Customer Privacy Concerns and Privacy Protective Responses

V. Kumar, W. Reinartz, *Customer Relationship Management*, Springer Texts in Business and Economics, https://doi.org/10.1007/978-3-662-55381-7_14

Overview

Companies increasingly collect and use data about their current and potential customers to improve their customer relationship management (CRM), sales, and service effectiveness. By obtaining information on customers' transactions and behaviors, as well as their socio-demographic profiles, companies can better understand their customers' preferences and desires. Thus they build up customer intelligence to enable them to refine their strategic marketing decision making and enhance customer relationships, especially with their most valuable customers. The value of such customer information to companies is clear from Facebook's market capitalization of over $300 billion, largely because the online social network site hosts customer profiles of more than 1 billion active users (Statista, 2016). However, companies are also finding a growing reluctance among customers, who prefer not to disclose their personal information or allow tracking of their behaviors out of their concerns for privacy (Wirtz & Lwin, 2009). For example, in 2011 Google aborted its online mapping project Street View in Germany, following massive protests from communities and a media outrage. More than 240,000 households in 20 cities demanded pixelating their addresses, German politicians called for strict adherence to data protection regulations. A more recent case is the transfer of user telephone and contact data from the instant messaging service WhatsApp to its parent company Facebook. As soon as word of this practice got out, downloads of WhatsApp rival Threema skyrocketed in Europe. This is largely attributed to the Swiss company's positioning as a secure and data conscious alternative to WhatsApp.

Although especially pronounced in Europe, privacy concerns and its consequences are pervasive (Martin & Murphy, 2016). In a 2015 study by data intelligence specialist GBG, up to 71% of consumers revealed to give incorrect information when asked for private details by companies (GBG, 2015). More than two out of three state as a reason that they believed costs of data disclosure outweigh the benefits. Furthermore, growing governmental regulations related to the gathering and use of personal information are raising new obstacles for companies. Accordingly, this chapter outlines customer privacy concerns and their respective implications for successful customer relationship management.

First, the chapter begins by presenting trends and drivers related to customer privacy concerns. Second, we discuss governmental regulations in a cross-country comparison to reflect the different prepositions that companies face in different markets. Third, the underlying psychological processes and respective customer responses are identified and summarized in a comprehensive conceptual framework that indicates implications for responsible privacy handling policies. We also shed light on the privacy paradox, namely, the relationship between consumers' intention to disclose personal information and their actual personal information disclosure behaviors (Norberg, Horne, & Horne, 2007). Our overall framework depicts the context of customer privacy concerns and the respective consequences and implications for companies, as we show in Fig. 14.1.

14.1 Customer Privacy Concerns

14.1.1 Customer Privacy

Definitions of privacy vary broadly depending on the setting and environmental factors. Especially in the context of CRM, the concept of customer privacy often has been merged with data protection, such that privacy represents a form of personal information management (Roznowski, 2003). Customer privacy then can be defined as «the power of the individual to personally control (vis-à-vis other individuals, groups, organizations, etc.) information about one's self,» which includes the collection, storage, usage, and release of personal information (Stone, Gueutal, Gardner, & McClure, 1983). If a company's CRM is to foster relationships with current customers and acquire new custom-

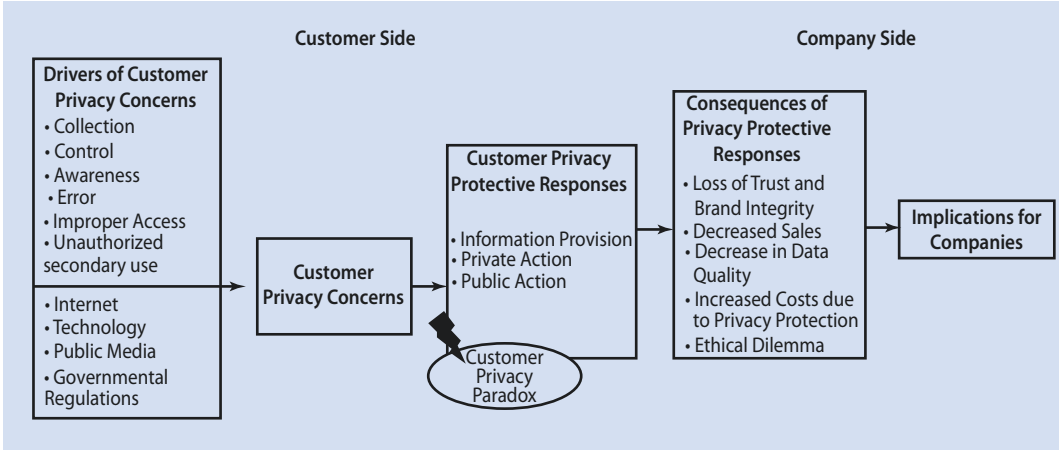


Fig. 14.1 Customer privacy concerns and implications for companies

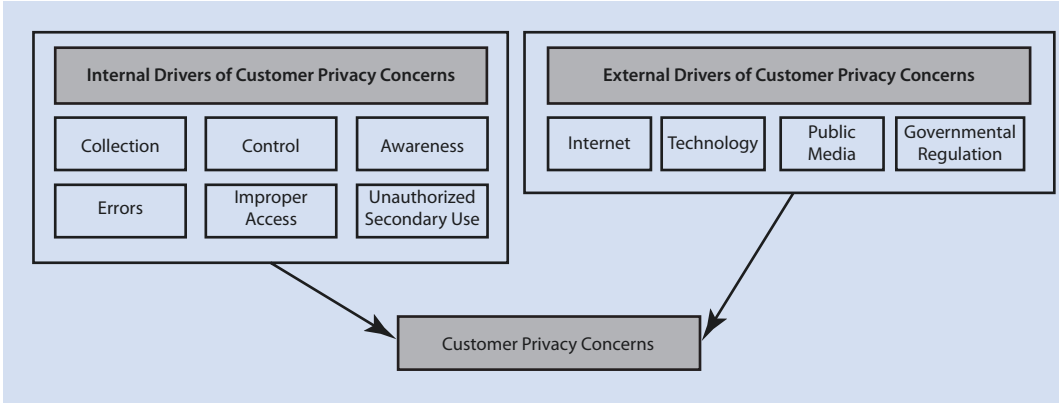


Fig. 14.2 Drivers of customer privacy concerns

ers, the firm must ensure a constant flow of up-to-date information about customers' buying habits and individual needs. However, if customers feel they are losing control over their personal information, they will begin to feel concern about their privacy, which can lead to reluctance to disclose any further personal information. Control also plays a crucial role in the context of advertising effectiveness: The less control customers perceive to have over their private data, the lower is their acceptance of personalized ads such as online display banners (Tucker, 2014). These scenarios create serious obstacles for the efficiency of a company's CRM practices. Thus, it is crucial for companies to know how they can positively influence customers' perceptions of the handling of their personal information to reduce privacy concerns. For this purpose, companies must pay attention to the factors that drive customers' privacy concerns.

14.1.2 Drivers of Customer Privacy Concerns

Customer privacy is one of the most important management practice issues. When customers become concerned about their privacy, CRM processes are especially affected, because they rely on a mutual exchange of information between the customer and the company. In the past 15 years, customers have paid increasing attention to privacy issues as their perceived ability to control access to their personal information has eroded. Goldfarb and Tucker (2012) find that privacy concerns have been increasing for both younger and older consumers, with this increase being more pronounced for the latter group. This development in customers' privacy concerns can be attributed to different internal, company-related factors, as well as several external conditions we present in Fig. 14.2.

Internal Drivers of Customer Privacy Concerns

Customer privacy concerns arise from different sources, such as the way companies collect personal information *(Collection)*, whether a customer can control the uses made of this information *(Control)*, and the clear understanding of the company's conditions and practices with respect to privacy *(Awareness)*. These primary dimensions determine the extent of customers' privacy concerns. Furthermore, customers' privacy concerns can be fostered if they fear that information is not accurate (*Errors*) or is accessible (*Improper Access*) to unauthorized entities. Personal information used for reasons not authorized by the customer also can increase privacy concerns (*Unauthorized Secondary Use*) (Malhotra, Kim, & Agarwal, 2004).

Collection

Collection can be defined as «the degree to which a person is concerned about the amount of individual specific data possessed by others relative to the value of benefits received.» Thus, collection comprises customer concerns about the amount of and the way in which personal information is collected.

Control

Control refers to a person's degree of «control over personal information as manifested by the existence of voice (i.e., approval, modification) or exit (i.e., opt-out)» (Malhotra et al., 2004). Customers' control over their personal data is exercised through approval, modification, or the right to opt-out or opt-in.

Awareness

Awareness indicates an «understanding of established conditions and actual practices» with respect to a company's information collection. Thus, awareness refers to the extent of transparency with which companies communicate the collection and usage of customer data.

Errors

Errors denote concerns that «protections against both deliberate and accidental errors in the data are not adequate» (Harris, Van Hoye, & Lievens, 2003).

Improper Access

Improper access relates to «concerns that data are readily available to parties not authorized to use it» (Harris et al., 2003).

