have an interest in talking with. On the other hand, when people start asking other people about topics they have not conversed about previously, it can become creepy even if it was posted online.

Personalized Analytics

It is possible to obtain a lot of background information about people online. Each of us has the capability to be a personal detective using Google, white page background sites, social networks, and the like. Increasingly, individuals are going online to learn about others' digital footprints and them making judgments about them (Labrecque, Markos, and Milne

2011). There are almost no transactions costs in doing so. The questions raised by Tene and Polonetsky are when is it appropriate to do background checks on people? Is it appropriate to use Zillow to check out one's property values? Is it appropriate to check on the parents of a carpool? Indeed, it is up to the individual here to decide what is creepy. Many would argue that if its public information, then this is appropriate. However, as the information viewed moves beyond Google searches to other more time intensive and expensive pursuits, this becomes creepy. Also, when other sites post profile information that is not necessarily public, this could be considered creepy.

Data-Driven Marketing

Underlying data-driven marketing is the covert use of big data to understand the consumer. Research has shown that covert actions with existing or loyal customers, if revealed, are accepted by consumers because the choices are improved. However, if covert actions are done to get new business and the consumer finds out about the covert activities, this can be seen in a negative light (Milne, Rohm, and Bahl 2009). The Target case mentioned earlier in the book, where a model was applied to purchases to predict which customers might be pregnant, was considered very creepy (Duhigg 2012). In many respects, this can be considered a very clever execution of online behavioral advertising. However, it is the novelty and unexpected uses of data that seem to provoke the strong reactions. For marketers, being first with a marketing technology that is behaviorally based runs the risk of being creepy.

New Product Launches

Perhaps the creepiest privacy reactions are for new products because they challenge social values. Google Glass has been discussed as a potentially creepy new product (Pogue 2013). When one has a conversation with someone wearing Google Glass, there is a disadvantage. The Glass wearer can access the web, possibly run facial recognition programs, and take pictures and videos. As a measure of the type of resistance toward the product, the term Glasshole (2013) has been introduced to name wearers of the product who do not do so responsibly (e.g., turning the glasses off in restrooms and not taking pictures and videos of conversations without permission). Being creepy comes down to social norms, which can vary by age group and the newness of the technology which is rapidly evolving.

Cohort Effect on the Future of Privacy and the Perception of Creepy

There is a common belief that younger consumers have different attitudes and behaviors with respect to privacy and what is creepy. Palfrey and Gasser (2008) suggested that younger consumers born into the Internet environment treat information differently than previous generations. Indeed, there are some studies that suggest that the younger generation is less concerned about privacy and more willing to provide information than prior generations (Brown and Muchira 2004; Gauzente 2004; Madden et al. 2007; Paine et al. 2007; Palfrey and Gasser 2008; Phelps, Nowak, and Ferrell 2000; Zukowski and Brown 2007). The implication of this view is that the future of privacy protection will be less important to the younger generation.

However, a counter perspective has been offered by other research suggesting that younger consumers do care about protecting privacy, and when compared to older consumers, their preferences are not that different (Turow et al. 2009). One of the issues in using this information is to understand the components of cohorts as they move through time. Figure 7.2 shows three factors for understanding privacy attitudes over time (Milne, Gabisch, Markos, and Phelps 2012). There are age effects (the difference in the ages of individuals at single time), period effects (which reflect the different technologies between time periods), and cohort effects (the attitudes of a group of consumers as they move through time). Thus, according to the diagram, a period effect is comparing an age group (young consumers) attitude toward privacy in 2000 with the same age group in a later time period (2009). The age effect is comparing the younger consumer's attitude in a time period (2009) with an older consumers' attitude in the same time period. A cohort effect is seeing how the attitude of young consumers in 2000 changes in 2009 as they became older.

Longitudinal research on privacy attitudes suggest that both younger and older consumers are more willing to provide information for benefits

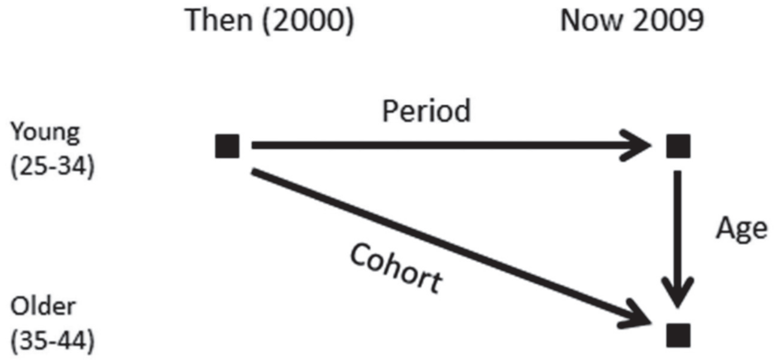

Figure 7.2 Cohort analysis for privacy

than they have been in the past. The biggest factor that explains change over time is the technological period. The evolution of the Internet seems to be changing how privacy is perceived and consumers' protection of personal information. As change takes place more rapidly, the differences between age groups in terms of privacy attitudes would seem to lessen. It is the degree of change in the new technology from the past that will have the biggest attitude toward privacy.

Erosion of Privacy

This chapter has reviewed the future of new technologies and discussed why some technological innovations are portrayed as creepy and others are not. Further, it was argued that rapid technological change will have the largest influence on privacy. To understand the toil that the technologies have on consumer ability to maintain privacy, consider the changes that technology has brought as examined through the four mechanisms for privacy introduced by Westin and discussed earlier in the book. That is, how do technological advances impinge upon a consumers' ability to achieve anonymity, solitude, intimacy, and reserve?

Loss of Anonymity

It used to be that a person could have his or her privacy by getting lost in a big city. This is not the case anymore. Surveillance cameras are everywhere and augmented by user generated content loaded on social networks. Facial recognition software can identify people. Smart phone camera apps can be uploaded to the Internet and the collective intelligence can also be used to identify images of people. As an example, the suspended Boston marathon bombers were caught by all the photo images and video surveillance cameras that captured images of them that day. As mentioned earlier, technologies are now tracing the shopping of individuals not only online but in stores. And, what one says online can now be traced to the individual; it is hard not to be observed or accountable for one's opinion.

There are both benefits and costs to the loss of anonymity. Online loss of anonymity means that there is more transparency. In this regard, the loss of anonymity does guard against uncivil behavior. However, the loss of anonymity limits individuals from being relaxed and having a chance to be authentic and engaging in unfiltered thought. As this ability to be unguarded is erased, people may have their freedoms impinged upon as they will be discovered in public and marketers will continue to send them messages. And as surveillance becomes more prevalent, the negative aspects of George Orwell's novel, 1984, come to fruition (Solove 2011).

Loss of Solitude

The pace of social media in modern society is eliminating the opportunity to be alone with one's thoughts. The computer and mobile devices with their texting capability are creating a culture of connecting. Some kids today find it scary to be alone and have to always work in groups or they become anxious (Deresiewicz 2009). One addiction that has resulted with the introduction of technology is fear of missing out (FOMO), the fear of missing out on something that is more interesting that what one is currently experiencing. This is why people are always checking their Facebook and Twitter feeds and texting constantly (Grohol n.d.). In Republic of Noise, Diana Senechal notes that we have become a culture of instant updates and communication at the expense of solitude (Senechal 2011). Indeed, Twitter and social media transcend the boundaries of the private and public worlds, eliminating the opportunity for solitude. Marketers are starting to invade these social spaces, increasing the volume of commercial messaging that is bombarded on people. In the future, solitude will be for those who seek it out and make a concerted effort to get it. Already, there is a rise in camps being offered in the woods where electronic connections are not allowed.

Loss of Intimacy

Technology is substituting for face-to-face conversations. The over reliance on texting and checking in with social media hurts intimacy with each other (Sarkis 2012). Instead of conversations being done with each other offline, more are taking places on public spaces such as Facebook and Twitter. Thus, it is difficult under these situations to keep information private. The problem with many users is that they assume their conversations are private. Even private conversations in private groups do not guarantee the information will stay private. At the same time, social listening is starting to be exercised by companies. They are paying attention to consumers and following up on what they are saying online. In an effort for consumers to gain intimacy, some consumers are turning to new technologies, such as Pair.com, which allow a private network of two to exist. These technologies, while sounding good at the onset, eventually have some wrinkles that limit consumers' privacy. Snapchat was supposed to be a privacy enhancing technology where intimate messages would dissolve. Now, the discovery that the messages still exist on servers has debunked such privacy claims (Snapchat's expired snaps 2013).

