Chapter 4
Customer Privacy and Database Marketing

Abstract Probably the single most important aspect of the legal environment pertaining to database marketing is customer privacy. We examine this issue in depth. Privacy is a multidimensional issue for customers, and we begin by reviewing the nature and potential consequences of these several dimensions. We discuss the evidence regarding the impact of customers' concerns for privacy on their behavior – there is some although not definitive evidence for example that privacy concerns hinder e-commerce. We discuss current firm practices regarding privacy, as well as some of the major laws regarding customer privacy. We conclude with a review of potential solutions to privacy concerns, including regulation, permission-based marketing, and a strategic focus on trust.

4.1 Background

4.1.1 Customer Privacy Concerns and Their Consequences for Database Marketers

Customer privacy in database marketing pertains to the *customer's ability to control the collection, usage, and anonymity of his or her data*. The basic premise of database marketing is exchange: companies collect and analyze customer data, and in return provide customers with more appropriate products, services, and offers. However, this premise is muddled when customers become concerned about privacy. Figure 4.1 outlines these concerns and their ramifications.[1]

[1] See Smith et al's (1996) and Stewart and Segars (2002) for a formally developed measurement instrument of privacy concerns – the "Concern for Information Privacy" (CFIP) scale. This scale taps the security, third-party access, none-of-your-business, and fear of errors dimensions of information privacy discussed in this section.

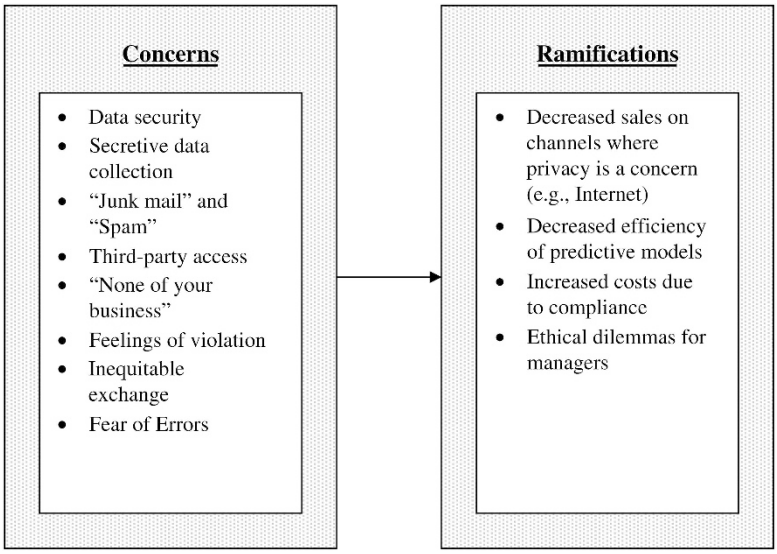

Fig. 4.1 Customers' privacy concerns and their ramifications for database marketers.

- *Data security*: Customers fear that computer hackers can gain access to their data. High-profile cases of "identity theft" fuel this fear. In one instance, ChoicePoint, a collector and seller of customer-level data available in the public domain, revealed that an identity-theft ring gained access to 145,000 records in its database (Perez 2005). The data included names, addresses, and social security numbers. Another well-known data company, Lexis-Nexis, revealed that criminals gained access to social security numbers, driver's license information, and addresses of 310,000 individuals (Timmons and Zeller Jr. 2005). These cases suggest to consumers that even if the companies collecting the data are well-meaning, these companies cannot protect the privacy of their data.

  Data security also pertains to access by persons within the organization. For example, a patient might be comfortable with a physician seeing his or her medical history, but not a medical student or a departmental administrator.
- *Secretive data collection* (George 2002): Customers suspect that companies collect data from them without their knowledge. The most conspicuous example is the use of cookies, a few lines of computer code inserted by an Internet website into the customer's computer that can then be used to track the customer over time (Turner and Dasgupta 2003). Cookies are usually inserted without the customer's permission. It is not the tracking *per se* that bothers customers, but the surreptitious nature of the data collection.
- *Junk mail and spam* (George 2002): Some customers fear that data collection leads to unwanted junk mail and emails. Good predictive models

should address this concern, as companies use these models only to target customers who will respond. But the best predictive models might boost a 1% response rate up to a 5–7% response rate. That can mean huge profits for the database marketers (Chapter 10), but the 93% who do not respond might view the solicitations as an invasion of privacy.

- *Third-party access* (Smith et al's 1996; Turner and Dasgupta 2003; George 2002): Customers realize that the company with whom they do business may sell the data it collects to unknown third parties euphemistically called "partners." Customers may not mind the company that collects the data using it, but want to control who else gets to use the data.
- *None of your business* (Smith et al's 1996; George 2002; Winer 2001): The customer may simply feel that it is none of the company's business to know what types of books, movies, electronic equipment, etc., that the customer prefers, or what areas of the country (or what countries) the customer calls on the telephone. These customers view their relationship with the company as purely transactional, and resent being classified as "mystery book readers" or "international callers".
- *Feelings of violation* (Winer 2001): Winer (2001) states this as, "How do they know that about me?" For example, a direct marketer may use a compiled database (Chapter 8) to learn that a customer reads *Newsweek* and recently purchased a high definition television. Even if the customer knows data are being collected and databases are being merged, when the company reveals what it knows to the customer, the overall data collection effort seems more invasive.
- *Inequitable exchange* (Fletcher 2003): While the premise of database marketing is for the customer to sacrifice some privacy in exchange for better service, prices, product, etc., some customers may not view this as an equitable exchange. Either they don't see the benefits of better targeting, or they view the costs of sacrificing privacy as too high. Either way, they view the database marketing exchange equation as an inequality, not favorably in their direction.
- *Fear of Errors* (Smith et al's 1996): Customers may fear that the data collected on them may include errors. The errors could occur through computer "glitches" or human mistakes. The end result is that the company may have an incorrect profile of the customer, without either the firm or the customer knowing it.