Unauthorized Secondary Use

Unauthorized secondary use refers to «concerns that information collected by the organization for one purpose will be used by the same organization for a different, unauthorized purposes (internal use) or given to another party for other purposes (external use)» (Harris et al., 2003).

CRM at Work 14.1

In practical applications, companies can gain insights into their customers' privacy perception of data handling and CRM practices through a customer survey. For instance, in the context of internet privacy Xu, Dinev, Smith, and Hart (2011) developed and tested a questionnaire to assess perceived privacy concerns, risks, control, and the credibility of the privacy policy implemented by a company. All the items we present here can be measured on seven-point scales anchored by «strongly disagree» and «strongly agree.»

Privacy Concerns

1. I am concerned that the information I submit to this company could be misused.
2. I am concerned that others can find private information about me from this company.
3. I am concerned about providing personal information to this company, because of what others might do with it.
4. I am concerned about providing personal information to this company, because it could be used in a way I did not foresee.

Privacy Risks

1. In general, it would be risky to give personal information to this company.
2. There would be high potential for privacy loss associated with giving personal information to this company.
3. Personal information could be inappropriately used by this company.
4. Providing this company with my personal information would involve many unexpected problems.

Privacy Control

1. I believe I have control over who can get access to my personal information collected by this company.
2. I think I have control over what personal information is released by this company.
3. I believe I have control over how personal information is used by this company.
4. I believe I can control my personal information provided to this company.

Effectiveness of Privacy Policy

1. I feel confident that this company's privacy statements reflect their commitments to protect my personal information.
2. With their privacy statements, I believe that my personal information will be kept private and confidential by this company.
3. I believe that this company's privacy statements are an effective way to demonstrate their commitments to privacy.

External Drivers of Customer Privacy Concerns

Several key external drivers—namely, the Internet, technological advances, public media coverage, and governmental regulations—further foster customers' privacy concerns. These drivers influence one another and ultimately increase customers' concerns about their privacy.

Internet

In 2000, Bill Gates, the founder and chairman of Microsoft Corp., recognized that «In an era where the internet is increasingly central to our lives at work, at home and at school, it is more important than ever that our industry gives customers the assurance that their information will remain secure, respected and private» (Microsoft, 2000).

Customer privacy has always been a significant issue in marketing, but it has gained even more importance with the advent of the Internet. Correspondingly, research has found that customers have grown even more alert to information privacy issues online, compared with those associated with traditional media (Hoffman, Novak, & Peralta, 1999).

The online environment also offers new and different conditions for companies with respect to their data collection and data processing efforts (Rust, Kannan, & Peng, 2002).

- Customer data collection is rendered relatively cheap and easy to execute.
- By means of cost-efficient data-mining processes, companies gain the opportunity to develop customer profiles, behavioral profiles, and insights for targeting and discriminating among their customers.
- The network environment in which the data is collected and coded facilitates the combination of seemingly disparate customer data to create complex profiles of customers.

As a result, customer data can be used efficiently and successfully to build and foster customer relationships. Consider a recent example. The U.S.-based hotel group Denihan Hospitality brought together transactional and customer data, combining it with customer feedback comments and reviews on rating websites to personalize their service. Staff across different hotel chains were equipped with smartphones which helped them anticipate the individual desires of a particular guest regarding meal choices, concierge services, sightseeing trips or whether she is likely to call room service for refreshments in the middle of the night. However, especially in privacy conscious societies such extensive usage and re-combination of information may offset customers, despite its obvious benefits. Therefore, firms need to be particularly sensitive when using online data that has been attained somewhat covertly (Aguirre, Mahr, Grewel, Ruyter, & Wetzels, 2015). Customer privacy concerns are the top reason non-users still avoid the Internet.

In an online setting, there are different ways to gather customer information:

- Customers voluntarily enter personal information, such as their name, address, and credit card number, into databases.
- Information on customers' online behavior is collected using cookies and click-stream technology, which largely require more or less explicit consent («opt-in» or «soft opt-in») by now, depending on legislation.

When browsing the web or making purchases online, customers must provide certain personal information to be able to gain access to content offerings or complete a purchase transaction. Thus, they face a trade-off between the advantages they receive from providing personal information (e.g., name, address, and credit card number) and their fear of the threats associated with sharing such sensitive information. It has even been argued that it is nearly impossible for customers to transact on the Internet without revealing

information about themselves that they might be unwilling to share (Rust et al., 2002). Massive databases continue to record customers' demographics and past purchase activities.

But what raises customer privacy concerns even more is the usage of covertly obtained data, like tracking behavior across different websites or devices (Aguirre et al., 2015). The application of behavioral advertising—personalized advertising messages that are based on customers' prior browsing behavior and online purchasing patterns—serves as an example. Aguirre et al., (2015) show that personalization are beneficial in terms of click-throughs only when customers know which information the company collects. According to Bleier and Eisenbeiss (2015), the effectiveness of personalized advertising is confined by the degree of trust when faced with privacy concerns. A customer survey by the Pew Research Center reveals that 86% of American Internet users take measures to prevent companies from tracking them online (Rainie, 2016). 64% believe the government should do more to regulate advertisers. Yet, the rise of online social media websites, such as Instagram, Twitter, or Facebook, and mobile communication applications like WhatsApp and Snapchat, means that customers voluntarily share personal information, giving advertisers detailed insights into their lives, which the companies then can use for customer segmentation and targeting (Kluth, 2008). Furthermore, concerns about privacy can arise in relation to potential breaches of confidential customer data. In July of 2015, the online adultery site Ashley Madison got hacked and blackmailed, with hackers revealing private data (credit card numbers, account details, contact information, transaction logs) of more than 37 million users in 40 countries publicly on the internet (Bisson, 2015). Later that year, the password-cracking group CynoSure Prime announced to have successfully deciphered 11.2 million Ashley Madison user passwords. In the aftermath of these hacks, website traffic dropped by more than 80%.

In summary, the Internet often represents a threat to privacy and has the potential to undermine a company's marketing performance in the long or even in the short run. Thus, privacy concerns raised by the Internet require a lot more attention by companies and their respective CRM departments.

Technology

Different technological innovations have made it easier for companies to gather, process, and use customer data to gain a competitive advantage, but they also have fostered customers' privacy concerns. The main innovations driving this development are as follows:

- Mobile and smart phones
- Location-based services
- Near-field communication (NFC) and radio frequency identification technology (RFID)

Mobile and smart phones have become steady companions in our daily lives. 95% of the global population have access to a mobile network, over 84% with broadband (3G or higher) internet connectivity (ICT, 2016). As a result, people have become comfortable using smartphones to engage in a variety of activities such as online shopping, news consumption, information sharing via social media, or mobile gaming. Many applications use GPS tracking to offer *location-specific services.*

For example, the mobile dating app Happn shows the user interesting people that they cross paths with. When another Happn user comes within 250 meters, his or her profile pops up. Nintendo's Pokemon Go, the most rapidly diffused mobile app of all time, uses augmented reality to create its unique, locally adapted gaming experience. Beyond creating location-specific customer value, such technological innovations also provide companies with the opportunity to get in touch with customers and offer targeted advertising based on their location, such that the distinction between public and private space seems to be eroding. Customers can no longer depend on the intuitive sense that «If I can see you, you can see me too» but instead feel they are losing control over their personal information. Many applications require access to a large catalog of private information, amongst others the user's calendar, contact list, and GPS tracking data. ▶ Pleaserobme.com collected posts from Twitter that showed that the posters were somewhere other than home; this initiative attempted to draw attention to customers' «oversharing» of personal information. Furthermore, the initiators wanted to inform people about potential risk associated with the use location-based services, such as criminals misusing customer information to rob empty houses (The Economist, 2010). They received notable attention for this effort. Although

people pay increasing attention to data privacy (Goldfarb & Tucker, 2012), these concerns do not seem to hinder the mass adoption of smartphones and intrusive mobile applications.

Another technical innovation, NFC, is increasingly being applied in retail environments and thus fueling customers' privacy concerns. NFC is not limited to enable smartphone payment, as already implemented on a growing scale, but to enhance the con-sumers' shopping experience as well. For example, at the French supermarket chain «Casino», consumers can use their smartphone to find out more about an item or add it to their shopping basket (Techworld, 2013). Stores can thereby track shopping routes and create customer profiles to use during the subsequent shopping trip. This also makes way for personalized couponing and advertising. Technologically different from NFC, but similar in its potential applications, is RFID. This item-tagging technology is reliable and relatively inexpensive, does not require a power supply, and can be attached to nearly any item. When exposed to a radio signal, RFID tags send back information, mostly a long number that identifies the object to which they are attached. In a clothing store, customer choices for try-on can be tracked, creating a profile of their preferred brands, styles, colors. This information can then be used to make recommendations and foster cross- and upselling (Nayak, Padhye, Wang, Chatterjee, & Gupta, 2015).

But this technology implies a risk of jeopardizing customer privacy and reducing or eliminating purchasing anonymity.