Loss of Reserve

Over sharing on social media can impinge on one's ability to maintain reserve when in public. Public listening by companies can also cross the line and limit one's ability to exercise reserve. Having businesses who know you well can enable better service but hamper one's ability to keep information private (Burns 2012). As one's digital profile expands, it becomes very difficult to exercise reserve in public. Research by Labrecque, Marcos, and Milne (2011) discuss how difficult it is to keep a balance of having enough social presence to be seen as normal but not too much or too little as to draw negative opinions.

Managing Creepy and the Future of Privacy

Managing creepiness in new technologies requires both marketers and consumers to take action.

In order to avoid engaging in creepy activities, marketers should consider the following:

- Understand consumer privacy concerns and technological social norms,
- Manage fears and ambiguity through education,
- Use privacy as a segmentation variable,
- Be aware where asymmetries in preferences exist,
- Use privacy by design principles, and
- Create a new set of social norms within the marketing organization by making privacy the fifth P.

Understanding Privacy Concerns and Technological Social Norms

Marketers can go a long way avoiding creepy situations through conducting market research that measures consumer privacy concerns and their comfort levels with particular technology. Companies should focus the research on their target audience and move away from general privacy concern questions to more specific questions that pertain to the use of technology. For example, if a marketer is considering using geofencing, the question should ask specifically whether the consumer is comfortable receiving communications on their smart phone if they are in a particular geographical proximity. In addition, the marketer should ask about the expected frequency of communication. How much communication is too much? Given that perceptions change over time, it is important to monitor the norms of consumers pertaining to this technology. Situations change and a negative reaction early on can change as consumers become educated about and familiar with the technology.

Manage Fears and Ambiguity Through Education

For marketers who have recently launched or are about to launch a new technology, customer education is an important tool for assuaging consumer fear or ambiguity—which can lead to creepiness. The technology should be clearly explained along with the privacy risks that consumers face when using the technology. If there are options to protect consumers' privacy, these features should be clearly explained. Google does a particularly good job of this by posting instructional videos on how to use and understand the features of their products. It is better for consumers to be educated by the marketers than some other third party. Managing this process effectively can also grow the level of trust.

Use Privacy as a Segmentation Variable

Consumers tend to have wide variance in their general attitudes toward privacy (Milne and Bahl 2010; Westin 1967). Roughly one-third are protective of privacy, one-third have a balanced view, and one-third are not concerned. Research has suggested that using privacy as a segmentation tool can be effective in tailoring communications about privacy sensitive topics (Milne, Rohm, and Bahl 2009). Differential messages could be delivered and more care could be given in terms of privacy protection assistance to the segment of the concerned consumer. By capturing attitudes toward privacy and appending this information to the consumer database, the better the customer relationship management. Based upon the privacy attitudes within the databases, it may be prudent to first introduce new information technologies to those consumers who are comfortable with the privacy issues.

Be Aware Where Asymmetries in Preferences Exist

A common mistake for technology-driven companies is to assume that consumers are as enthusiastic with the new technology as the company. Research has shown that asymmetries exist and that the asymmetries are larger for newer technologies. Companies such as IBM have patents of new technologies that they put on hold because they realize that the consumer market has not yet caught up in comfort and enthusiasm levels for the technologies. Similarly, Google has slowly introduced new technologies such as Google Glass due to consumer resistance. In monitoring consumer segments, it is also important to measure the level of asymmetry especially for the protective segment. Their attitudes will highlight possible privacy concern.

Use Privacy by Design Principles

Privacy by design is important to consider when introducing new technologies so as to understand all the ways that the technology could be used and potential problems. Examples of good design are Google+, which use circles to create private groups. Another is the GMAT exam, which used to rely upon fingerprints for identification. But after realizing that this information could be cross checked with criminal databases, switched to scans of palm veins (Hill 2011, July 28).

When privacy design is not used, there is the real possibility of embarrassment by design. Fitbit was an example of embarrassment by design when it made the decision to make user activity public (on Google) by default and one of the activities captured was sexual activity (Hill 2011, July 5). In these situations, the attitude of consumers should be made known to the product developers—who may be overly enthusiastic—so alterations can be made. More importantly, the privacy by design principles can help create a development process that incorporates consumer feedback throughout. The privacy by designed principles, if followed, can avoid embarrassing situations.

Create a New Set of Social Norms That Elevates Privacy to the Fifth P within the Marketing Organization

In order to stay away from privacy mistakes in the marketplace, it is necessary for all employees inside an organization to be privacy sensitive. For many companies, the process of changing the norms is guided by the privacy officer who monitors processes and can even serve as the within company educator.

To highlight the importance of privacy in the organization, a new norm can be created by promoting privacy to the fifth P (as discussed in Chapter 4). By doing so, the privacy implications of the choices pertaining to the other four Ps are explicitly examined a priori. Thus privacy implications of product (i.e., customization and information transition), place (i.e., GPS, RFID, in store tracking), price (i.e., dynamic pricing, yield management), and promotion (i.e., covert marketing, behavioral advertising) were thought out. In so doing and by introducing norms of transparency, customer trust will be enhanced. Further, the fifth P also addresses third party relationships, ensuring consumer interests are kept in mind.

As discussed throughout the book, privacy is a two-way street. With respect to privacy violations due to creepy uses of technology, consumers need to accent some responsibility. In order avoid or eliminate having creepy experiences, consumers should consider the following:

- Keep up with technology and understand its implications,
- Use technology responsibly, and
- Manage one's privacy.

Keep Up with Technology and Understand Its Implications

Technological change is a fact of life. If consumers are going to engage in the marketplace, they need to understand implication of the technology they are using. This requires consumers to read the user agreements and privacy statements. This also requires consumers to understand the defaults in terms of data sharing. A paradox of technology is that it is more difficult to use new technologies with new features that are geared to improve one's experience. Thus, one should expect it will take a reasonable time for consumers to figure out new technology and the privacy implications before using it.

Use Technology Responsibly

Consumers need to use the technology responsibly and carefully consider what information is sent over the Internet. One technology that has been misused by consumers is Snapchat. While Snapchat advertises images that disappear, it is possible for the receiver of the Snapchat to screenshot the image. Several teenage girls found out the hard way that sending nude photos of themselves over Snapchat was not responsible after their images were captured, they were blackmailed, and their photos were distributed over the Internet (Hill 2013). While marketers can have some responsibility, consumers need to be cautious. This can be done by learning about the experiences of early adopters.

Manage One's Privacy

When dealing with new technologies especially, consumers need to be vigilant and take an active role in managing their privacy. This book has discussed several actions and technological tools that consumers can follow and use to improve their privacy. Prior to using new technologies, consumers need to monitor agreements and notices, and check online to see if any other consumers have had problems. On the back end, consumer needs to use the technology responsibly and make checks on one's online reputation periodically via Google and credit checks.

Concluding Thoughts about the Future

This chapter addressed how the new information technologies such big data and the Internet of Things, while adding tremendous value to individuals and society, will require new approaches to privacy concerns. The problem is that the rapid pace of technological advancement creates situations where the use of technology breaks down existing norms, and new norms of behavior have not been established. The actions of marketers can become creepy and have a great chance of eroding consumers' traditional approaches for obtaining privacy.

Taking a broader lens, this book has examined the information exchange process between marketers and consumers. The content was offered to provide the reader with a broad overview of the privacy issue. In Chapter 1, there was a case made about why privacy is important to protect. In Chapter 2, a case was made for why privacy is needed. In Chapter 3, there was a review of the academic perspective of privacy, covering the technological history and leading academic theories. In Chapter 4, there was a detailed examination of privacy exchange in the market place. In Chapter 5, there was an examination of the particular risks consumers face from exchanging information. In Chapter 6, the perspectives of privacy protection were discussed. In this chapter, the future of privacy was discussed.

While the content in this book serves as an introduction, it is prudent to realize that this book provides only a glimpse at the tip of the iceberg to what is one of the more important social issues of our time. It is important for all of us to pause and think about privacy and our future. How we come to grips with how data is exchanged and managed will deeply impact the quality of ourselves, our lives, and the society we live in.