As Fig. 4.1 shows, there are four key ramifications of these privacy concerns. First, customer fears about privacy can decrease sales volume. Stewart and Segars (2002) found that consumers who were concerned with privacy intended to remove their names from mailing lists or were less likely to purchase products simply because of the manner in which the company used personal data. The issue is especially relevant for the Internet. Udo (2001) surveyed 158 online users and found that privacy and security concerns were the number one issue hampering more purchasing on the Internet. A Microsoft "Presspass" (Microsoft 2000) suggested, based on a Forrester Research study,

that customer privacy concerns decreased Internet sales by $12.2 billion in 2000.

Second, privacy concerns may limit the data available to companies, therefore decreasing the precision and profitability of predictive modeling. Stewart and Segars (2002) found that consumers who were concerned with privacy were more likely to refuse to give information to companies. For existing customers, purchase history is typically the most important variable driving predictive model accuracy (e.g., Knott et al. 2002), and companies automatically collect those data. However, when acquiring new customers, the prospect has no purchase history with the company, so demographic and other customer characteristic data become very important. If cookies were outlawed, companies would not be able to track customers' Internet search preferences and behaviors – variables that are becoming important in predictive models. In the extreme, if companies were prohibited from using prior purchase histories to tailor campaigns, predictive modeling would virtually be brought to a standstill.

Third, privacy can increase costs. Turner (2001) notes that restrictions on access to external customer data could increase costs by 3.5–11%. This diminishes the efficiency of database marketing.

Fourth, managers may face difficult ethical questions if they find themselves collecting data the customer doesn't want them to collect. A good test of ethical behavior is, "Would I be embarrassed if the public knew my actions?" In the case of collecting and utilizing data that customers would prefer to remain private, the answer to that question may be "yes." This puts well-meaning managers in an ethical dilemma.

In summary, consumers have several concerns about privacy. The ramifications of these concerns are: (1) lower customer expenditures especially on the Internet, (2) less data available for predictive models, (3) higher costs for companies complying with various privacy rules, and (4) difficult ethical concerns for managers.

4.1.2 Historical Perspective

Concerns about customer privacy are not new. They probably emerged when customer data were first punched onto computer cards in the 1960s. One of the first uses of customer data was in the financial sector, where decisions needed to be made about customer credit-worthiness. Concerns about privacy led to the Fair Credit Reporting Act of 1970 and the Privacy Act of 1974, which delineated consumers' rights with regard to credit information (Turner and Dasgupta 2003). As technological sophistication increased and firms began to match and merge files and communicate information seamlessly, more legislation was passed – the Electronic Communications Privacy Act of 1986 and the Computer Matching and Privacy Protection Act of 1988 (Turner and Dasgupta 2003). Despite these steps, a 1992 survey found that

76% of consumers felt they had lost control over how information about them was collected and used by organizations (Turner and Dasgupta 2003).

A landmark privacy event of the Internet age was DoubleClick's purchase of Abacus in 1999 (Winer 2001). DoubleClick's specialty was the placement of Internet ads, and accordingly had cookie-based information on many consumers. Abacus was a customer-list exchange company that as a result had data on off-line purchase habits, as well as names and addresses, of millions of customers. DoubleClick's strategy was to merge their Internet data with Abacus' offline data. This would create a highly revealing portrait of millions of customers. The resounding negative publicity resulted in DoubleClick's declaring it would refrain from this plan. What DoubleClick was proposing was no different from many of the merge–purge operations that go on when various lists are combined. However, the magnitude of DoubleClick's endeavor, plus the involvement of the Internet, raised public awareness and kindled the fears raised above.

The Internet and rising privacy concerns in areas such as health care and the exploitation of children have given rise to a plethora of privacy laws; we will briefly review a few of these in Sect. 4.3.3. The fact that these regulations are part of a historical progression suggests that as technology develops and data collection and dissemination becomes more and more seamless, more legislation will be forthcoming.

4.2 Customer Attitudes Toward Privacy

While the above suggests the nature of the fears customers have regarding privacy, there has been some research that has measured customer attitudes and their impact on purchase behavior. In addition, segmentation schemes have been proposed for conceptualizing customer heterogeneity with respect to privacy.

4.2.1 Segmentation Schemes

Ackerman et al. (1999) surveyed web users and identified three segments with regard to privacy and the Internet. (a) Fundamentalists, who are very concerned about the use of data and do not want to provide any data through websites. (b) Pragmatists, who are concerned about privacy but whose fears could be allayed by laws, privacy policy statements, and the like. (c) Marginalists, who are only marginally concerned with the issue. The authors found that Fundamentalists comprised 17% of their sample, Pragmatists 56%, and Marginalists 27%. This suggests that extreme concerns about privacy are confined to a minority. However, if Fundamentalists publicize privacy concerns (e.g., the DoubleClick escapade) and if companies do not allay the concerns