Consider some examples of RFID-related threats (Garfinkel, Juels, & Pappu, 2005):

- **Action threat:** By embedding hidden RFID tags into or on objects and documents, companies are able to infer individual behavior, without the knowledge or consent of the individual engaging in the behavior. For example, in 2003 Walmart equipped cosmetic shelves in one of its stores in Broken Arrow, Oklahoma, with RFID technology to track Max Factor Lipfinity lipsticks being removed from shelves. Then Proctor & Gamble researchers used video monitoring to observe customers' behaviors after they picked up the lipstick. This major violation of customer privacy rights without prior consent became publicly known as the Broken Arrow Affair (Hildner, 2006).
- **Association threat:** A customer's identity can be associated with the item's electronic serial number and, with rich data stored in back-end systems (e.g., from a loyalty program), lead to the creation of comprehensive customer profiles that reveal the customers' brand or item preferences in a specific product category. In contrast to the use of loyalty cards, this type of association can be clandestine and even involuntary. Even if item-level information remains generic, identifying items people wear or carry could associate them with particular events or ideas, such as political rallies.
- **Location threat:** If people carry unique tags attached to the items they purchase, they can be located even after they leave the retail store. This possibility also evokes the danger of unauthorized third-party disclosures.

Technological innovations continue to provide companies with opportunities to gain customer information more easily and at a lower cost and thus better serve their customers and improve their customer relationships. Smart fitting rooms are among the latest trends among clothing retailers. RFID tags identify the items that are brought in and transmit their information to interactive mirrors. Here, consumers are shown additional information about the garment at hand, they can request different colors or sizes via touchscreen from shopping assistants, or directly log on to their account and add the item to a virtual shopping basket (Davies, 2015). The mirror can also provide 360-degree views of outfits, give advice about fit and style, and suggest complements and accessories. Nordstrom's, Ralph Lauren, and Bloomingdale's have all tested the technology. However, even such helpful uses of RFID technology can be perceived as intrusive into customers' privacy though and increase concerns about the collection and usage of the obtained information.

Public Media

Public media also play a key role in shaping perceptions of privacy issues. During the past decade, increasing attention in both electronic and print media has focused on privacy issues and actively shaped customers' concerns. Greater media coverage of privacy issues ultimately can increase information privacy concerns. In addition, private consumer groups, such as the Electronic Privacy

Information Center (EPIC), report privacy breaches to popular media, heightening customers' attitudes and concerns about privacy issues. A study of mass media coverage of customer privacy issues between 1990 and 2001 across newspapers, consumer magazines, and trade publications revealed that the number of total articles across all three formats increased by 70%, from 2278 articles in 1990 to 3876 in 2000 (Roznowski, 2003). Other recent research shows that actual media coverage of privacy issues, especially through the increased diffusion of social networks, has grown even more. This growth also reflects new conceptualizations of journalism, exemplified by non-professional authors publishing news on blogs that blur the distinction between independent journalism and other information sources (Peltier, Milne, & Phelps, 2009). In 2013, after the revelations about the NSA's PRISM program by Edward Snowden, up to 240,000 news documents about the affair were published each day on the Internet (Preibusch, 2015). Massive media coverage even continued the following 30 days, with the daily volume of new websites being 18 times higher than before the affair.

Even companies acknowledge the importance of media coverage; Facebook reacted to reports of a customer privacy breach of its social network site only after the problem was prominently covered by *The Wall Street Journal* (The Economist, 2011). Public media in all its forms thus shapes customers' perceptions of information privacy, and newer platforms such as Twitter and social networks can help spread negative news immediately and worldwide, with dramatic potential impacts on companies' bottom lines.

Government Regulation

Government regulation, or the lack thereof, has a powerful impact on customer privacy concerns. A perceived lack of business policy or governmental regulation results in greater privacy concerns (Wirtz, Lwin, & Williams, 2007), and different regulatory approaches to customer privacy, as well as the extent to which governments (mis)use personal information, highlight cross-national differences in privacy concerns. Access to personal information can help governments serve their citizenry better, collect taxes, and enforce laws and regulations. But governments must take a very different position toward personal information than either businesses or individuals. Governments have the power to take and use information without permission; Great Britain maintains a closed-circuit television surveillance system in public and private sectors with around 5 million cameras, over 400,000 in public and independent schools, and extensive government and commercial databases (The Telegraph, 2013). Its police-run DNA database is the largest per capita worldwide. However, with the passing of the Protection of Freedoms Act in 2012, the collection and usage of biometric data was regulated in accordance with rising privacy concerns.

The USA Patriot Act, which introduced legislative changes after the September, 11, 2001, attacks in an attempt to prevent terrorism, serves as another example. The surveillance and investigative powers of law enforcement agencies were significantly increased, and agencies such as the Department of Defense received permission to search telephone, e-mail communications, and the medical, financial, and other records of U.S. citizens without their consent, which in turn stoked significant privacy concerns (EPIC, 2011).

Privacy International, a human rights group established in 1990 to provide information about surveillance and privacy invasions by governments and corporations, recently published a comprehensive report on the surveillance industry along with case studies of government surveillance of its citizens (Privacy International, 2016). It revealed that the U.S. intelligence budget in 2013 totals to approx. $52.6 billion, double that of 2001. Most of it goes to private companies. Figure 14.3 shows the global distribution of surveillance companies, with the majority based in the United States.

With respect to the constitutional protection of privacy, significant differences become apparent even among European countries. Germany traditionally obtains very strict protection and safeguards when it comes to privacy protection, whereas the United Kingdom or the USA give companies and government institutions more freedom in collecting and processing private data, inter alia to counteract terrorism. For example, Privacy International (2015, p. 1) states that UK legislation «does not ensure that interception and access to communications data is carried out in accordance with applicable international human rights standards to respect and protect the right to privacy».

Yet these ratings do not always fully represent customers' concerns about privacy protection in

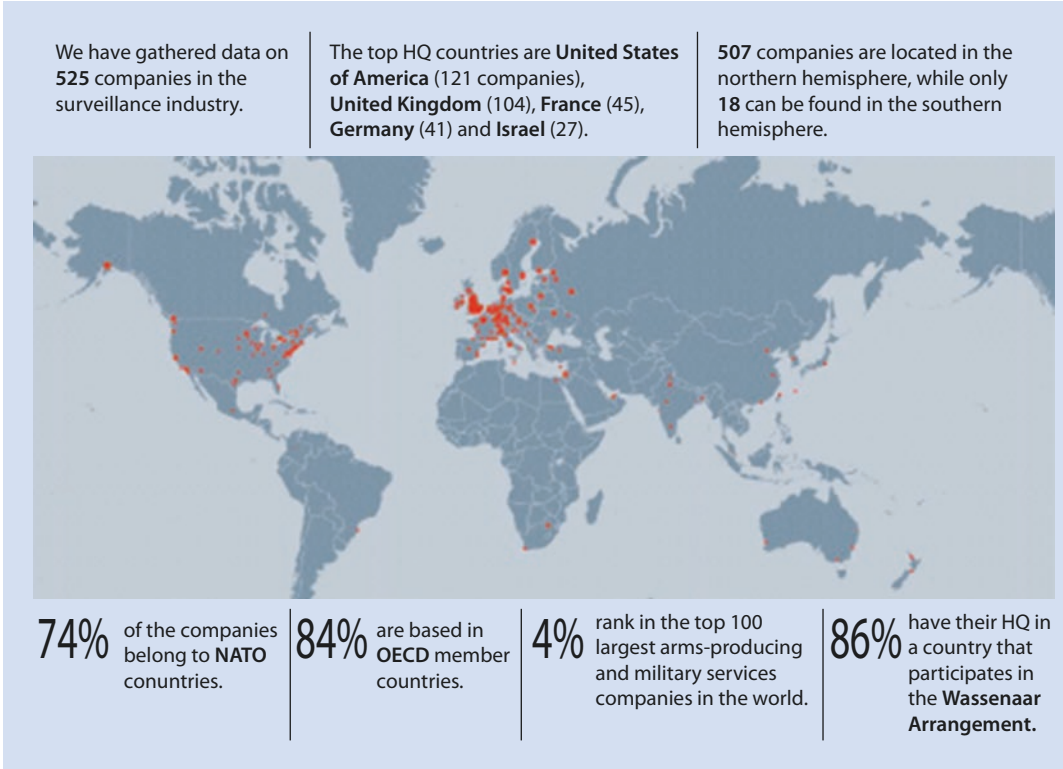


Fig. 14.3 Global distribution of surveillance companies (*Source*: ▶ https://privacyinternational.org)

their home countries. Rather, privacy concerns raised by customers (or the media) in a country can demand legislative actions by the government, leading to improved privacy protections (Roznowski, 2003). Germany, with its very concerned customers and high position in the privacy ranking, serves as a good example.

14.2 Regulations to Protect Customer Privacy

The difference between European and U.S. regulation of customer privacy is well-established: In general, information privacy is protected more under European law than U.S. law (despite differences among EU members). Specifically, customer privacy regulations generally reflect two perspectives: *industry self-regulation* or *government-imposed regulation*. These two approaches summarize the difference between the protection frameworks established by the EU and the United States, as well as the extent to which the respective government controls privacy protection. Whereas the EU has adopted a data protection directive that sets strict privacy standards, U.S. privacy protections tend to be left to self-regulation within industries. These approaches represent the differences in their cultural and societal values and thus their different perceptions of customer privacy. For example, from a German viewpoint, the protection of personal dignity (e.g., image, name, reputation) is threatened primarily by the media, whereas in the U.S. mindset, protection of liberty within one's home is threatened primarily by the government. These differences have their roots in the countries' histories. The German privacy law and protection of personality and position within society have emerged as reactions to fascism and the strictly hierarchical society structures of the seventeenth and eighteenth centuries. In contrast, the United States has embraced the principal of a «limited government,» which idealizes minimal governmental intervention in personal liberty and the economy, ever since the introduction of the Bill of Rights in 1789 (Whitman, 2004). We therefore present both types of protection frameworks using the United States and Germany as representative examples.