References

5 alternative search engines that respect your privacy. (n.d.). *How To Geek*. Retrieved May 28, 2014, from http://www.howtogeek.com/113513/5-alternative-search-engines-that-respect-your-privacy/.

8 new health-tracking sensors. (n.d.). *Boston.com*. Retrieved June 1, 2014, from http://www.boston.com/lifestyle/health/gallery/wearable_trackers/.

About TRUSTe. (n.d.). *Online Privacy Solutions, Privacy Seals & Protection from TRUSTe*. Retrieved May 28, 2014, from http://www.truste.com/about-TRUSTe/.

About the IAPP. (n.d.). *IAPP*. Retrieved May 28, 2014, from https://www.privacyassociation.org/about_iapp/.

Adam, A. (2002). Cyberstalking and Internet pornography: Gender and the gaze. *Ethics and Information Technology* 4(2), 133–142.

Albrecht, K., and McIntyre, L. (2005). *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID*. Nashville, TN: Nelson Current.

Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Monterey, CA: Brooks/Cole Pub. Co.

Altman, I. and Taylor, D. (1973). *Social penetration: The Development of Interpersonal Relationships*. New York: Holt.

Alderson, W. (1965). *Dynamic Marketing Behavior: A Functionalist Theory of Marketing*. Homewood, Illinois: Richard D. Irwin.

Angwin, J. (July 30, 2010). The Web's New Gold Mine: Your Secrets. *The Wall Street Journal.* Retrieved November 10, 2014, from http://online.wsj.com/articles/SB10001424052748703940904575395073512989404

Antivirus software. (May 25, 2014). *Wikipedia*. Retrieved May 28, 2014, from http://en.wikipedia.org/wiki/Antivirus_software.

Ariely, D. (n.d.). 3 main lessons of psychology. *Dan Ariely Blog*. Retrieved August 28, 2014, from http://danariely.com/2008/05/05/3-main-lessons-of-psychology/.

Bagozzi, R.P. (1975). Marketing as exchange. *Journal of Marketing* 39(4), 32–39.

Bahny, W. (February 13, 2013). Five enterprise instant messaging systems. *TechRepublic*. Retrieved May 28, 2014, from http://www.techrepublic.com/blog/five-apps/five-enterprise-instant-messaging-systems/#.

Barrell, J., and Jourard, S. (1976). Being honest with persons we like. *Journal of Individual Psychology* 32(2), 185–193.

Belanger, F., Hiller, J., and Smith, W. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems* 11(3–4), 245–270.

Belk, R.W. (1988). Possessions and the extended self. *Journal of Consumer Research* 15(2), 139.

Bellman, S., Johnson, E.J., and Lohse, G.L. (2001). On site: To opt-in or opt-out?: It depends on the question. *Communications of the ACM* 44(2), 25–27.

Berghel, H. (2000). Identity theft, social security numbers, and the Web. *Communications of the ACM* 43(2), 17–21.

Besbes, O., and Scarsini, M. (May 16, 2013). On information distortions in online ratings. *Columbia Business School Research Paper No. 13–36.*

Bloom, P.N., Milne, G.R., and Adler, R. (1994). Avoiding misuse of new information technologies: Legal and societal considerations. *Journal of Marketing* 58(1), 98–110.

Bosker, B. (April 29, 2010). Zuckerberg's privacy stance: Facebook CEO doesn't believe in privacy. *The Huffington Post*. Retrieved August 19, 2014, from http://www.huffingtonpost.com/2010/04/29/zuckerberg-privacy-stance_n_556679.html.

Bracetti, A. (May 10, 2012). 25 Facebook posts that have gotten people fired. *Complex Tech*. Retrieved May 28, 2014, from http://www.complex.com/tech/2012/05/25-facebook-posts-that-have-gotten-people-fired/.

Brady, D. (January 22, 2014). Nest's Tony Fadell keeps his cool as Google deal brings heat. *Bloomberg Business Week*. Retrieved June 1, 2014, from http://www.businessweek.com/articles/2014-01-22/nests-tony-fadell-keeps-his-cool-as-google-deal-brings-heat.

Brinkman, B. (July 28, 2011). *Augmented reality for decisional interference* [Video file]. Retrieved from http://www.youtube.com/watch?v=JROvsAMzSW4.

Brown, M., and Muchira, R. (2004). Investigating the relationship between Internet privacy concerns and online purchase behavior. *Journal of Electronic Commerce Research* 5(1), 62–70.

Burns, C. (April 17, 2012). 5 new social networking apps: Cool or creepy? *IBM Social Business Insights Blog*. Retrieved August 19, 2014, from https://www-304.ibm.com/connections/blogs/socialbusiness/entry/5_new_social_networking_apps_cool_or_creepy16?lang=en_us.

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

Chelune, G.J. (1975). Self-disclosure: An elaboration of its basic dimensions. *Psychological Reports* 36(1), 79–85.

Chief privacy officer. (May 24, 2014). *Wikipedia*. Retrieved May 28, 2014, from http://en.wikipedia.org/wiki/Chief_privacy_officer.

Christofides, E., Muise, A., and Desmarais, S. (March 26, 2010). *Privacy and Disclosure on Facebook: Youth and Adults' Information Disclosure and Perceptions* *of Privacy Risks*. Retrieved from University of Guelph website: http://www.psychology.uoguelph.ca/faculty/desmarais/files/OPC_Final_Report-Facebook_Privacy.pdf.

Clifford, S., and Hardy, Q. (July 14, 2013). Attention, shoppers: Store is tracking your cell. *The New York Times*. Retrieved June 1, 2014, from http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html?pagewanted=all.

Collier, J., and Bienstock, C. (2006). Measuring service quality in e-retailing. *Journal of service research 8*(3), 260–275.

Couple (app). (October 8, 2014). *Wikipedia*. Retrieved August 19, 2014, from http://en.wikipedia.org/wiki/Couple_(app).

Cranor, L.F., Kelley, P.G., Sadeh, N., and Tsai, J.Y. (2010). Location-sharing technologies: Privacy risks and controls. *I/S: A Journal of Law and Policy for the Information Society* 6(2), 119–151.

Cranor, L.F., Reagle, J., and Ackerman, M.S. (2000). Beyond concern: Understanding net users' attitudes about online privacy. In I. Vogelsang and B.J. Companine (eds.), *The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy* (pp. 47–70). Cambridge, MA: MIT Press.

Crawford, D. (n.d.). The ultimate privacy guide. *Best VPN*. Retrieved May 28, 2014, from https://www.bestvpn.com/the-ultimate-privacy-guide/.

Culnan, M.J., and Armstrong, P.K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science* 10(1), 104–115.

Culnan, M.J. and Milberg, S.T. (1998). *The Second Exchange: Managing Customer Information in Marketing Relationships* (unpublished manuscript). Washington, DC: Georgetown University.

Culnan, M.J. (1993). "How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly* 17(3), 341–363.

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

Culnan, M. (2000). Protecting privacy online: Is self-regulation working? *Journal of Public Policy & Marketing 19*(1), 20–26.

CVS Caremark settles FTC charges: Failed to protect medical and financial privacy of customers and employees; CVS Pharmacy also pays $2.25 million to settle allegations of HIPAA violations. (February 18, 2009). *Federal Trade Commission*. Retrieved May 28, 2014, from http://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial.

D'Innocenzo, A. (January 10, 2014). Target: Data breach caught up to 70M customers. *MSN News*. Retrieved August 20, 2014, from http://news.msn.com/us/target-data-breach-caught-up-to-70m-customers.

Dahl, D., Manchanda, R., and Argo, J. (2001). Embarrassment in consumer purchase: The roles of social presence and purchase familiarity. *Journal of Consumer Research* 28(3), 473–481.

Davis, G. (January 22, 2014). Smart TVs, refrigerators used in Internet-of-things cyberattack. *McAfee Blog Central*. Retrieved June 1, 2014, from https://blogs.mcafee.com/consumer/internet-of-things-cyberattack.

Deighton, J., and Johnson, P. (2013). *The Value of Data: Consequences for Insight, Innovation, and Efficiency in the U.S. Economy*. Retrieved from Data Driven Marketing Institute on May 31, 2014.

Dellarocas, C. (2010). Online reputation systems: How to design one that does what you need. *MIT Management Review* 51(3), 33–37.