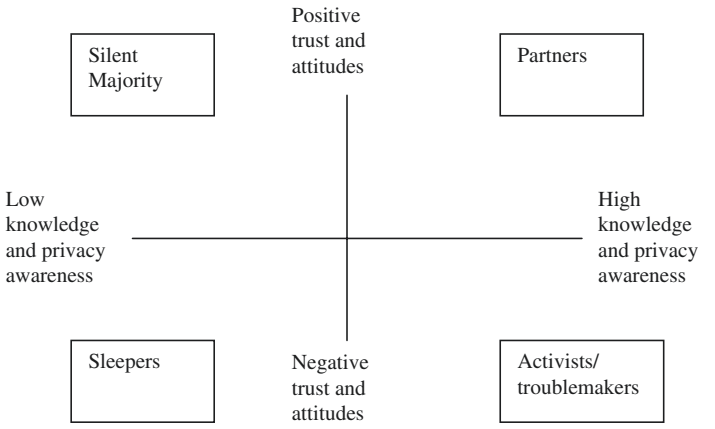

Fig. 4.2 A segmentation scheme of consumer attitudes toward privacy (From Fletcher 2003).

of the Pragmatists, these consumers could easily move to the Fundamentalist camp.

A follow-up study conducted in Germany (Grimm and Rossnagel 2000) similarly found 30% Fundamentalists and 24% Marginalists. The 45% Pragmatists were further subdivided into those concerned with identity (20%) versus profiling (25%). Identity would appear easier to deal with, because companies can use household ID's and contact individuals only after merging the ID's with the names/addresses/phone number file, which could be held by a third party or at least by a limited set of individuals in the organization. However, concerns about profiling seem endemic to what database marketing is all about. Predictive models essentially profile customers most likely to respond, most likely to churn, most likely to be profitable, etc.

Fletcher (2003) proposes a segmentation scheme depicted in Fig. 4.2. The scheme is based on two factors: attitudes toward and trust of the benefits of direct marketing, and knowledge and awareness with respect to privacy issues. Fletcher identifies four segments. (a) Silent majority, who have low knowledge awareness of privacy issues, but positive attitudes toward direct marketing. This group is cooperative but should be educated about the use of data and privacy issues, so they do not turn on companies if they see negative publicity. (b) Sleepers, who also have low knowledge and awareness of privacy issues, but are inherently hostile to direct marketing. There is little that can be done with this group in terms of bringing them into the CRM world. (c) Partners, who are highly aware of privacy issues but have positive views on direct marketing. These are the customers who "buy into" the database marketing exchange equation. (d) Activists, who are highly aware of privacy issues and have negative views on direct marketing. These are similar to the Fundamentalists. CRM companies need to try to educate these people on the value of direct marketing.

The above segmentation schemes are useful but need more testing and refinement. Complicating the picture is that segment sizes and intensity of feelings probably differ by product category (see Bart et al. 2005).

4.2.2 Impact of Attitudes on Database Marketing Behaviors

The key issue is how consumer attitudes toward privacy affect their attitudes toward various purchase behaviors in a database marketing environment. As mentioned earlier, Stewart and Segars found that consumers who were more concerned about privacy stated they would be more likely to request their names be removed from a mailing list, more likely to refuse to give information to a company, and more likely to refuse to buy a product because of the manner in which a company used personal information.

Verhoef et al. (2007) related customer attribute ratings of various sales channels (Internet, Catalog, Telephone) to their attitudes toward searching and purchasing on these channels. One attribute was the extent to which their privacy was guaranteed when purchasing on these channels. This attribute related negatively to purchasing on the Internet, significantly but less importantly to purchasing via catalog, and was not a significant determinant of purchasing in the store. These results make sense and highlight the privacy concerns evoked by the Internet. They also demonstrate that privacy concerns inhibit purchasing, and therefore slow down Internet commerce.

George (2002) studied the relationships among Internet experience, belief that one's data belong to oneself ("Property View"), trust in the privacy offered by the Internet, concerns with the security of buying on the Internet, Internet purchase intent, and Internet purchasing. The main results, based on a 1998 survey of Internet users, are depicted in Fig. 4.3.

The results show that Internet experience builds Internet trust, which begets favorable attitudes toward Internet security, which in turn increases

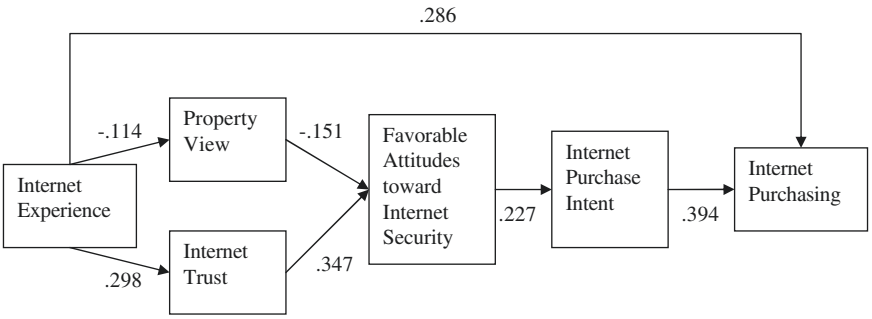

Fig. 4.3 The relationship between privacy attitudes and Internet purchasing (From George 2002).

Internet purchase intent and purchasing. Also, Internet experience is negatively associated with the property view of one's data, which in turn begets more favorable attitudes toward Internet security, and ultimately, higher Internet purchase intent and purchasing. In short, Internet experience induces favorable attitude changes that further enhance Internet usage.

George combines "trust" and "privacy" in his Internet Trust scale. Bart et al. (2005) separate the two. They measured trust as an overall belief that the website delivers on its promises and that the information on the website is believable. Privacy was measured in terms of the clarity of the privacy policy. They find that privacy affects trust, which in turn affects behavioral intent to use the Internet.