14.2.1 United States: Customer Privacy Protection Based on Industry Self-regulation

- **U.S. Constitution:** The U.S. Constitution does not explicitly provide citizens a right to privacy, though a limited constitutional right of privacy has been established, according to several provisions in the Bill of Rights.
- **Robinson list:** The U.S. government has established a Do-Not-Call registry for people to register to avoid receiving telemarketing calls. Registration is free, and telephone numbers placed on the registry will remain there permanently, according to the Do-Not-Call Improvement Act of 2007 (FTC, 2015). Similar approaches also exist for Germany, such as the Robinson list of the German Direct Marketing Association, though they are not government regulated.
- **FTC:** The main agency protecting U.S. customer privacy also handles violations of the Federal Privacy Act of 1974. The Federal Trade Commission (FTC) also has outlined the Fair Information Practices Principles, a series of reports, guidelines, and model codes that represent widely accepted principles concerning fair information practices (FTC, 2000).

Notice and Awareness

Customers should receive notice of an entity's information practices before being requested to provide any personal information. Without notice, a customer cannot make an informed decision about whether and to what extent to disclose personal information. Moreover, three other principles—choice and consent, access and participation, and enforcement and redress—are meaningful only when a customer has notice of an entity's policies and his or her rights thereto.

Choice and Consent

Choice means giving customers options as to how any personal information collected from them will be used. Specifically, choice relates to secondary uses of information, or those beyond the uses necessary to complete the contemplated transaction. Such secondary uses can be internal, such as placing the customer on the company's mailing list to market additional products or promotions, or external, which implies the transfer of the information to third parties.

Access

Customers have the right to view their personal data and to contest that data's accuracy and completeness. The access process must be timely and relatively inexpensive, and incorrect information should be easy to contest, verify, or amend.

Integrity and Security

To ensure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing customer access to data, and destroying untimely data or converting it to anonymous forms. Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.

Enforcement and Redress

Without an enforcement and redress mechanism, even a fair information practice code is merely suggestive; it cannot ensure compliance with core fair information principles. Alternative enforcement approaches include industry self-regulation, legislation that creates private remedies for customers, and/or regulatory schemes enforceable through civil and criminal sanctions. ◘ Appendix 1 gives an overview of recent FTC settlements related to violations of the fair information practice principles.

Furthermore, the FTC has published a report to protect customer privacy in the online environment. Titled «Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers,» this report includes the FTC's recommendation for the «Do Not Track» mechanism that customers can use to opt out of the collection of information about their Internet activity for the development of targeted advertisements, recognizing: «Industry must do better. For every business, privacy should be a basic consideration—similar to keeping track of costs and revenues, or strategic planning» (FTC, 2010). Although the FTC has been successfully enforcing its privacy guidelines in many court cases, it seems not yet to have managed to

set a legal precedent to simplify legal enforcement. But, analysts predict that settlements, like the one reached with Facebook in 2011 as a reaction to a series of privacy violations by the network, could be decisive for inducing change in U.S. privacy practices and strengthening the FTC's position (Gartner, 2011). Thus, the overall extent to which U.S. customers' privacy is protected, in comparison with EU consumers, remains very limited. A lack of governmental legislation and associated privacy concerns push customers to attempt to regain control over their privacy, such as by fabricating false personal information or even refusing to purchase (Wirtz et al., 2007). This development could be fueled further by media publicity; the U.S. government already is dedicating more attention to the topic of customer privacy and is likely to increase governmental regulation. The failure of the Safe Harbor treaty between the United States and the EU and the fast agreement on the successive EU-US Privacy Shield bear witness to this development. Safe Harbor used to allow U.S. firms to save private data of EU citizens signed up for the treaty. However, the European Court of Justice declared Safe Harbor void in 2015, as an indirect consequence of Edward Snowden's revelations about mass surveillance by the American National Security Agency (NSA). In July of 2016, the EU Commission and the USA agreed up-on the EU-US Privacy Shield as its successor. However, criticism of the novel agreement re-mains widespread. Whether additional privacy protection laws and treaties will reduce cus-tomer privacy concerns ultimately depends to a large degree on their enforcement.

14.2.2 Germany: Customer Privacy Protection Based on Governmental Legislation

The German Constitution

Article ten of the Basic Law (as the German Constitution is known) states: «(1) Privacy letters, posts, and telecommunication shall be inviolable. (2) Restrictions may only be ordered pursuant to a statute. Where a restriction serves to protect the free democratic basic order or the existence or security of the Federation, the statute may stipulate that the person affected shall not be informed of such restriction and that recourse to the courts shall be replaced by a review of the case by bodies and auxiliary bodies appointed by Parliament.»

Data Protection Law

Germany has one of the strictest data protection laws in the EU. The general purpose of this act is to protect individual rights to avoid impaired privacy. The act covers the collection, processing, and use of personal data by public federal authorities and state administrations and by private bodies that rely on data processing systems or non-automated filing systems for commercial or professional use. Most federal statutes with any impact on personal information or privacy contain references to the Federal Data Protection Act, if they do not carry special sections on the handling of personal data themselves.

The German Teleservices Data Privacy Act

This Act protects customer privacy online and requires explicit user consent before the usage logs of a session may be stored beyond its duration, usage profiles of different services combined, or user profiles constructed in a non-pseudonymous manner. Websites may not decline service if customers decline to grant approval but instead must abandon these methods or use other legitimate methods in these situations.

Section 7 of the German Unfair Competition Act

Direct marketing issues are addressed by Section 7 of the German Unfair Competition Act. According to its general clause, it is unfair to annoy market players (customers) inappropriately. By default, this rule applies to unwanted advertisements, unsolicited commercial phone calls, marketing methods that use automated calling machines, fax machines or e-mail (spam) received without prior consent, and any direct marketing that cannot be linked to the senders' identity.

Direct marketing via e-mail is not prohibited as spam if:

- The organization has received the e-mail address in the context of selling goods or services to the customer.

- The organization uses the e-mail contact for marketing very similar products and services.
- The customer has not opposed the use of e-mail for further direct marketing.
- At the time of the collection and each usage, the company clearly sets out the right to opt-out from direct marketing via e-mail (Section 7, Paragraph 3, Items 1–4 Unfair Competition Act).
- There is no cold calling, which is a violation of the Unfair Competition Law.

As a member of the EU, Germany also has incorporated Article 8 of the European Convention of Human Rights, which protects «the right to respect for private and family life,» and the new Charter of Fundamental Rights, which contains articles on both «Respect for Private and Family Life» and «Protection of Personal Data,» into its own law (Whitman, 2004). Even despite these comprehensive data protection laws, information privacy remains a vital topic of discussion both for customers and the German government.

Table 14.1 contains an overview of important customer privacy regulation aspects for companies to consider when doing business in the United States or Germany.

14.2.3 The General Data Protection Regulation (GDPR)

In 2016, the European Union adopted its new data protection framework – the General Data Protection Regulation (GDPR). It will replace the current Directive 95/46/EC from 1995, which is still the basis of data protection in the EU today. The GDPR is set out to strengthen data protection for individuals and provide a common set of rules for all member countries by 2018. Unlike the Directive, it will be directly applicable and does not need to be implemented by national legislation.

Among others, the regulation introduces the following major changes:

Rule Harmonization and One-Stop Shop

By making the regulation take effect in all EU member countries at once and without national adaptations, a single set of rules applies across states. Supervisory Authorities (SA) will be established in each country to function as the central point of contact for monitoring compliance, investigating complaints, and imposing sanctions. If companies keep multiple establishments in more than one country, there will be only one responsible SA,

Table 14.1 Customer privacy protections in the U.S. and Germany

	U.S.	Germany
Cold calling Contacting prospective clients or customers with unexpected telephone calls	Allowed (if not on Robinson List)	Forbidden
Unsolicited commercial e-mails Commercial electronic messages, typically sent out in bulk without any prior request or consent given by the consumer	Forbidden	Forbidden
Cross-country data transfer (U.S. to Germany and vice versa) Transfer of customer-related data to a different country than where it has been collected, such as when consumers make online purchases from sellers located in a different country	Allowed	Only allowed with Safe Harbor compliance
Data transfer to third parties (without consent) Provision of personal data to other companies, such as marketing service providers, without notifying the customer	Allowed	Forbidden
Right to opt-out from data collection Upon providing their personal information, customers are able to deny any further use of their data	Not given	Given

namely that of the country in which said company keeps its main establishment. The SAs will be supervised by a central European Data Protection Board (EDPB) (European Commission, 2012).

Expanded Territorial Reach

Data processing and monitoring activities of entities outside the EU fall under the GDPR, if they pertain to EU data subjects. This primarily refers to companies offering goods or services to EU consumers. But it also extends to profiling through website tracking and other monitoring behavior in case users access the website within the EU (Allen & Overy, 2016).