Deresiewicz, W. (January 30, 2009). The end of solitude. *The Chronicle of Higher Education*. Retrieved May 29, 2014, from http://chronicle.com/article/The-End-of-Solitude/3708.

Derlega, V.J., and Chaikin, A.L. (1977). Privacy and self-disclosure in social relationships. *Journal of Social Issues* 33(3), 102–115.

Derlega, V.J. (1993). *Self-disclosure*. Newbury Park: Sage Publications.

Dixon, P. (December 18, 2014). Congressional testimony: What information do data brokers have on Consumers? *World Privacy Forum*. Retrieved July 29, 2014, from http://www.worldprivacyforum.org/2013/12/testimony-what-information-do-data-brokers-have-on-consumers/.

Direct Marketing Association (n.d). DMA choice consumer Fact Sheet. *Dma.org*. Accessed November 13, 2014, from http://thedma.org/dma-choice-background/

Do the right thing (p. 60). (2009). DMA Corporate Responsibility Department. Washington, DC: Direct Marketing Association. Retrieved from http://www.dmaresponsibility.org/DoTheRightThing/.

Dolnicar, S., and Jordaan, Y. (2007). A market-oriented approach to responsibly managing information privacy concerns in direct marketing. *Journal of Advertising* 36(2), 123–149.

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

Duhigg, C. (February 18, 2012). How companies learn your secrets. *The New York Times*. Retrieved August 20, 2014, from http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

Dunfee, T.W., Smith, N.C., and Ross, W.T. (1999). Social contracts and marketing ethics. *Journal of Marketing* 63(3), 14–32.

Dwyer, F.R., Schurr, P.H., and Oh, S. (1987). Developing buyer-seller relationships. *Journal of Marketing* 51(2), 11–27.

Eckholm, E., and Zezima, K. (March 29, 2010). 9 teenagers are charged after suicide of classmate. *The New York Times*. Retrieved August 20, 2014, from http://www.nytimes.com/2010/03/30/us/30bully.html?pagewanted=all.

EFF's top 12 ways to protect your online privacy. (April 9, 2002). *Electronic Frontier Foundation*. Retrieved May 27, 2014, from https://www.eff.org/wp/effs-top-12-ways-protect-your-online-privacy.

Enforcing privacy promises. (n.d.). *Federal Trade Commission*. Retrieved May 28, 2014, from http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises.

EPIC online guide to practical privacy tools. (n.d.). *EPIC*. Retrieved May 28, 2014, from http://epic.org/privacy/tools.html.

European convention on human rights. (May 25, 2014). *Wikipedia*. Retrieved May 28, 2014, from http://en.wikipedia.org/wiki/European_Convention_on_Human_Rights.

Facebook spammer slapped with $873M CAN-SPAM fine. (November 24, 2008). *CRN*. Retrieved August 20, 2014, from http://www.crn.com/news/security/212200253/facebook-spammer-slapped-with-873m-can-spam-fine.htm.

FTC charges deceptive privacy practices in Google's rollout of its buzz social network. (March 30, 2011). *Federal Trade Commission*. Retrieved May 28, 2014, from http://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.

FTC settlement puts an end to "history sniffing" by online advertising network charged with deceptively gathering data on consumers. (December 5, 2012). *Federal Trade Commission*. Retrieved May 28, 2014, from http://www.ftc.gov/news-events/press-releases/2012/12/ftc-settlement-puts-end-history-sniffing-online-advertising.

FTC to study data broker industry's collection and use of consumer data. (December 18, 2012). *Federal Trade Commission*. Retrieved May 28, 2014, from http://www.ftc.gov/news-events/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data.

Federal Trade Commission. (February, 2009). *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising.* (FTC). Federal Trade Commission. Retrieved November 13, 2014, from http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf

Federal Trade Commission. (March, 2012). *Protecting Consumer Privacy in an Era of Rapid Change.* (FTC). Federal Trade Commission. Retrieved November 13, 2014 from http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

Federal Trade Commission. (n.d.). *What Is Identity Theft?* Retrieved May 28, 2014, from http://www.consumer.ftc.gov/media/video-0023-what-identity-theft.

Feistel, H. (1973). Cryptography and computer privacy. *Scientific American* 228(5), 15–23.

Fertik, M. (October 22, 2010). 10 ways to protect your privacy online. *Newsweek*. Retrieved May 28, 2014, from http://www.newsweek.com/10-ways-protect-your-privacy-online-73969.

Foxman, E., and Kilcoyne, P. (1993). Information technology, marketing practice, and consumer privacy: Ethical issues. *Journal of Public Policy and Marketing* 12(1), 106–119.

Gabisch, J.A., and Milne, G.R. (2014). The impact of compensation on information ownership and privacy control. *Journal of Consumer Marketing* 31(1), 13–26.

Ganapati, P. (2014). Cellphone case tracks your vitals with built-in health sensors. *WSJ*. Retrieved June 1, 2014, from http://blogs.wsj.com/personal-technology/2014/03/07/wello-cellphone-case/.

Gauzente, C. (2004). Web merchants' privacy and security statements: How reassuring are they for consumers? A two-sided approach. *Journal of Electronic Commerce Research* 5(3), 181–198.

Geiger, H. (December 6, 2011). Facial recognition and privacy. *Center for Democracy & Technology*. Retrieved August 20, 2014, from https://cdt.org/blog/facial-recognition-and-privacy/.

Glasshole. (February 20, 2013). *Urban Dictionary*. Retrieved August 20, 2014, from http://www.urbandictionary.com/define.php?term=Glasshole.

Godin, S. (1999). *Permission Marketing: Turning Strangers into Friends, and Friends into Customers*. New York, NY: Simon & Schuster.

Goffman, E. (1959). *The Presentation of Self in Everyday Life*. Garden City, NY: Doubleday.

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy and Marketing* 10(1), 149–166.

Goodwin, C. (1992). A conceptualization of motives to seek privacy for nondeviant consumption. *Journal of Consumer Psychology* 1(3), 261–284.

Greenfield, H. (December 20, 2013). Major study sheds light on online privacy, security values, behavior. *CCIA.org*. Retrieved November 10, 2014, from https://www.ccianet.org/2013/12/major-study-sheds-light-online-privacy-security-values-behavior/.

Grohol, J. (n.d.). FOMO addiction: The fear of missing out . *Psych Central*. Retrieved June 1, 2014, from http://psychcentral.com/blog/archives/2011/04/14/fomo-addiction-the-fear-of-missing-out/.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society,* (pp. 71–80). ACM.

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

Haley, K. (April 8, 2014). The 2013 Internet security threat report: Year of the mega data breach. *Symantec*. Retrieved May 28, 2014, from http://www.symantec.com/connect/blogs/2013-internet-security-threat-report-year-mega-data-breach.

Hays, C.L. (October, 1999). Variable-Price Coke Machines Being Tested. *New York Times*. Retrieved December 9, 2014, from http://www.nytimes.com/1999/10/28/business/variable-price-coke-machine-being-tested.html.

Heide, J.B., and John, G. (1992). Do norms matter in marketing relationships? *Journal of Marketing* 56(2), 32.

Hill, K. (December 26, 2012). Oops. Mark Zuckerberg's sister has a private Facebook photo go public. *Forbes*. Retrieved August 20, 2014, from http://www.forbes.com/sites/kashmirhill/2012/12/26/oops-mark-zuckerbergs-sister-has-a-private-facebook-photo-go-public/.

Hill, K. (July 5, 2011). Fitbit moves quickly after users' sex stats exposed. *Forbes*. Retrieved August 20, 2014, from http://www.forbes.com/sites/kashmirhill/2011/07/05/fitbit-moves-quickly-after-users-sex-stats-exposed/.

Hill, K. (July 28, 2011). Why "privacy by design" is the new corporate hotness. *Forbes*. Retrieved June 1, 2014, from http://www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness/.

Hill, K. (April 8, 2013). Another day, another group of teen girls blackmailed with nude photos. *Forbes*. Retrieved June 1, 2014, from http://www.forbes.com/sites/kashmirhill/2013/04/08/another-day-another-group-of-teen-girls-blackmailed-with-nude-photos/.

Hoffman, B. (n.d.). How Google Glass may compromise your privacy. *Cybercrime News*. Retrieved August 20, 2014, from http://www.yoursecurityresource.com/nortonpc/feature/emerging_threats/google_glass_security_issues/index.html#.U4pyKSTD-M8.