In a study reported by Peppers and Rogers (2004a), Intel and Urban found that levels of trust affected the number of software downloads from an Intel website. Privacy was not part of this study, but it reinforces the importance of trust in Internet marketing (see also Pepe 2005).

The emergence of trust as a key factor is very important. Trust is a broader issue than privacy – for example, it involves trusting the product recommendations made from the site, which is not a privacy issue – but it is not surprising that privacy concerns manifest themselves in a lack of trust. Note there may be reverse causality here. Surely privacy concerns undermine trust, but lack of trust could also trigger privacy concerns.

While the above studies clearly show that privacy concerns inhibit Internet purchasing Turner and Dasgupta (2003) suggest that consumers may be more willing to provide data than their attitudes indicate. Chain Store Age (2002) reports that 70% of US consumers report worrying about privacy, but only 40% bother to read privacy policies. On the other hand, Clampet (2005a) reports that 86% of consumers have asked to be removed from a mailing list, and 83% have refused to provide information because it was too personal.

4.2.3 International Differences in Privacy Concerns

An interesting question is whether privacy concerns differ across countries. Milberg et al. (1995) examined the inter-relationships among cultural values, regulatory environment, and information privacy concerns across nine countries. Cultural values included uncertainty avoidance index (UAI), power distance index (PDI), and individualism (IDV) (Hofstede 1980, 1991). UAI measures the degree to which society is averse to uncertainty. Milberg et al. hypothesized that consumers from countries with high UAI should have higher concerns for privacy. PDI measures the degree of inequality among various social classes. Milberg et al. hypothesized that consumers from high PDI countries will be more concerned about privacy, since high PDI countries are characterized by lower levels of trust. IDV measures the degree of independence encouraged in

society. Milberg et al. hypothesized that consumers from high IDV countries would be associated with higher concerns for privacy.

For each of the nine countries, cultural values were measured using Hofstede's classifications. Regulatory levels were measured using the authors' judgments of the degree of regulation (low to high). The authors surveyed 900 members (IT professionals and financial auditors) of the Information Systems Audit and Control Association (ISACA) to measure the concern for privacy, using Smith et al's (1996) privacy measurement instrument.

The results were that (1) the level of concern for privacy differs across countries, (2) however, the prioritization of concerns for various privacy issues is the same, with secondary use first, improper access second, errors third, and collection fourth, (3) cultural values were not associated with privacy concerns, and (4) cultural values were associated with the degree of privacy regulation. Power distance and uncertainty avoidance were positively associated with the degree of regulation, and individuality was negatively associated with the degree of regulation.

These results are interesting and establish inter-country differences in privacy concerns. However, it is interesting that cultural values affected the degree of regulation while not apparently affecting concern for privacy. Milberg et al. (2000) conducted another survey of 595 ISACA members. They examined 19 countries rather than 9, and used partial least squares analysis rather than simple F-tests. In this study, they found that indeed, cultural values affected both the degree of regulation and the concern for privacy. PDI, IDV, and Masculinity (MASC) were positively associated with privacy concerns, whereas UAI was negatively associated with privacy concerns. Like their previous study, they found that UAI was positively associated with degree of regulation, and that IDV was negatively associated with regulation. They also found that MASC was negatively associated with degree of regulation. However, contrary to their previous study, they found that PDI was negatively associated with degree of regulation.

Bellman et al. (2004) surveyed 534 Internet users across 38 countries. Their research differs from the Milberg et al. studies in that Bellman et al. survey consumers. The authors examined three potential correlates of concern for information privacy: (1) cultural values (PDI, IND, UAI, and MASC), (2) current privacy regulatory structure, and (3) experience with using the Internet. Current privacy regulations were classified across countries as "No regulation or self help," "Sectoral" (meaning regulations specific to particular industries), and "Omnibus" (meaning general regulations that apply across industries).

The authors examined the role of regulatory approach as a mediator of the relationship between cultural values and concern for information privacy. Their results suggested that indeed regulatory approach mediated this relationship, in that the relationship between cultural values and overall concern for information privacy became insignificant when regulatory approach was added to the analysis.

However, there were relationships between cultural values and various subscales of the concern for information privacy measure. For example, respondents from cultures with lower IND indices indicated higher levels of concern for errors in the database; respondents from cultures with low PDI and low MASC had higher levels of concern about unauthorized secondary use; respondents from cultures with low PDI desired more privacy regulation and those from cultures with low MASC were more concerned about data security. In addition, online privacy concerns were negatively related to Internet experience.

Summarizing the Milberg et al. and Bellman et al. studies, concerns for privacy differ across countries. However, findings regarding the relationships between these concerns and cultural values, the desire for regulation, and regulatory environment have not been consistent. Milberg et al. (1995) find no relationship between cultural values and overall concern for privacy, whereas Milberg et al. (2000) find several results, and Bellman et al. (2004) find relationships between cultural values and particular subscales of the overall concern for privacy.

The studies differ in several ways. The Milberg et al. studies sample information system experts and financial auditors, whereas Bellman et al. sample consumers. Milberg et al. (1995) use simple statistical tests, Milberg et al. (2000) use partial least squares, and Bellman et al. use multivariate analysis of variance and mediation tests. An underlying issue here is to decide what is the underlying structural model?