Data Protection Officers

Public authorities and private companies have to, under certain circumstances, appoint a Data Protection Officer (DPO). The DPO is similar to a Compliance Officer, whose presence is already required in larger companies today. However, the DPO's skill set stretches beyond that of a Compliance Officer as he not only needs to be knowledgeable about data protection legislation, but proficient in technical aspects of data security as well (e.g., privacy by design, IT infrastructure, reaction to cyber-attacks). Contrary to the current Directive, DPOs may be assigned to multiple entities (Allen & Overy, 2016).

Profiling

Profiling consumers will be subject to appeal (EU-GDPR, Article 22). Profiling is de-fined as «any form of automated processing of personal data evaluating the personal as-pects relating to a natural person» (EU-GDPR, Recital 71). Examples given by the Recital are automatic refusal of an online credit application or e-recruiting practices without any human intervention. Even if such profiling is lawful, consumers may object this practice (EU-GDPR, Article 21), making it very difficult to be resumed by public or private entities. In case data processing, including profiling, is used for direct marketing purposes, the objection is final and prohibits all subsequent activities under any circumstances.

Privacy by Design and by Default

Data protection measures must be included in the business processes of new products and services, taking into account potential threats to consumer privacy already in the early stage of product development (EU-GDPR, Article 25). Examples for such measures in-clude pseudonymization, data minimization, and IT security.

Furthermore, privacy protection must be implemented by default, setting high standards for data collection and processing, unless explicit consent allows otherwise.

Consent

Consent needs to be explicit for sensitive data (opt-in). If a consumer wants to withdraw her consent, she must be able to do so just as easily as she was able to give consent in the first place (Allen & Overy, 2016). The obligation to prove that consent was given rests with the data controller, i.e., the entity which decides how and why personal data is processed. Also, consent must be given freely. For example, it is generally questionable whether this is the case, if «the performance of a contract is made conditional on the consent to processing data that is not necessary to perform that contract» (Allen & Overy, 2016). Especially many mobile applications may therefore have to change their data collection policies when offering services to EU consumers.

Right to Erasure

Individuals may require the data controller to erase personal data. The request must be answered within one month and realized without inappropriate delay. Further, the data controller has to inform third parties that processed the data (e.g., by making them public) of the request and ask them to delete any links and copies (EU-GDPR, Article 17). The right to erasure was formulated after Google Spain was required to remove links that related to initially lawfully obtained data, which had become inaccurate over time (Court of Justice of the European Union, 2014). Specifically, a Spanish national resident demanded a link to two regional newspapers to be erased, which contained articles about the individual's historical debts. The court ruled that individuals have the right to request the removal of data where it is inaccurate, inadequate, irrelevant or excessive.

Fines

Infringements of the GDPR may yield to drastically increased penalties of up to €20 million or 4% of the annual worldwide turnover (EU-GDPR, 2016). The magnitude of the fine depends, inter alia, on the nature, gravity, and the duration of the

infringement (Allen & Overy, 2016). Article 83 of the GDPR provides two different categories of infringements and corresponding maximum penalties.

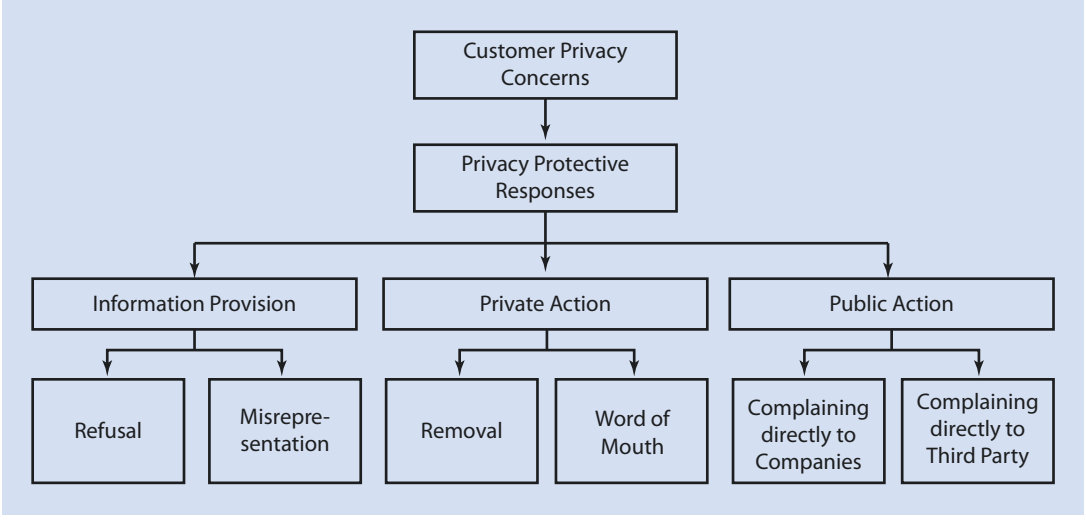
14.3 Customer Privacy Protective Responses

The Symantec (2015) found that 57% of Europeans are worried their data is not safe and 59% of respondents have experienced a data protection issue in the past. Increasing privacy concerns among customers have led to the development of negative attitudes toward CRM practices. The more customers fear that their privacy is endangered, the higher the level of risk they will perceive. Meanwhile, an increase in customers' privacy concerns reduces trust in the company. A high level of risk and a low level of trust in the company together increase customers' intentions to protect their privacy while reducing their willingness to provide any personal information. Furthermore, customers who perceive threats to their privacy respond with defensive actions that may enable them to regain control over their personal information, such as refusing to purchase.

Many of these responses increase costs for marketers and ultimately reduce the effectiveness of CRM initiatives. Furthermore, this defensive demeanor represents a substantial threat to the development of new forms of information-led marketing. Thus, companies must realize the different ramifications of customer privacy concerns. Our proposed taxonomy of privacy protective responses, in ◘ Fig. 14.4, identifies six behavioral responses, classified into three categories: (1) information provision, (2) private action, and (3) public action (Son & Kim, 2008).

14.3.1 Information Provision

If customers are concerned about their information privacy, they sometimes provide falsified personal data (*Misrepresentation*), which threatens the data quality that is so crucial to ensuring efficient CRM (Wirtz et al., 2007). Furthermore, some customers just refuse to give out personal information (*Refusal*). ► Anonymizer.com, a protective online service, blocks attempts to identify ISP domains, browser settings, surfing histories, and e-mail addresses, thus providing customers with a means to hinder companies from collecting online information. Because CRM relies on customer-provided information as a vital source of data, which then enables accurate relationship-fostering efforts and better targeting of prospective customers, such responses constitute major threats to CRM practices.



◘ **Fig. 14.4** Taxonomy of privacy protective responses (*Source*: Based on Son & Kim, 2008 taxono-my)

14.3.2 Private Action

In addition to information disclosure, concerned customers might take private actions such as boycotts of particular retailers, service providers, or products. For example, online information privacy concerns might lead to information boycotts, such that customers remove their personal information from company databases or online communities (*Removal*).

Online customers also might choose to opt-out and explicitly restrict a website from transferring their data to any third party not directly involved in processing the transaction for which the data were collected.

If they perceive a threat to their information privacy, customers often voice negative comments to their friends and relatives (*Negative Word-of-Mouth*). Because a customer's in-group includes like-minded people, companies that are subject to such negative word of mouth lose the chance to recruit new potential customers and bear the potential damage to their reputations.

14.3.3 Public Action

Taking public action is another type of customer response to information privacy concerns: The customer either directly complains to the company (*Complaining Directly to Companies*) or indirectly notifies a third-party organization (*Complaining Indirectly via Third Party*). When customers turn to the company to complain about its handling of their data, the company has the opportunity to respond adequately and even solve the issue, which means it gains a chance to retain customers. If companies do not deal with the complaints adequately though, customers often turn to third-party organizations, such as EPIC and the FTC. In this case, the audience for the complaint is much larger. Unlike private actions, such public actions aim not only to obtain a personal benefit but also to help the general public, because the accused company can no longer violate customers' privacy.

Although customers' privacy protective responses pose a serious constraint on companies' CRM practices, intentions to respond to privacy concerns do not always directly translate into actual behavior—especially when it comes to information disclosure. Many studies have shown that customers often contradict themselves by stating that they would not give out information to a company but then actually do so (KPMG, 2010), the so-called *privacy paradox*.

14.4 Privacy Paradox

«Isn't it strange that 88 percent of the people claim that they are worried about who has access to their data? 86 percent claim that they are getting increasingly more security-conscious about their data. 85 percent expect that governments should impose penalties on companies that misuse data. And in the US some 83 percent of consumers say they would stop doing business with a company entirely if they heard or read that the company misused customer information. At the same time, 845 million people are active on Facebook, every day over 250 million photos are uploaded to the platform. In many countries, over 70 percent of shoppers use loyalty cards. Isn't this a discrepancy?» (Spiekermann, 2012). This evidence uniformly points to the privacy paradox, namely, the discrepancy between people's intentions to protect their own privacy and their actual behaviors in the marketplace. This phenomenon also has been observed in research that demonstrates that people claim they are less willing to provide personal information to marketers than they actually provide when a marketer directly requests such information. This gap appears due to the different perceptions of risk and trust that arise in response to intention measures versus actual disclosure settings (Norberg et al., 2007).