Hoffman, J. (June 27, 2010). Online bullies pull schools into the fray. *The New York Times*. Retrieved August 29, 2014, from http://www.nytimes.com/2010/06/28/style/28bully.html?pagewanted=all&_r=0.

Hogg, T., and Adamic, L. (2004). Enhancing reputation mechanisms via online social networks. In J. Breese (General Chair), EC '04 fifth ACM conference on electronic commerce 2004 (pp. 236–237). New York, NY: ACM.

Holtzman, D.H. (2006). *Privacy Lost: How Technology Is Endangering your Privacy*. San Francisco: Jossey-Bass.

Houston, F.S., and Gassenheimer, J.B. (1987). Marketing and exchange. *Journal of Marketing* 51(4), 3.

Hoy, M.G., and Phelps, J. (2003). Consumer privacy and security protection on church web sites: Reasons for concern. *Journal of Public Policy & Marketing* 22(1), 58–70.

Hoy, M.G., and Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising* 10(2), 28–45.

Huitric, E. (September 5, 2008). Timeline: A history of privacy in America. *Scientific American*. Retrieved May 28, 2014, from http://www.scientificamerican.com/article.cfm?id=timeline-a-history-of-privacy.

Hume, T. (August 22, 2012). BA Googles passengers: Friendlier flights or invasion of privacy? *CNN*. Retrieved June 1, 2014, from http://www.cnn.com/2012/08/22/travel/ba-google-image-passengers/.

IBM RFID Commercial. (2006). *The Future of E-business* [Television commercial]. Retrieved from https://www.youtube.com/watch?v=eob532iEpqk

Internet 2012 in numbers. (January 16, 2013). *Pingdom*. Retrieved August 20, 2014, from http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/.

Jacoby, G.J., and Kaplan, L.B. (1972). The components of perceived risk. In M. Venkatesan (ed.), *Proceedings of the 3rd Annual Conference of the Association for Consumer Research* (pp. 382–392). College Park, MD: ACR.

Johnson, E., Bellman, S., and Lohse, G. (2002). Defaults, framing and privacy: Why opting in-opting out. *Marketing Letters* 13(1), 5–15.

Jouvenal, J. (2013, July 20). Social media becomes stalkers' tool. *Japan Times RSS*. Retrieved May 28, 2014, from http://www.japantimes.co.jp/news/2013/07/20/national/social-media-becomes-stalkers-tool/#.UtggcSQo6M8.

Kaikati, A.M., and Kaikati, J.G. (2004). Stealth marketing: How to reach consumers surreptitiously. *California Management Review* 46(4), 6–22.

Kelly, M. (August 23, 2013). Data breach interactive chart shows major increase in security flaws. *VentureBeat*. Retrieved May 28, 2014, from http://venturebeat.com/2013/08/23/data-breach-graphic/.

Kerr, J. (February 22, 2014). Stores can see where you go by tracking phones. *USA Today*. Retrieved June 1, 2014, from http://www.usatoday.com/story/money/business/2014/02/22/retailers-tracking-shoppers-smartphones-in-store/5711945/.

Kirkpatrick, M. (September 22, 2011). Facebook's new timeline, beacon & the uncanny valley. *ReadWrite*. Retrieved June 1, 2014, from http://readwrite.com/2011/09/22/facebooks_new_timeline_beacon_creepy#awesm=~ozITtjFnp2H2aI.

Krishnamurthy, S. (2001). A comprehensive analysis of permission marketing. *Journal of Computer-Mediated Communication* 6(2), 0.

Kumaraguru, P., and Cranor, L.F. (December, 2005). *Privacy Indexes: A Survey of Westin's Studies*. Retrieved from Carnegie Mellon University Website: http://repository.cmu.edu/cgi/viewcontent.cgi?article=1857&context=isr&sei-redir=1&referer=http%3A%2F%2Fscholar.google.com%2Fscholar_url%3Fhl%3Den%26q%3Dhttp%3A%2F%2Frepository.cmu.edu%2Fcgi%2Fviewcontent.cgi%253Farticle%253D1857%2526context%253Disr%26sa%3DX%26scisig%3DAAGBfm378EfPspV4GLHDGXZxju9GZNkDAw%26oi%3Dscholarr#search=%22http%3A%2F%2Frepository.cmu.edu%2Fcgi%2Fviewcontent.cgi%3Farticle%3D1857%26context%3Disr%22.

Labrecque, L.I., Markos, E., and Milne, G.R. (2011). Online personal branding: processes, challenges, and implications. *Journal of Interactive Marketing* 25(1), 37–50.

Labrecque, L.I., Milne, G.R., Peltier, J.W., and Phelps, J.E. (2012). The viability of removing personal information from online White Page directories: Are consumer perceptions aligned with reality? *Journal of Consumer Affairs* 46(2), 345–356.

Lady Godiva. (August 14, 2014). *Wikipedia*. Retrieved August 22, 2014, from http://en.wikipedia.org/wiki/Lady_Godiva.

Langenderfer, J., and Linhoff, S. (2005). The emergence of biometrics and its effect on consumers. *Journal of Consumer Affairs* 39(2), 314–338.

Lapore, J. (October 8, 2013). The hidden history of privacy. *The New Yorker*. Retrieved August 23, 2014, from http://www.newyorker.com/online/blogs/festival/2013/10/the-hidden-history-of-privacy.html.

Laufer, R.S., Proshansky, H.M., and Wolfe, M. (1976). Some analytic dimensions of privacy. In H.M. Proshansky, W.H. Ittelson, and L.G. Rivlin (eds.), *Environmental Psychology: People and Their Physical Setting* (pp. 206–217). New York, NY: Holt, Rinehart & Winston.

Laufer, R.S., and Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues* 33(3), 22–42.

Lubin, G. (February 24, 2012). KLM introduces a new way to be creepy on an airplane. *Business Insider*. Retrieved June 1, 2014, from http://www.businessinsider.com/klm-introduces-a-new-way-to-be-creepy-on-an-airplane-2012-2.

Macneil, I.R. (1980). *The New Social Contract: An Inquiry into Modern Contractual Relations*. New Haven: Yale University Press.

Madden, M., Fox, S., Smith, A., and Vitak, J. (December 16, 2007). Digital footprints. *Pew Research Internet Project*. Retrieved August 30, 2014, from http://www.pewinternet.org/2007/12/16/digital-footprints/.

Margulis, S. (2003). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues* 59(2), 411–429.

Markos, E., and Milne, G. (2011). Sensitive Information, Benefits, and Trust: Effects on Consumers' Likelihood to Disclose Personal Information. Working Paper University of Massachusetts Amherst.

Markos, E. (January 1, 2010). Consumer privacy: A two essay dissertation examining perceptions of information sensitivity. Doctoral dissertation. Retrieved May 31, 2014 from Proquest. (Paper AAI3427593).

Marshall, T.C. (2012). Facebook surveillance of former romantic partners: Associations with postbreakup recovery and personal growth. *Cyberpsychology, Behavior, and Social Networking* 15(10), 521–526.

Masnick, M. (September 27, 2013). The war on fake reviews ramps up: NY fines companies for fake Yelp reviews. *Techdirt*. Retrieved May 28, 2014, from https://www.techdirt.com/articles/20130927/01425424673/war-fake-reviews-ramps-up-ny-fines-companies-fake-yelp-reviews.shtml.

Mayer-Schonberger, V. (2009). *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press.

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

McCoy, S., Everard, S., Polak, P., and D. Galletta, (2007). The effects of online advertising. *Communications of the ACM* 50(3), 84–88

McCoy, D., Kohno, T., and Sicker, D. (2008). Shining light in dark places: Understanding the Tor network. In N. Borisov and I. Goldberg (eds.), *The 8th Privacy Enhancing Technologies Symposium* (pp. 63–76). Leuven, Belgium: Springer.

McFarland M. (2014). American Eagle Outfitters lures customer into fitting rooms with help of beacons. *The Washington Post.* Retrieved November 14, 2014, from http://www.washingtonpost.com/blogs/innovations/wp/2014/10/15/american-eagle-outfitters-lures-customers-into-fitting-rooms-with-help-of-beacons/

Milne, G. R. (1997). Consumer Participation in Mailing Lists: A Field Experiment. *Journal of Public Policy & Marketing* 16(2), 298–309.