One possible structure is shown in Fig. 4.4. In this model, the most straightforward path is that cultural values influence concern for privacy, which in turn influences desire for regulation, which in turn influences regulatory structure. However, cultural values might also have a direct impact on desire for regulation, which also influences regulatory structure, so concern for privacy might not play a role in determining regulatory structure. In addition, regulatory structure can influence concern for privacy as well as the desire for regulation. So there is also reverse causality in the model. Unraveling these relationships would be difficult but important. In addition, Bellman et al. show that consumers' Internet experience is associated with lower privacy concerns. Perhaps "Database Marketing Experience" should be added to the framework.

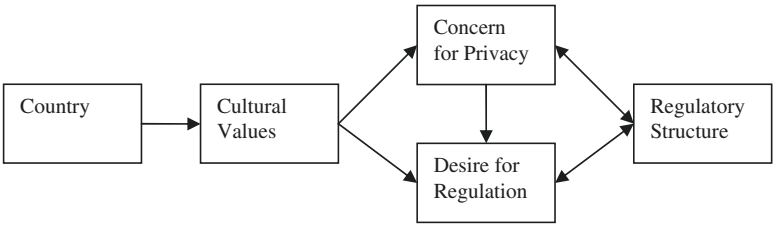

Fig. 4.4 Potential framework for analyzing country differences in concern for privacy and regulatory structure.

4.3 Current Practices Regarding Privacy

4.3.1 Privacy Policies

Companies – especially those selling through the Internet and catalogs – have adopted official privacy policies that they make available to consumers, typically on web-sites. There are three key components of these policies:

- *Opt-in vs. Opt-out*: "Opt-in" means that the customer has the opportunity *proactively* to agree to various uses of their data, where the "null" is that the data *will not* be used. Opt-out means that the customer can proactively assert that their data are not to be used, where the "null" is that the data *will* be used.
- *Internal vs. third-party usage*: Companies may use the data only for their own marketing efforts, or they may "partner" with other companies. They may sell the data to another company, e.g., a magazine may sell its subscription list to direct marketers, or the company might serve as an intermediary for transmitting offers to customers. For example, a cell-phone company might partner with an electronics company and offer a certain subset of its customers a deal on a DVD player.
- *Customer characteristic versus purchase history data*: Some companies only collect customer characteristic data such as age, gender, etc. Others, in fact most, also collect purchase history data.

These components suggest a taxonomy for privacy policies. For example, a company might be opt-in/only for internal use, for customer characteristic data, and opt-out/third-party use, for purchase history data. To gauge the prevalence of the various policies, we analyzed the privacy policies of the top 50 catalogers ranked by Catalog Age (2003). We visited each company website, read its privacy statement, and classified the policy accordingly.[2] The results are in Fig. 4.5. It was often difficult to interpret the various policies (this is an issue itself) and so these results should be taken as exploratory. However, the figure suggests some interesting findings:

- Opt-out is more prevalent than Opt-in. This is interesting, but begs the question of why opt-out is more popular. One hypothesis is that consumers make the choice that requires the least effort (see Bellman et al. and Sect. 4.4.3).
- Both personal characteristic and purchase history data are collected. This was sometimes difficult to gauge, especially regarding purchase history, and we classified nine companies as "don't say" regarding their use of purchase history data. But it appears that companies do inform customers that they are collecting both personal characteristic and purchase history data.

[2] The authors expressly thank Carmen-Maria Navarro for invaluable research assistance in this endeavor.

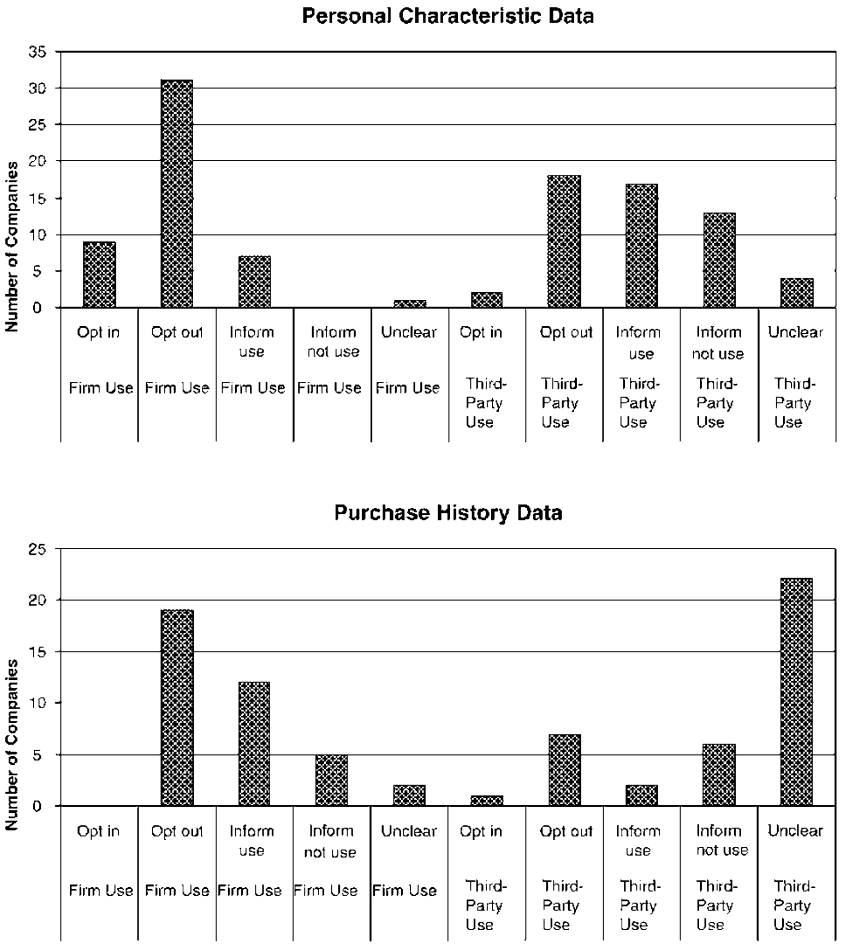

Fig. 4.5 Privacy statement practices among top 50 catalog companies in 2003.