Companies must pay close attention to this discrepancy though, especially with respect to their CRM practices. Specifically, CRM managers need a deep understanding of the link between customers' intentions to disclose information and their actual behaviors, to avoid alienating customers and to align their CRM initiatives appropriately and fairly. They especially need to take into account that even if customers give out their personal information, overly intrusive CRM practices can agitate public media, which likely means damage to the company's image. Furthermore, companies should strive to find ways to increase consumers' willingness to share important information vol-

untarily, such as offering small monetary incentives. Such voluntary sharing of information can enhance the data accuracy and effectiveness of knowledge management systems designed to help organizations interact with customers, as well as maximize the benefits of customer relationships.

14.5 Consequences of Privacy Protective Responses

If customers fear their privacy is being endangered and react with privacy protective responses, several consequences are likely for companies. Especially in the context of CRM practices, companies should be aware of the following potential ramifications (Blattberg, Kim, & Neslin, 2008):

14.5.1 Loss of Trust and Brand Integrity

If breaches of customer privacy become public, customers' privacy concerns increase and lead to a loss of trust in the company. This negative impression can harm a company's brand image and ultimately alter customers' choices and consumption patterns.

14.5.2 Decreased Sales

Goldfarb and Tucker (2011) found that in Europe, where strict privacy laws have been implemented, banner advertising's effectiveness decreased by 65% in terms of stated purchase intention. This is a significant number as the total Internet advertising revenue is forecasted to increase from $135.42 billion in 2014 to $239.87 billion in 2019 globally (PWC, 2016).

14.5.3 Decrease in Data Quality

If customers falsify their personal information or refuse to give out any data, data quality becomes threatened and decreases the effectiveness of CRM practices. Limited access to accurate customer data paints a biased picture of the customer and thus decreases the precision of predictive models and targeting initiatives (Wirtz et al., 2007).

14.5.4 Increased Costs due to Privacy Protection

Compliance with stricter privacy rules is estimated to increase the total costs of catalog or online apparel retailers by 3.5–11% (Turner, 2001). This cost applies especially in the United States; the EU privacy protection framework is already very strict.

14.5.5 Ethical Dilemma

Collecting data that consumers do not want to be collected places managers in an ethical dilemma. Do they ignore customers' wishes to protect their privacy, and thus increase their chances of economic success, but also run the risk of alienating their most valuable assets?

In summary, privacy concerns pose a real threat to companies practicing CRM. Negligence leads to decreased sales and lower efficiency for their predictive modeling. Moreover, compliance and litigation costs can reduce profitability. Thus companies must carefully balance the benefits of obtaining additional customer information, such as more accurate targeting of their offerings and marketing communications, against the increasing concerns of customer privacy, which can lead to disloyalty and customer churn.

14.6 Implications for Companies

This discussion of customer privacy concerns and their implications reveals that customer privacy is an important topic for companies, to be considered especially in the context of CRM. Consequently, CRM mangers and marketers constantly look for appropriate ways to react to or even prevent customers' privacy concerns. Using a checklist adapted from Harriet Pearson, vice president, security council, and chief privacy officer at IBM, we seek to provide insights into where companies must consider privacy issues, what legal requirements they must take into account, and how they can achieve the successful implementation of responsible privacy protection practices in a CRM context (Pearson, 2007).

14.6.1 Align Privacy with Strategy

Privacy concerns can translate into negative brand images and harm a company's valuable assets. It is thus especially important for businesses with very valuable brands or that compete in information-intensive industries (e.g., health care, finance, high-tech) to take the lead when it comes to privacy and data protection.

14.6.2 Look Beyond Rules to Values

Trust perceptions of a company and its CRM practices generally are determined through direct customer–employee contacts. Embedding privacy and security values into corporate cultures thus will yield greater returns than even the most comprehensive set of rules. When values are developed from the bottom up, they tend to be lived, not just recited.

14.6.3 Anticipate Issues

It should be someone's job to scan for products or practices, within the business or across the industry, that raise legitimate privacy concerns, and then collaborate with stakeholders to develop reasonable solutions. Firms must be prepared to work across the industry as well as internally. Furthermore, they should think about implementing a third-party certification, such as TRUSTe or the Better Business Bureau, to obtain recognizable privacy seals and thereby signal high privacy standards to customers.

14.6.4 Create Accountability

The role of a privacy or security officer is to unite and coordinate efforts across functional silos. All those involved in setting and implementing information policies—the head of human resources, the chief information officer, and the marketing vice president, for example—should participate, but there also must be a single person who is responsible and accountable for privacy efforts.

14.6.5 Do Not Conflate Security and Privacy

Getting privacy right in a business context means meeting societal or regulatory expectations for what type of information is collected, how much, with whom it may be shared, how it will be used and protected, and how long it is retained. Resist the temptation to focus solely on data security; firms must be aware of the different legal requirements in different countries in which they operate.

14.6.6 Treat Privacy as a Social Responsibility

In globally connected, information-rich societies, privacy and data protection belong on the corporate citizenship agenda, right alongside the environment, diversity, and other important issues.

14.6.7 Manage Your Data Supply Chain

Data handling obligations flow with data that cross corporate or national boundaries. Business ecosystems that include global sources of talent and services need standards for data management that can rationalize an international patchwork of expectations and regulations.

14.6.8 Rely on Technology When Appropriate

They cannot substitute for leadership, common sense, and good policies, but simple tools (e.g., automated checklists, encryption, audit logs) can do wonders to enable compliance. And emerging capabilities, such as face masking in digital surveillance systems or privacy-preserving data mining, can help resolve conflicts between information use and privacy.

14.6.9 Plan for Disaster Recovery

No information system is fail-safe. In case of a data loss or breach, a rehearsed response should be in place to address technical, individual, legal, and other needs.

14.6.10 Heed both Boomers and Millennials

The under-25 crowd is not dismissive of privacy, but it embraces online, collaborative work and play

CRM at Work 14.2

Problem
Though consumers worry about how their personal data is gathered and used, they're surprisingly ignorant of what data they reveal when they're online, and most companies opt not to enlighten them. This dynamic erodes trust in firms and customers' willingness to share information.

Solution
Companies need to design products and services with transparency and data pri-vacy in mind. They must provide customers with appropriate value in exchange for data, educate them about how it is collected, and allow them to have control over it.

Best Practice
Disney devised electronic wristbands that give park visitors access to attractions and hotel rooms and allow them to charge food. Disney uses the bands to collect data on customers but clearly spells out its practices and privacy policies. The tradeoffs are transparent to the customers, who find the convenience and other benefits the bands offer worthwhile.
Source: Morey, Forbath, and Schoop (2015), p. 99.

far more than earlier generations. Privacy thinking should span generational norms and expectations. One employee may freely post pictures and personal information online but recoil from having an employer or the government collect a biometric identifier; another may prefer just the opposite.

14.7 Future Issues: Data as Currency

In 2009, Meglena Kuneva (European Consumer Commissioner) already stated that «Personal data is the new oil of the Internet and the new currency of the digital world» (World Economic Forum, 2011, p. 5). A vast variety of different types of personal data exist, such as web searches and sites visited, purchase histories, likes, tweets, real-world location coordinates, or tracked health-related data. This personal data creates economic and societal value. For example, companies can use personal data of their customers to develop customized products and services and thus monetize these data (World Economic Forum, 2011). Not only companies understand the value of personal data, but also consumers increasingly recognize their huge value. By now, they are less willing to give companies their sensitive data for free and start taking advantage of their worth (Datafloq, 2016). The number of consumers stating that their personal data are a useful tool to negotiate better deals from companies increased from 40% in 2012 to 52% in 2015. The majority of consumers expects stronger incentives with increasing sensitivity of personal data. Consumers are most likely to share their data for direct incentives that pad their wallets or pockets, such as direct financial rewards, free products or services, or discounts (Direct Marketing Association, 2015). For example, Google's Screenwise Trends panel pays up to $8 to consumers who are willing to share data on their browsing behavior with Google and its partners. Raptr, another example that refers to an application with nearly 26 million users, provides its users with free games, hardware or discounts in exchange for data on their video gaming habits (Datafloq, 2016).

As both parties—data providers and data users—might monetarize personal data, provision of these data can represent a win-win situation. However, despite the increasing amount of data generated daily by consumers and the growing sentiment to regard this personal data as a currency, research on why and when consumers exchange personal infor-mation for incentives and how companies determine those incentives is scarce. Therefore, in ◘ Fig. 14.5 we provide a brief research agenda that provides fruitful ideas for future analyses. Distinguishing between a data provider and data user perspective, these ideas are interrelated.