Milne, G.R., and Bahl, S. (2010). Are there differences between consumers' and marketers' privacy expectations? A segment - and technology-level analysis. *Journal of Public Policy & Marketing* 29(1), 138–149.

Milne, G., Bahl, S. and Rohm, A. (2008). Toward a Framework for Assessing Covert Marketing Practices. *Journal of Public Policy & Marketing 22(1)*, 57–62.

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

Milne, G. and Boza, M. (1998). Consumers' trust and concern about organizations use of personal information in direct marketing, *Marketing Science Institute Report.* No 98–117

Milne, G.R., Culnan, M.J., and Greene, H. (2006). A longitudinal assessment of online privacy notice readability. *Journal of Public Policy & Marketing* 25(2), 238–249.

Milne, G.R., and 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.

Milne, G., and Culnan, M. (2002). Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998–2001 US web surveys. *The Information Society 18*(5), 345–359.

Milne, G.R., Gabisch, J., Markos, E., and Phelps, J. (2012). Changes in consumer willingness to provide information over the last decade: A cohort analysis. *International Journal of Integrated Marketing Communications* 4(2), 44–59.

Milne, G.R., and Gordon, M. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing* 12(2), 206–215.

Milne, G.R., and Gordon, M. (1994). A segmentation study of consumers' attitudes toward direct mail. *Journal of Direct Marketing* 8(2), 45–52.

Milne, G.R., Labrecque, L., and Cromer, C. (2009). Toward an understanding of the online consumers risky behavior and protection practices. *Journal of Consumer Affairs* 43(3), 449–473.

Milne, G.R., Markos, E.C., and Bahl, S. (May 30, 2008). What Did You Buy? When Consumers Consider this Information Sensitive. Paper presented at 2008 Marketing and Public Policy Conference, Philadelphia, PA.

Milne, G.R., Rohm, A., and Bahl, S. (2009). If it's legal, is it acceptable?: Consumer reactions to online covert marketing. *Journal of Advertising* 38(4), 107–122.

Milne, G., Rohm, A. and Bahl, S. (2005). Consumers' protection of online privacy and identity. *Journal of Consumer Affairs*. 38(2), 217–232.

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

Milne, G.R. (2003). How well do consumers protect themselves from identity theft? *Journal of Consumer Affairs* 37(2), 388–402.

Milne, G.R. (2000). Privacy and ethical issues in database/interactive marketing and public policy: A research framework and overview of the special issue. *Journal of Public Policy & Marketing* 19(1), 1–6.

Milne, G.R., Hajjat, F., and Markos E. (2014). *Privacy Risk*. Working Paper. University of Massachusetts Amherst.

Milne, G.R., and Ross, S. (2013). The Changing Landscape of Consumers Attitudes toward Database Marketing: 1997 vs. 2013. Working Paper. University of Massachusetts Amherst.

Miyazaki, A., and Fernandez, A. (2000). Internet privacy and security: An examination of online retailers. *Journal of Public Policy & Marketing* 19(Spring), 54–61.

Miyazaki, A.D. (2008). Online privacy and the disclosure of cookie use: Effects on consumer trust and anticipated patronage. *Journal of Public Policy & Marketing* 27(1), 19–33.

Miyazaki, A.D., and Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs* 35(1), 27–44.

Moon, Y. (2000). Intimate exchanges: Using computers to elicit self-disclosure from consumers. *Journal of Consumer Research* 26(4), 323–339.

Moorman, C. (2013). Why companies should compete on privacy (and what customers should do to help). *www.forbes.com*. Retrieved November 10, 2014. http://www.forbes.com/sites/christinemoorman/2013/09/23/why-companies-should-compete-on-privacy/.

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

Morgan, R.M., and Hunt, S.D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing* 58(3), 20.

Moschel, M. (n.d.). The beginner's guide to quantified self (plus, a list of the best personal data tools out there). *Technori*. Retrieved June 1, 2014, from http://technori.com/2013/04/4281-the-beginners-guide-to-quantified-self-plus-a-list-of-the-best-personal-data-tools-out-there.

Myspace settles FTC charges that it misled millions of users about sharing personal information with advertisers. (May 8, 2012). *Federal Trade Commission*. Retrieved May 28, 2014, from http://www.ftc.gov/news-events/press-releases/2012/05/myspace-settles-ftc-charges-it-misled-millions-users-about.

Nathan. (November 28, 2007). The beacon: clever or creepy? *Blogstring*. Retrieved August 23, 2014, from http://blogstring.com/2007/11/28/the-beacon-clever-or-creepy/.

National Science Foundation. (n.d.). *What is identity (ID) theft? (NSF). National Science Foundation*. Retrieved from http://www.nsf.gov/oig/identitytheft.pdf.

Nearly one million LifeLock victims to receive refund checks from FTC. (November 18, 2010). *Federal Trade Commission*. Retrieved May 28, 2014, from http://www.ftc.gov/news-events/press-releases/2010/11/nearly-one-million-lifelock-victims-receive-refund-checks-ftc.

New, T. (May 27, 2013). Do not untick this box if you do not want to not receive updates. *Formisimo*. Retrieved August 23, 2014, from http://www.formisimo.com/blog/do-not-untick-this-box-if-you-do-not-want-to-not-receive-updates/.

Norberg, P.A., Horne, D.A., and Horne, D. (2009). Standing in the footprint: including the self in the privacy debate and policy development. *Journal of Consumer Affairs* 43(3), 495–515.

Nosowits, D. (August 9, 2013). What are your options now for secure email? *Popular Science*. Retrieved May 28, 2014, from http://www.popsci.com/technology/article/2013-08/what-are-your-options-secure-email.

Online privacy and security certification service settles FTC charges. (February 25, 2010). *Federal Trade Commission*. Retrieved May 28, 2014, from http://www

.ftc.gov/news-events/press-releases/2010/02/online-privacy-and-security-certification-service-settles-ftc.

Ortega, S. (n.d.). The 12 best add-ons for private and secure Internet browsing. *About.com*. Retrieved May 28, 2014, from http://browsers.about.com/od/addonsplugi2/tp/browser_security_privacy.htm.

Orwell, G. (1949). *Nineteen Eighty-four.* 1st American ed. New York: Harcourt, Brace.

Ouellette, P. (August 27, 2013). Advocate medical group endures massive data breach. *Health IT Security*. Retrieved August 19, 2014, from http://healthitsecurity.com/2013/08/27/advocate-medical-group-endures-massive-data-breach/.

Paine, C., Reips, U., Stieger, S., Joinson, A., and Buchanan, T. (2007). Internet users' perceptions of privacy concerns and privacy actions. *International Journal of Human-Computer Studies* 65(6), 526–536.

Palfrey, J.G., and Gasser, U. (2008). *Born Digital: Understanding the First Generation of Digital Natives*. New York, NY: Basic Books.

Paul, I. (September 9, 2013). 3 essential techniques to protect your online privacy. *PCWorld*. Retrieved May 27, 2014, from http://www.pcworld.com/article/2052813/3-essential-techniques-to-protect-your-online-privacy.html.

Perreault, William D. (1992). The Shifting Paradigm in Marketing Research. *Journal of the Academy of Marketing Science*, 20(fall), 367–376.

Peters, J., and Stelter, B. (November 6, 2010). The Facebook skeletons come out. *The New York Times*. Retrieved August 30, 2014, from http://www.nytimes.com/2010/11/07/fashion/07indiscretions.html?_r=0.

Peslak, A. (2005). An Ethical Exploration of Privacy and Radio Frequency Indentification. *Journal of Business Ethics* 59(4), 327–345.

Petronio, S. (2002). *Boundaries of Privacy: The Dialectics of Disclosure*. Albany: State University of New York Press.

Petty, R.D. (2000). Marketing without consent: Consumer choice and costs, privacy, and public policy. *Journal of Public Policy & Marketing* 19(1), 42–53.

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

Pinola, M. (January 4, 2014). AVG PrivacyFix stops retailers from tracking you with your phone. *The Courant*. Retrieved August 19, 2014, from http://articles.courant.com/2014-01-04/business/hc-ls-avg-privacy-app-20140104_1_wi-fi-android-devices-phone.

Pinola, M. (October 28, 2011). How to create a fake identity and stay anonymous online. *Lifehacker*. Retrieved May 28, 2014, from http://lifehacker.com/5854203/how-to-create-a-fake-identity-and-stay-anonymous-online.