- While opt-out is the most popular policy, there are a surprising number of instances where customers are simply informed of how the data are used and nothing stated about opting in or out.

Again, these results are exploratory, but they suggest a number of issues for further investigation in company use of privacy statements. First is that indeed, privacy statements are commonly made public but they are non-standardized and often difficult to interpret (see also Martin et al. 2000).

Second, companies seem to prefer opt-out. However, it isn't clear that this is the optimal policy. Since many customers do not read the privacy statements, they may not realize that their data is going to be used, possibly by third parties as well as the collecting firm. When they receive various offers that they then feel are an invasion of privacy, this only exacerbates the privacy

problem and lowers response. It might be that if companies publicized their privacy statements better and utilized opt-in, privacy fears would be allayed and companies would be left with a highly responsive group. Opt-in might provide the first node in a decision tree predictive model in that those who do not op-in probably are less responsive.

Third, what is the optimum combination of policies for own versus third-party use, and for personal characteristics versus purchase history? Chen et al. (2001) use a game-theoretic analysis to show it may be of interest for a firm to sell its customer information to another firm (see Sect. 4.4.7). Another consideration in sharing information is whether to identify the partner with whom the information is shared. If that firm is prestigious, the customer may be more satisfied with the firm's sharing data with third parties and view it as an opportunity to form relationships with prestigious firms.

Fourth, exactly what it means to use or share data needs to be explained *thoroughly* to the customer. In the experience of the authors, a company would rarely provide their customers' complete purchase history data to a third party together with names and addresses. Instead, a third party might make a request, e.g., "extend this offer to customers who've bought a high definition television set over the last year". Serving as a conduit rather than actually giving the data to the third party might be perceived as less invasive by customers. In short, the black box of what it means to share customer information with third parties perhaps should be opened up for consumers.

4.3.2 Collecting Data

The manner in which companies collect data can increase privacy concerns. For example, companies often compile purchase histories directly from transactions. This is a seamless, unobtrusive way of collecting data. Internet companies, however, may want to collect data on customer search behavior. For this, they use cookies, thus potentially alarming the customer that their privacy is being invaded. Bricks-and-mortar stores have an even more challenging situation. It is often very difficult for them to "match-back" store purchases to the company's house file. Retailers therefore find themselves instituting a loyalty program, primarily for the purpose of collecting customer data! Registration for the card usually requires the customer to answer a few questions, at a minimum name and address, so it is easy to track customers who use their loyalty card.

Data on personal characteristics are collected in various ways: (1) upon registration at a web site or for a loyalty card, (2) from "complilers" such as Equifax, that collect as much publicly available information as possible on millions of individuals, (3) from purchasing lists (e.g., a company can purchase a list subscribers to a particular magazine), and (4) from data sharing (Stone and Condron 2002) and cooperative exchanges.

A well-known exchange forum in the catalog industry is run by Abacus. Companies contribute names to a database (perhaps with additional information such as whether the person has purchased in the last X months) and in turn withdraw names from the pool. Companies can specify certain competitors that cannot be allowed access to their names. In addition, sometimes companies exchange names directly. For example, company A and company B may provide each other access to 100,000 customers on their "12-month buyer" list. These exchanges can be a crucial way that companies acquire customers, and acquisition efforts arguably lower prices for the sought-after customers. In addition, the availability of list exchanges lowers the costs of customer acquisition, further driving down prices.

But should customers be informed of this practice? If informed, would so many customers opt out that this would cease to become a productive way of acquiring customers, driving up price? Chen et al. (2001) also would argue that information exchange could increase prices because it cushions price competition. How would customers react to this theory in terms of their attitudes toward sharing data?

4.3.3 The Legal Environment

A host of legislation has been enacted in the USA, Europe, and the rest of the world as well. Europe is known for its 1995 "Directive on Data Privacy," (http://europa.eu.int/eurlex/lex/Notice.do?val = 307229:cs&lang = en&list = 307229:cs,&pos = 1&page = 1&nbl = 1&pgs = 10&checktexte = checkbox&visu = #texte), which places the burden on organizations to seek permission before using personal information for any purpose (Turner and Dasgupta 2003). Specific provisions include:

- Data must be "collected for specified, explicit and legitimate purposes."
- The consumer ("data subject") must be told "the purposes of the processing for which the data are intended."
- "Personal data may be processed only if the data subject has unambiguously given his consent."
- The consumer must be informed of the "right of access to and the right to rectify the data concerning him . . . to guarantee fair processing in respect of the data subject."
- The company "controller" of the data must notify a "supervisory authority," a public authority for the correct administration of the law, "before carrying out . . . automatic processing . . . " of data.
- Data transfer to another country can take place only if "the third country in question ensures an adequate level of protection."

The directive pursues a full disclosure policy – the consumer will know what data are being processed for what purposes, will have access to the data, and

can consent or not consent to particular analyses of the data. In addition, the directive sets up a public official to administer the law, and requires companies to report to this official.