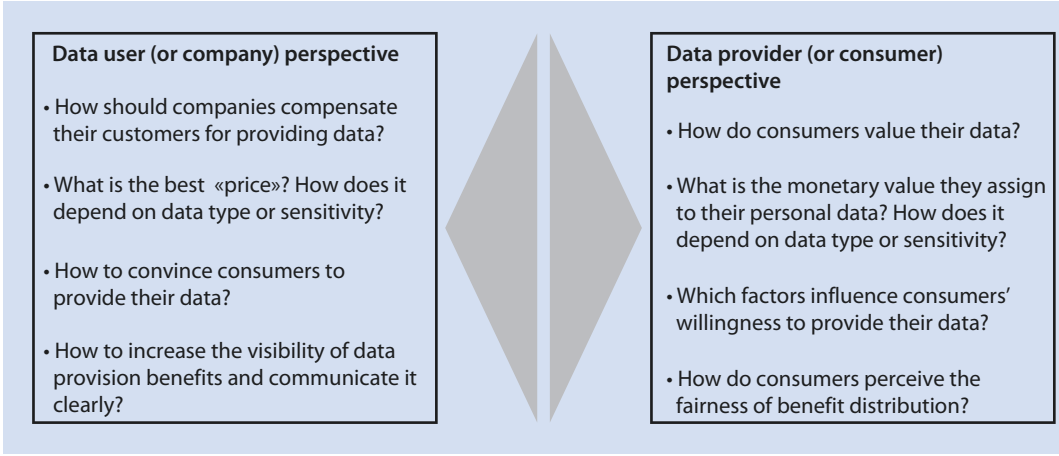


Fig. 14.5 Future research agenda on «data as currency» from a data provider and data user perspective

Summary

In the present chapter, we discuss the central role of customer privacy concerns in CRM practices. For this purpose, we firstly introduce and define customer privacy in the context of CRM. Thereafter, we identify drivers of customer privacy concerns, both internal and external. Internal drivers hereby advert to company-related operations which evoke customers' fears about the disclosure and handling of their personal information. In this context, the way companies collect personal information *(Collection)*, whether a customer can control the uses made of this information *(Control)*, and the clear understanding of the company's conditions and practices with respect to privacy *(Awareness)* are especially recognizable. In a next step, we identify external drivers which foster customers' privacy concerns, namely Internet, technological advances, public media coverage as well as governmental regulations. We find that the rise of the Web 2.0 and online social networks provides customers with various possibilities to share personal information, thereby opening doors for companies to collect openly available data about customers. But in this context especially companies' data collection without customers' consent fosters privacy concerns thus posing a risk for efficient CRM practices. Additionally, technological advances, such as RFID technology and location-based services, as well as the coverage of this topic in public media add to customers' increasing fear of losing control over their personal data. Different privacy regulatory frameworks in different countries also affect customers' privacy concerns. Thus in the following, we compare the regulatory frameworks of both the EU and the U.S. We find privacy protection in the U.S. to be mainly industry self-regulated. One central role is hereby occupied by the Federal Trade Commission (FTC) which protects customer privacy in the U.S. and handles violations of the Federal Privacy Act. On the other hand, Germany as a member of the EU protects customers' privacy by means of different governmental laws and regulations. This has implications for companies such that in Germany it is not allowed to contact customers via telephone (Cold Calling) or email (Unsolicited Emails) without their prior consent. For multinational companies operating in the U.S. and the EU, it is especially difficult to comply with the requirements of privacy protective frameworks in different markets. CRM managers have to be aware of customers' privacy concerns and the respective protective responses they might face. In this regard, we identify three categories of customers' reactions to privacy concerns, namely the refusal or misrepresentation of information (Information Provision), the removal from the respective company or the spreading of

negative word-of-mouth (Private Action) as well as complaining to either the company itself or a third party (Public Action). Although customers' privacy protective responses pose a serious constraint on companies' CRM practices, intentions to respond to privacy concerns do not always directly translate into actual behavior—especially when it comes to information disclosure. We also discuss this phenomenon, the so-called privacy paradox. In a concluding step, we list potential ramifications for companies of customers' privacy concerns in the context of CRM and give advice on how responsible privacy protection practices can be implemented in a company. Finally, we propose some avenues for further research in the context of data valuation from the firm and consumer perspective.

International Perspectives: Did You Know?

1. Although the EU applies a strict privacy regime and often is a thought leader in protecting its citizens' personal information, Asian governments are also tightening the thumb screws on company practices: Japan, for instance, has just amended its data privacy law «APPI», which now poses theft or transfer of personal information as a federal crime. Companies or even single employees may be charged with up to one year in prison or a fine of 500,000 yen. South Korea, which already has one of the strictest privacy laws worldwide, also amended their legislation in 2016, increasing fines for data breaches and requiring consent by the information subject to transfer data abroad (Global Legal Group, 2016; Sidley, 2016).
2. In a survey among almost 10,000 corporate executives from 115 countries it was reported that, on average, each organization faces 10 incidents endangering computer security every day. That is an increase of almost 50% reported two years earlier and a major threat to private customer data. Most incidents are related to global cybercrime by individual professionals or competitors (PWC, 2014). The average cost of a data breach has risen to $3.8 million in 2015 (IBM, 2016).
3. The biggest threat to consumer privacy today is the rise of the Internet of Things (IoT). According to Gartner Research, the IoT will consist of 26 billion units by 2020, sending and receiving a multiple of the data generated by people today. Security professional Josh Corman has started a movement named «I Am the Cavalry», which serves as a sharing platform for vulnerability research in the areas of medical devices, automobiles, home services and public infrastructure. Researchers and hackers can share their discoveries to make products more secure. Tesla Motors has been operating a program with a similar goal: it has given away rewards for individuals uncovering security issues in their software to make their vehicles safer. As formerly integral products increasingly rely on software components, steps to prevent unauthorized access to the code will become crucial not only for consumer privacy but also product safety (Gartner, 2014).

Exercise Questions

1. Please explain the role of public media as a driver of customers' privacy concerns.
2. The U.S. and Germany reflect two different perspectives of customer privacy regulation. Please state and describe both perspectives and explain their historical and cultural origin.
3. Imagine you are the manager of a U.S. company selling apparel over the Internet. What are the main privacy regulations to be kept in mind when selling to a German customer?
4. Please give examples for customers' privacy protective responses and explain the potential consequences for companies.
5. Please explain the phenomenon of the privacy paradox.
6. What is meant by «data as currency»? Where does such a development lead in the long-run? What effect does this have on data privacy and transparency of data collection and usage practices?

Appendix 1: Selected settlements in violation of FIP principles (Peltier et al., 2009)

FIP	Company/settlement date	Case
Notice/awareness	Centurion Financial Benefits (2007)	Consumers were told they were providing information for a $2000 credit card limit. Instead, they received an application for a scored value/cash card with no line of credit
	Sony BMG (2005)	Sent flawed and overreaching computer program via millions of music CDs that was officially intended to restrict the consumers' use of the music. The program also could report listening habits and installed undisclosed and sometimes hidden files on computers that could expose users to tampering by third parties
	DoubleClick (2002)	Violated state and federal laws by surreptitiously tracking and collecting consumers' personally identifiable data and combining it with information on their web surfing habits
Choice/consent	Bank of America (2007)	Disclosed consumers' personal, private, and confidential information to third parties without consent
	Gateway Learning Corporation (2004)	Rented personal information, in violation of promises made in its privacy policy statement. After collecting consumers' information, privacy policies were changed to allow sharing of information without prior notice or consent given by customers
	Cartmanager International (2005)	The FTC alleged that CartManager did not adequately inform consumers or merchants that it would collect and rent information and that the company acted knowing that it was contrary to the privacy policies of many merchants
Access	Quicken Loans (2002)	Failed to provide «adverse action» notices in violation of the Fair Credit Reporting Act and failed to comply with the provisions of the Act to notify the consumers when an action was based wholly or partly on their credit report
	Performance Capital Management (2001)	Provided credit bureaus with inaccurate «delinquency dates» for its accounts, resulting in negative information remaining on consumers' credit reports. PCM failed to investigate consumer disputes referred by credit bureaus or notify bureaus when consumers disputed collection accounts
Integrity/security	Guidance Software (2006)	The FTC charged that failure to take reasonable security measures to protect sensitive customer data contradicted security promises made on the website. This failure allowed hackers to access sensitive credit card information for thousands of consumers
	ChoicePoint Inc. (2006)	Failure to take appropriate security measures to protect sensitive information of tens of millions of customers resulted in fraudulent purchases worth millions of dollars
	Microsoft Corp. (2007)	The FTC alleged that Microsoft did not employ reasonable and appropriate measures to maintain and protect the privacy and confidentiality of consumers' personal information collected through its Passport and Passport Wallet service, including credit card numbers and billing information

Supplemental readings on customer privacy

European Union

- ▶ http://ec.europa.eu/justice/policies/privacy/index_en.htm
- ▶ www.privacyinternational.org

United States

- ▶ www.ftc.com
- ▶ http://www.export.gov/safeharbor/
- ▶ https://www.donotcall.gov/

Germany

- ▶ http://www.bfdi.bund.de/EN/Home/homepage_node.html
- ▶ http://www.robinsonliste.de/

Research/Reports

- ▶ http://blogs.wsj.com/wtk-mobile/
- ▶ http://www.digitalcenter.org/

References

Aguirre, E., Mahr, D., Grewel, D., Ruyter, K. D., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing, 91*(1), 34–59.