Pogue, D. (May 14, 2013). Why Google Glass is creepy. *Scientific American Global RSS*. Retrieved June 1, 2014, from http://www.scientificamerican.com/article/why-google-glass-is-creepy/.

Prabhu, J., and Stewart, D. (2001). Signaling strategies in competitive interaction: Building reputations and hiding the truth. *Journal of Marketing Research* 38(1), 62–72.

Protecting customer information online. (n.d.). *TRUSTe*. Retrieved May 28, 2014, from http://www.truste.com/resources/privacy-best-practices.

Provider of medical transcript services settles FTC charges that it failed to adequately protect consumers' personal information. (January 31, 2014). *Federal Trade Commission*. Retrieved May 28, 2014, from http://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it.

Rainie, L., Kiesler, S., Kang, R., and Madden, M. (September 5, 2013). Anonymity, privacy, and security online. *Pew Research Centers Internet American Life Project*. Retrieved May 28, 2014, from http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/.

Rao, J.M., and Reiley, D.H. (2012). The economics of spam. *Journal of Economic Perspectives* 26(3), 87–110.

Rodriguez, D. (May 1, 2013). Ten steps to a quality privacy program: Taking your program to the next level. *IAPP*. Retrieved May 28, 2014, from https://www.privacyassociation.org/publications/2013_05_01_ten_steps_to_a_quality_privacy_program_taking_your_program_to.

Rogers, K. (February 5, 2014). Someone became an identity theft victim every 2 seconds last year. *Fox Business*. Retrieved May 28, 2014, from http://www.foxbusiness.com/personal-finance/2014/02/05/someone-became-identity-theft-victim-every-2-seconds-last-year/.

Rose, A. (n.d.). The Internet of things is set to change security priorities. *Computer Weekly*. Retrieved June 1, 2014, from http://www.computerweekly.com/feature/The-internet-of-things-is-set-to-change-security-priorities.

Sackmann, S., Straker, J., and Accorsi, R. (2006). Personalization in privacy-aware highly dynamic systems. *Communications of the ACM* 49(9), 32.

Salter, M., and Bryden, C. (2009). I can see you: harassment and stalking on the Internet. *Information and Communications Technology Law* 18(2), 99–122.

Sarkis, S. (May 1, 2012). Technology and the loss of intimacy. *Psychology Today*. Retrieved June 1, 2014, from http://www.psychologytoday.com/blog/%5Bfield_blog_ref-title-raw%5D/201205/technology-and-the-loss-intimacy.

Sasso, B. (September 12, 2013). FTC examines if Facebook breaking 2011 privacy deal. *The Hill*. Retrieved May 28, 2014, from http://thehill.com/blogs/hillicon-valley/technology/321825-ftc-reviewing-facebook-privacy-changes.

Schlosser, A.E., White, T.B., and Lloyd, S.M. (2006). Converting web site visitors into buyers: How web site investment increases consumer trusting beliefs and online purchase intentions. *Journal of Marketing* 70(2), 133–148.

Scoble, R., and Israel, S. (2013). *Age of Context: Mobile, Sensors, Data and the Future of Privacy*. N.p.: Self-published.

Selinger, E. (November 2, 2012). Why we need new rights to privacy. *Slate Magazine*. Retrieved June 1, 2014, from http://www.slate.com/articles/technology/future_tense/2012/11/harry_surden_suggests_rfid_and_other_tech_advances_necessitate_new_privacy.html.

Senechal, D. (2011). *Republic of Noise: The Loss of Solitude in Schools and Culture*. Lanham, Md.: Rowman & Littlefield Education.

Schwartz, P., and Solove, D. (2011). The PII problem: privacy and a new concept of personally identifiable information. *N.Y.U. Law Review*. 1814–1894.

Sheehan, K. and Hoy, M. (2000). Dimensions of privacy concern among online customers. *Journal of Public Policy & Marketing* 19(1), 62–73.

Shookman, S. (October 14, 2013). Allyssa Griffiths' 5-year battle with social media stalker. *WUSA 9*. Retrieved May 28, 2014, from http://www.wusa9.com/news/article/277968/373/Womans-5-year-battle-with-social-media-stalker.

Singer, N. (May 17, 2014). Never forgetting a face. *The New York Times*. Retrieved August 23, 2014, from http://www.nytimes.com/2014/05/18/technology/never-forgetting-a-face.html?_r=0.

Slane, A. (2005). Home is where the Internet connection is: Law, spam and the protection of personal space. *University of Ottawa Law & Technology Journal* 2(2), 255–290.

Smith, R.E. (2000). *Ben Franklin's web site: Privacy and curiosity from Plymouth Rock to the internet*. Providence, RI: Privacy Journal.

Snapchat's expired snaps are not deleted, just hidden. (May 15, 2013). *The Guardian*. Retrieved June 1, 2014, from http://www.theguardian.com/media-network/partner-zone-infosecurity/snapchat-photos-not-deleted-hidden.

Solano, C., and Dunnam, M. (1985). Two's company: Self-disclosure and reciprocity in triads versus dyads. *Social Psychology Quarterly* 48(2), 183–187.

Solove, D. (June 22, 2011). The virtues of anonymity. *The New York Times*. Retrieved June 1, 2014, from http://www.nytimes.com/roomfordebate/2011/06/21/youre-mad-youre-on-youtube/the-virtues-of-anonymity.

Solove, D.J. (2007). *The Future of Reputation Gossip, Rumor, and Privacy on the Internet*. New Haven: Yale University Press.

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

Spam. (n.d.). *Merriam-Webster*. Retrieved May 28, 2014, from http://www.merriam-webster.com/dictionary/spam.

Spam (Monty Python). (May 24, 2014). *Wikipedia*. Retrieved May 28, 2014, from http://en.wikipedia.org/wiki/Spam_(Monty_Python).

Sprenger, P. (January 26, 1999). Sun on privacy: "Get Over It". *WIRED*. Retrieved August 23, 2014, from http://archive.wired.com/politics/law/news/1999/01/17538.

Spy vs. spy. (October 3, 2010). *Concordia University–Wisconsin Department of History*. Retrieved May 28, 2014, from http://cuwhist.wordpress.com/history-culture/spy-vs-spy/.

Stolze, J. (February 6, 2009). Could you live without the Internet? *Ted University*. Lecture conducted from Ted, Long Beach.

Swire, P.P., and Bermann, S. (2007). *Information Privacy: Official Reference for the Certified Information Privacy Professional (CIPP)*. York, ME: International Association of Privacy Professionals.

Tene, O., and Polonetsky J. (2013). "A Theory of Creepy: Technology, Privacy and Shifiting Social Norms, *Yale J.L & Tech.* 16, 59–102.

Tsai, J., Kelley, P., Cranor, L., and Sadeh, N. (2010). Location Sharing Technologies: Privacy Risks and Controls, *I/S: A Journal of Law and Policy for the Information Society* 6(2), 119–151.

Tsang, M.M., Ho, S., and Liang, T. (2004). Consumer attitudes toward mobile advertising: An empirical study. *International Journal of Electronic Commerce* 8(3), 65–78.

TRUSTe. (May 21, 2014). *Wikipedia*. Retrieved May 28, 2014, from http://en.wikipedia.org/wiki/TRUSTe.

Titlow, J. (March 18, 2013). Smart homes: Our next digital privacy nightmare. *ReadWrite*. Retrieved June 1, 2014, from http://readwrite.com/2013/03/18/smart-homes-our-next-digital-privacy-nightmare#awesm=~oxyNcwbEagwLtY)].

Toor, A. (June 3, 2010). Facebook harms American marriages, survey suggests. *Switched*. Retrieved May 28, 2014, from http://www.switched.com/2010/06/03/facebook-kills-american-marriages-survey-suggests/.

Turow, J. (June 25, 2003). *Americans & Online Privacy: The System is Broken*. Retrieved from The Annenberg Public Policy Center of The University of Pennsylvania website: http://cdn.annenbergpublicpolicycenter.org/wp-content/uploads/20030701_online_privacy_report2.pdf.

Turow, J., King, J., Hoofnagle, C.J., Bleakley, A., and Hennessy, M. (September 29, 2009). *Americans Reject Tailored Advertising and Three Activities that Enable It*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

Tyson, J. (n.d.). How firewalls work. *HowStuffWorks*. Retrieved May 28, 2014, from http://computer.howstuffworks.com/firewall.htm.