The dictum that data transfer can take place only to a country that has an "adequate" level of protection raised concerns among US companies, since the USA does not offer as much protection as the European Directive. As a result, customer lists that flow freely within the USA might not flow from Europe to the USA. This would hamper direct marketing efforts of US companies in Europe, for example, US credit card companies seeking to acquire new customers. In 2000, negotiators created a "Safe Harbor" agreement, whereby American companies that ascribe to seven principles could do business without fear of European sanctions (Harvey and Verska 2001; Carlson 2001). Many American companies did not sign this agreement because it would still require full notification of customers whenever their data are being processed and for what purpose, and European customers could forbid specific analyses. However, in 2001, Microsoft signed onto Safe Harbor (Lucas 2001) and by 2005, 400 US companies had followed.

While the Safe Harbor system seems to be in place, as recently as 2005, the European Commission complained to the USA that its companies were not fully complying, and urged the US Department of Commerce to enforce the agreement fully (Swartz 2005). A complete description of the Safe Harbor agreement is available at http://www.export.gov/safeharbor/safeharbordocuments.htm. While it is a relaxation of the European Directive, it still has several strong requirements, including that (1) companies notify European consumers about the purposes for which it collects and uses their data, (2) if the company wishes to disclose data to a third party, consumers must have the right to opt out of any disclosure to a third party, or out of any use other than that originally notified, and (3) also must have access to the personal information companies hold on them (with the exception when the "expense of providing access would be disproportionate to the risks to the individual's privacy").

Clearly this is a regulatory issue in flux. There are many questions that will undoubtedly be resolved over the next few years. For example, if a cataloger obtains a list from a European company (assuming the consumer has consented), does the cataloger have to inform the consumer each time he or she is included in a predictive model?!? What are reasonable costs of providing consumers access to their data? If one division of a company obtains data, say the magazine division of AOL/Time Warner, would the magazine division need permission from the consumer in order for AOL to use the data? Finally, will the Safe Harbor agreement, or even its more highly regulatory European Directive parent, become law for transactions within the USA?

In addition to the European Directive and Safe Harbor agreement, there have been some specific laws passed in the USA pertaining to data privacy. Following is a brief summary of four significant laws (see

also Goldstein and Lee 2005; for a summary of additional laws, see http://www.consumerprivacyguide.org/law/):

- The CAN-SPAM Act: This applies to commercial e-mail messages used for direct marketing (Dixon 2005). It requires that firms accurately identify the sender of the message, provide a clear mechanism for the customer to opt-out, and make clear that the message is an advertisement or a solicitation.
- Children's Online Privacy Protection Act (COPPA): Protects the privacy of children with regard to the Internet (http://www. consumerprivacyguide.org/law/). The law requires websites that cater to children 12 and under to inform parents as to their information practices and obtain parent consent before collecting personal information from children. It also allows parents to review and correct information the website might have collected about their children.
- Gramm-Leach-Bliley Financial Modernization Act (GLB): Regulates the sharing of customer information in the domain of financial products and services (http://www.consumerprivacyguide.org/law/). It informs customers about the privacy policies of financial companies, and gives customers opt-out privileges over how financial companies share financial information.
- Health Insurance Portability and Accountability Act (HIPAA): The HIPAA Act of 1996 and subsequent regulations govern patient medical information, covering three main areas: privacy (e.g., when patient consent is needed to release medical records, when patients can access their records, etc.), security (protecting the confidentiality of data in electronic networks and transmissions, and transactions (standards for content and format of medical information when shared between health insurers, providers, and other health organizations) (Speers et al. 2004).

One can see elements of the European Directive incorporated in these laws. For example, they emphasize clearly informing customers of privacy policies (if not actual use of the data) and the right to opt-out and patient consent.

An additional regulatory step taken in the USA is the National Do-Not-Call Registry (www.donotcall.gov). Citizens can sign up and as a result cannot be called for many telemarketing purposes. There are some obvious exceptions – calls that are for survey purposes, political campaigns, and charities. In addition, the registry allows calls from companies with whom the customer has an existing relationship. This would appear to favor large companies, since they have more customers they could call. One might argue this decreases competition. For example, if a customer has a cell-phone contract with Verizon, Verizon can call him or her to cross-sell services or adjust the contract. This in turn gives Verizon more monopoly power over the customer, which enables higher prices. Whether this is in fact a consequence of the do-not-call registry is of course conjecture, but it is an important consideration and illustrates the potentially subtle economic impact of all privacy regulations.

4.4 Potential Solutions to Privacy Concerns

In this section, we review steps for addressing the privacy concerns listed in Fig. 4.1. Table 4.1 shows which steps might address each concern. We also discuss what the net effect of each step might be on the consequences of privacy concerns.

4.4.1 Software Solutions

A number of software solutions have been proposed to ensure customer privacy. Software is available that allows companies to take into account customer privacy preferences when marketing to their customers (Maselli et al. 2001). The software also allows sensitive data such as financial and credit information to be linked via a user ID but not to a specific name and address. As a result, very few people in the company would be able to associate a particular name with sensitive data. Software is also being developed to enable data mining of data owned by different organizations without the data actually having to be shared (Kantarcioglu and Clifton 2004).

A host of software solutions have been developed specifically for the Web and e-commerce (Turner and Dasgupta 2003). For example "anonymizers" provide customers with the ability shield their computer's IP address, or provide a new IP address each log in, so that the company cannot use cookies to record the customer's transactions. In fact, Hoffman et al. (1999) recommend that companies allow customers to be anonymous or "pseudo-anonymous", although they still need to be addressable in order to conduct database marketing. There are also tools the customer can use to block certain e-mails, counter the placement of cookies, or the customer can simply delete cookies.