Allen, & Overy. (2016). *The EU general data protection regulation*. http://www.allenovery.com/SiteCollectionDocuments/RadicalchangestoEuropeandataprotectionlegislation.pdf. Accessed October 14, 2016.

Bisson, D. (2015). *The Ashley Madison hack—A timeline*. http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-ashley-madison-hack-a-timeline. Accessed October 10, 2016.

Blattberg, R. C., Kim, B. D., & Neslin, S. A. (2008). *Database marketing: Analyzing and managing customers*. New York: Springer.

Bleier, A., & Eisenbeiss, M. (2015). The importance of trust for personalized online advertising. *Journal of Retailing, 91*(3), 390–409.

Court of Justice of the European Union. (2014). *An internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties*. https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf. Accesed February 7, 2018.

Datafloq. (2016). *From data ownership to data usage: How consumers will monetize their personal data*. https://datafloq.com/read/data-ownership-data-usage-consumers-monetize-data/68. Accessed November 17, 2016.

Davies, S. (2015). *The smart fitting room is the future of retail*. http://tech.co/smart-fitting-room-future-retail-2015-12. Accessed October 10, 2016.

Direct Marketing Association. (2015). *Data privacy: What the consumer really thinks*. https://dma.org.uk/uploads/ckeditor/Data-privacy-2015-what-consumers-really-thinks_final.pdf. Accessed November 17, 2016.

EPIC. (2011). *US Patriot Act*. http://epic.org/privacy/terrorism/usapatriot/#introduction. Accessed September 29, 2011.

European Commission. (2012). *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. Accessed October 10, 2016.

EU-GDPR. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679. Accessed October 14, 2016.

FTC. (2000). *Privacy online: Fair information practices in the electronic marketplace*. http://www.ftc.gov/reports/privacy2000/privacy2000.pdf. Accessed September 29, 2011.

FTC. (2010). *Protecting consumer privacy in an era of rapid change—A proposed framework for businesses and policymakers*. http://www.ftc.gov/os/2010/12/101201privacyreport.pdf. Accessed September 29, 2011.

FTC. (2015). *National do not call registry*. https://www.consumer.ftc.gov/articles/0108-national-do-not-call-registry#reregister. Accessed October 10, 2016.

Garfinkel, S. L., Juels, A., & Pappu, R. (2005). RFID privacy: An overview of problems and proposed solutions. *IEEE Privacy & Security, 3*(3), 34–43.

Gartner. (2011). *Google-FTC settlement may have important privacy implications*. http://www.gartner.com/DisplayDocument?id=1620221. Accessed September 29, 2011.

Gartner. (2014). *Gartner Says the Internet of Things Will Transform the Data Center*. http://www.gartner.com/newsroom/id/2684915. Accessed April 10, 2017.

GBG. (2015). *Data distrust pits consumers against business*. www.thetrusteconomy.com/news/. Accessed October 10, 2016.

Global Legal Group. (2016). *The International Comparative Legal Guide to: Data Protection 2016*. https://iclg.com/practice-areas/data-protection/data-protection-2016. Accessed April 10, 2017.

Goldfarb, A., & Tucker, C. E. (2011). Privacy regulation and online advertising. *Management Science, 57*(1), 57–71.

Goldfarb, A., & Tucker, C. E. (2012). Shifts in privacy concerns. *American Economic Review: Papers & Proceedings, 102*(3), 349–353.

Harris, M. H., Van Hoye, G., & Lievens, F. (2003). Privacy and attitudes towards internet based selection systems: A cross cultural comparison. *International Journal of Selection and Assessment, 11*(2–3), 230–236.

Hildner, L. (2006). Defusing the threat of RFID: Protecting consumer privacy through technology-specific leg-

islation at the state level. *Harvard Civil Rights-Civil Liberties Law Review, 41*(1), 133–176.

Hoffman, D. L., Novak, T. P., & Peralta, M. A. (1999). Building consumer trust in online environments: The case for information privacy. *Communications of the ACM, 42*(4), 80–85.

IBM. (2016). *2016 Ponemon cost of data breach study*. https://www.ibm.com/security/data-breach/. Accessed May 11, 2017.

ICT. (2016). *ICT facts and figures 2016*. http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf. Accessed October 10, 2016.

Kluth, A. (2008). The perils of sharing. *The Economist*. http://www.economist.com/node/12499877. Accessed February 7, 2018.

KPMG. (2010). *Consumers & convergence IV*. http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/consumers-and-convergence/Documents/Consumers-Convergence-IV-july-2010.pdf. Accessed September 29, 2011.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355.

Martin, K. D., & Murphy, P. E. (2016). The role of data privacy in marketing. *Journal of the Academy of Marketing Science, forthcoming*.

Microsoft. (2000). *Bill Gates opens SafeNet 2000 summit*. http://www.microsoft.com/Presspass/press/2000/dec00/safenetpr.mspx. Accessed September 29, 2011.

Morey, T., Forbath, T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard Business Review, 93*(5), 96–105.

Nayak, R., Padhye, R., Wang, L., Chatterjee, K., & Gupta, S. (2015). The role of mass customisation in the apparel industry. *International Journal of Fashion Design, Technology and Education, 8*(2), 162–172.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126.

Pearson, H. (2007). Privacy checklist for business. *Harvard Business Review, 86*(10), 123–130.

Peltier, J. W., Milne, G. R., & Phelps, J. E. (2009). Information privacy research: Framework for integrating multiple publics, information channels, and responses. *Journal of Interactive Marketing, 23*(2), 191–205.

Preibusch, S. (2015). Privacy behaviors after Snowden. *Communications of the ACM, 58*(5), 48–55.

Privacy International. (2016). *The global surveillance industry*. https://www.privacyinternational.org/node/911. Accessed October 10, 2016.

Privacy International. (2015). *The right to privacy in the United Kingdom*. https://www.privacyinternational.org/sites/default/files/PI%20submission%20UK.pdf. Accessed October 10, 2016.

PWC. (2016). *Internet advertising. Key insights at a glance*. https://www.pwc.com/gx/en/global-entertainment-media-outlook/assets/2015/internet-advertising-key-insights-1-advertising-segment.pdf. Accessed October 13, 2016.

PWC. (2014). *Defending yesterday. Key findings from The Global State of Information Security Survey 2014*. http://www.pwc.com/gx/en/consulting-services/information-security-survey/pwc-gsiss-2014-key-findings-report.pdf. Accessed May 11, 2017.

Rainie, L. (2016). *The state of privacy in post-Snowden America*. http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/, Pew Research Center. Accessed October 10, 2016.

Roznowski, J. L. (2003). A content analysis of mass media stories surrounding the consumer privacy issue 1990–2001. *Journal of Interactive Marketing, 17*(2), 52–69.

Rust, R. T., Kannan, P. K., & Peng, N. (2002). The customer economics of internet privacy. *Journal of the Academy of Marketing Science, 30*(4), 455–464.

Sidley. (2016). *South Korea Enacts Stricter Penalties for Data Protection Violations by Telecommunications and Online Services Providers*. http://datamatters.sidley.com/south-korea-enacts-stricter-penalties-for-data-protection-violations-by-telecommunications-and-online-services-providers/. Accessed April 10, 2017.

Son, J. Y., & Kim, S. S. (2008). Internet Users' information privacy-protective responses: A taxonomy and nomological model. *MIS Quarterly, 32*(3), 503–529.

Spiekermann, S. (2012). *The privacy paradox*. http://derstandard.at/1330390059705/The-Privacy-Paradox. Accessed October 10, 2016.

Statista. (2016). *Market capitalization of the largest U.S. internet companies as of March 2016 (in billion U.S. dollars)*. https://www.statista.com/statistics/209331/largest-us-internet-companies-by-market-cap. Accessed October 14, 2016.

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology, 68*(3), 459–468.

Symantec. (2015). *State of privacy report*. https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf. Accessed October 11, 2016.

Techworld. (2013). *How NFC is transforming the weekly shopping experience*. http://www.techworld.com/mobile/how-nfc-is-transforming-weekly-shopping-experience-3438410. Accessed October 10, 2016.

The Economist. (2010). Location-based services on mobile phones—Follow me. *The Economist*. http://www.economist.com/node/15612291. Accessed February 7, 2018.

The Economist. (2011). Anonymous no more. *The Economist*. http://www.economist.com/node/18304046. Accessed February 7, 2018.

The Telegraph. (2013). *One surveillance camera for every 11 people in Britain, says CCTV survey*. http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html. Accessed October 10, 2016.

Tucker, K. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research, 51*(5), 546–562.

Turner, M. A. (2001). The impact of data restrictions on consumer distance shopping. *Direct Marketing Association*. http://www.the-dma.org/isec/9.pdf. Accessed September 28, 2011.

Whitman, J. Q. (2004). The Two western cultures of privacy: Dignity versus liberty. *Yale Law Journal, 113*(6), 1151–1221.

Wirtz, J., & Lwin, M. O. (2009). Regulatory focus theory, trust, and privacy concerns. *Journal of Service Research, 12*(2), 190–207.

Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management, 18*(4), 326–348.

World Economic Forum. (2011). *Personal data: The emergence of a new asset class*. http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf. Accessed November 17, 2016.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association of Information Systems, 12*(12), 798–824.