Tzeng, E. (n.d.). Customer spotlight: KLM's meet & seat connects flyers through social. *Gigya Blog*. Retrieved June 1, 2014, from https://blog.gigya.com/customer-spotligh-klms-meet-seat-connects-flyers-through-social/.

Urken, R. (June 27, 2011). Is the E-ZPass Box a Trojan Horse for privacy invasions? *Aol Autos*. Retrieved June 1, 2014, from http://autos.aol.com/article/e-zpass-privacy-invasion/.

The U.S. Chamber Institute for Legal Reform (October, 2013). *The Juggernaut of TCPA Litigation: The Problems with Uncapped Statutory Damages*. Retrieved from http://www.instituteforlegalreform.com/resource/the-juggernaut-of-tcpa-litigation--the-problems-with-uncapped-statutory-damages/.

Valentino-Devries, J., Singer-Vine, J., and Soltani, A. (December 24, 2012). Websites vary prices, deals based on users' information. *The Wall Street Journal*. Retrieved May 28, 2014, from http://online.wsj.com/news/articles/SB10001424127887323777204578189391813881534.

Vogel, P. (July 11, 2012). The high privacy price of auto insurance monitoring discounts. *E-Commerce Times*. Retrieved June 1, 2014, from http://www.ecommercetimes.com/story/75600.html#sthash.FQQv5rxj.dpuf.

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

Weible, R.J. (1993). Privacy and data: An empirical study of the influence of types of data and situation context upon privacy perceptions. Unpublished doctoral dissertation. Mississippi State University, Mississippi State, MS.

Weiss, S. (2008). The need for a paradigm shift in addressing privacy risks in social networking applications. *The International Federation for Information Processing* 262, 161–171.

Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.

White, T.B. (2004). Consumer disclosure and disclosure avoidance: A motivational framework. *Journal of Consumer Psychology* 14(1–2), 41–51.

Whittaker, Z. (September 4, 2012). Apple patent could remotely disable protesters' phone cameras. *ZDNet*. Retrieved May 28, 2014, from http://www.zdnet.com/"apple-patent-could-remotely-disable-protesters-phone-cameras-7000003640/.

Wingfield, N. (February 6, 2013). Microsoft attacks Google on Gmail privacy. *The New York Times*. Retrieved August 23, 2014, from http://bits.blogs.nytimes.com/2013/02/06/microsoft-attacks-google-on-gmail-privacy/?_php=true&_type=blogs&_r=0.

Wolverton, T. (May 27, 2013). Google is flirting with what company chairman Eric Schmidt once called "the creepy line." *Marin Independent Journal*. Retrieved August 23, 2014, from http://www.marinij.com/ci_23328535/wolverton-google-is-flirting-what-company-chairman-eric.

Woodyard, C., and O'Donnell, J. (March 25, 2013). Your car may be invading your privacy. *USA Today*. Retrieved June 1, 2014, from http://www.usatoday.com/story/money/cars/2013/03/24/car-spying-edr-data-privacy/1991751/.

Wright, M. (August 16, 2013). Sexual blackmail on Skype: how sadistic crooks drive young people to the point of suicide. *The Telegraph*. Retrieved May 28, 2014, from http://blogs.telegraph.co.uk/technology/micwright/100009856/sexual-blackmail-on-skype-how-sadistic-crooks-drive-young-people-to-the-point-of-suicide/.

Xanga.com to pay $1 million for violating children's online privacy protection rule. (n.d.). *Federal Trade Commission*. Retrieved September 7, 2006, from http://www.ftc.gov/news-events/press-releases/2006/09/xangacom-pay-1-million-violating-childrens-online-privacy.

Yang, J., and Jayakumar, A. (January 10, 2014). Target says up to 70 million more customers were hit by December data breach. *The Washington Post*. Retrieved August 23, 2014, from http://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media* 49(1), 86–110.

Zara, C. (January 8, 2013). The mouse is watching: Disney's bracelets spark big brother fears. *International Business Times*. Retrieved June 1, 2014, from http://www.ibtimes.com/disney-worlds-rfid-tracking-bracelets-are-slippery-slope-warns-privacy-advocate-1001790.

Zara, C. (April 20, 2013). Invasion of privacy? RFID tracking kids on school buses; privacy advocates concerned by attendance management pilot program in Gordon County, Ga. *International Business Times*. Retrieved June 1, 2014, from http://www.ibtimes.com/invasion-privacy-rfid-tracking-kids-school-buses-privacy-advocates-concerned-attendance-management.

Zhang, M. (October 30, 2013). The emperor's new photographs: Are appropriated street view shots art? *PetaPixel*. Retrieved May 28, 2014, from http://petapixel.com/2012/10/30/the-emperors-new-photographs-are-appropriated-street-view-shots-art/.

Zukowski, T., and Brown, I. (October, 2007). Examining the influence of demographic factors on internet users' information privacy concerns. In *Proceedings of the 2007 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries* (pp. 197–204). New York, NY: ACM.

Index

OTHER TITLES IN OUR DIGITAL AND SOCIAL MEDIA MARKETING AND ADVERTISING COLLECTION

Vicky Crittenden, Babson College, Editor

- *Viral Marketing and Social Networks* by Maria Petrescu
- *Herding Cats: A Strategic Approach to Social Media Marketing* by Andrew Rohm and Michael Weiss
- *Effective Advertising Strategies for Your Business* by Cong Li
- *Social Roots: Why Social Innovations Are Creating the Influence Economy* by Cindy Gordon, John P. Girard, and Andrew Weir
- *Social Media Branding For Small Business: The 5-Sources Model* by Robert Davis
- *A Beginner's Guide to Mobile Marketing* by Karen Mishra and Molly Garris

Forthcoming In This Collection

- *Using and Managing Online Communities* by Edward Boon
- *Electronic Word of Mouth for Service Businesses* by Linda W. Lee
- *Fostering Brand Community Through Social Media* by Debra A. Laverie, Shannon B. Rinaldo, and William F. Humphrey, Jr.
- *Digital Marketing Management: A Handbook for the Current (or Future) CEO* by Debra Zahay

Announcing the Business Expert Press Digital Library

Concise e-books business students need for classroom and research

This bok can also be purchased in an e-book collection by your library as

- a one-time purchase,
- that is owned forever,
- allows for simultaneous readers,
- has no restrictions on printing, and
- can be downloaded as PDFs from within the library community.

Our digital library collections are a great solution to beat the rising cost of textbooks. E-books can be loaded into their course management systems or onto student's e-book readers.
The **Business Expert Press** digital libraries are very affordable, with no obligation to buy in future years. For more information, please visit www.businessexpertpress.com/librarians. To set up a trial in the United States, please contact **Adam Chesler** at adam.chesler@businessexpertpress.com. For all other regions, contact **Nicole Lee** at nicole.lee@igroupnet.com.

Digital Privacy in the Marketplace

Perspectives on the Information Exchange

George R. Milne

Digital Privacy in the Marketplace focuses on the data exchanges between marketers and consumers, with special attention to the privacy challenges that are brought about by new information technologies. The purpose of this book is to provide a background source to help the reader think more deeply about the impact of privacy issues on both consumers and marketers. It covers topics such as: why privacy is needed, the technological, historical and academic theories of privacy, how market exchange affects privacy, what are the privacy harms and protections available, and what is the likely future of privacy.

George R. Milne is a professor of marketing and director of the Isenberg PhD program at the University of Massachusetts Amherst. He holds a PhD in marketing from the University of North Carolina at Chapel Hill and an MA and BA in economics from the University of Utah. A majority of Dr. Milne's research has focused on public policy and marketing and interactive marketing topics, particularly related to the area of information privacy. Dr. Milne has published over 60 articles in journals such as *Journal of Marketing*, *Journal of Interactive Marketing*, *Journal of Public Policy* and *Marketing*, and *Journal of Consumer Affairs*. He lives in Amherst, MA and finds privacy by spending time in nature and through his mediation practice.

DIGITAL AND SOCIAL MEDIA MARKETING AND ADVERTISING COLLECTION
Victoria L. Crittenden, *Editor*

BEP BUSINESS EXPERT PRESS

e-ISBN 978-1-60649-849-1
90000
9 781606 498491