In summary, software can address privacy concerns pertaining to data security, secretive data collection, third-party access, and fears of violation. One possible benefit is that ethical dilemmas can be avoiding by distancing managers from the data. For example, they would no longer have access to personally identifiable information. To the extent that companies use software to integrate customer privacy preferences with their marketing efforts, it can also diminish junk mail and spam and the "none-of-your-business" attitude. If customers interpret a company's use of sophisticated privacy software as a cue that the company cared about the customer, they might be more receptive to its marketing efforts. While these benefits are uncertain, it is certain that software and software maintenance is always expensive.

4.4.2 Regulation

Regulation can be thought of as a continuum from no regulation to self-regulation to government regulation (Milberg et al. 1995).

Table 4.1 Potential solutions to privacy concerns

Concerns	**Potential solution**							
	Software solutions	Government regulation	Self-regulation	Permission marketing	Customer data ownership	Engendering customer trust	Top management support	Privacy as profit maximization
Data security	√	√	√	–	√	√	√	–
Secretive data collection	√	√	√	√	√	√	√	–
Junk mail and spam	√	√	√	√	–	√	√	–
Third-party access	–	√	√	√	–	√	√	√
None-of-your-business	–	√	√	√	√	√	√	–
Violation of privacy	√	√	√	√	√	√	√	–
Inequitable exchange	–	–	–	√	√	√	√	–
Fear of data errors	√	–	–	–	–	–	√	–

A "√" means that the potential solution might address the corresponding concern.

4.4.2.1 Government Regulation

Regulations such as the European Directive and the other initiatives discussed in Sect. 4.3.3 can address many privacy concerns, including data security, secretive data collection, junk mail and spam, third-party access, and none-of-your-business attitudes. For example, the European Directive includes provisions on third-party access and informing customers what data are being collected. The CAN-SPAM Act curtails spam. The Gramm-Leach-Bliley Financial Modernization Act (GLB) regulates sharing of financial information among companies. The Do-Not-Call Registry alleviates concerns about unwanted telephone solicitations. Government regulation in the USA focuses especially on the privacy of truly sensitive data, such as medical information (HIPAA), financial data (GLB), and children's information (COPPA).

Government regulation provides an easy "out" on ethical issues, e.g., "What we did was legal under the Such-and-Such Act." However, government regulation is costly in that it often includes compliance monitoring, which can be expensive both for the government and for firms. Whether the benefits of regulation result in higher sales and profits depends on how customers interpret the regulations. If customers view regulations as addressing their fears so they can do business with companies and not be concerned about privacy, customers might be more receptive to firms' marketing efforts. The key unanswered question is, does government regulation increase trust (Turner and Dasgupta 2003)?

4.4.2.2 Self-Regulation

Self-regulation often consists of standards set by an industry trade organization and adhered to by its members. A prime example is the Direct Marketing Association's "Privacy Promise" (Direct Marketing Association 2007). This contains four key provisions: (1) provide annual notice of the customer's right to opt out of third-party information exchanges, (2) honor customer requests to opt out of these exchanges, (3) accept customer requests that they be added to in-house "suppression" files – lists of customers that are not to be contacted by the company, (4) use the DMA's Mail Preference, e-Mail Preference, and Telephone Preference Service lists to weed out prospects who do not wish to be contacted.

Another example of self-regulation is the Platform for Privacy Preferences (P3P) initiative. P3P was developed and recommended for company adoption by the World Wide Web Consortium (WC3) in 2002 (Computer and Internet Lawyer 2002). P3P offers the capability for the Internet customer to access the website's privacy policy in a standard format and compare to his or her own preferences (Matlis 2002; Grimm and Rossnagel 2000).

This type of self-regulation can allay the same customer fears that government regulation addresses. The problem however is whether customers

perceive self-regulation to be as effective. For example, while all DMA member companies sign a statement agreeing to the Privacy Promise as part of their membership, identify a Privacy Promise contact person, and re-affirm compliance each year, customers may be concerned about whether the DMA monitors compliance. P3P has no compliance mechanism (Matlis 2002). As a result, self-regulation is less costly, but its effectiveness depends on whether customers are aware of it and believe it works.

4.4.3 Permission Marketing

Permission marketing (also called "permission-based marketing") refers to obtaining the customer's consent before initiating database marketing efforts (see Peppers and Rogers 2004b). The main benefit of permission marketing is to make clear the exchange proposition: the company wants to collect data on the customer and in return will use the data to personalize products and offers. Permission marketing should also address customer fears of secretive data collection, junk mail and spam, third-party access, and feelings of none-of-your-business and violation.

If permission marketing delivers on its promise, targeting can be more efficient. First, the customers who do not want to participate in permission marketing probably would be low responders anyway. Customers who directly permit database marketing messages probably are more apt to respond to them (Godin 1997). Second is that the customer presumably would allow the collection of a lot of data. Permission marketing is also ethical in that the customer has full information on the system, although it may increase costs in terms of gaining and recording the permission. A key question is whether sales and profits increase under permission marketing. To the extent that targeting efficiency is higher, profitability in the sense of ROI should increase. But whether absolute profits increase depends on how many customers agree to participate. It is quite possible that under permission marketing, the firm is left with a lucrative but small number of customers with whom it can undertake database marketing.

A central issue of permission marketing is the format of soliciting customers, i.e., how to "pop the question" of whether they wish to participate. There are two basic considerations in posing this question: (1) the framing of the request, which can be either positive "I wish to participate" or negative "I wish not to participate", and (2) the default action assumed, which can be "yes," "no", or neither. For example, if the question is framed, "I wish to participate" and a "yes" box is checked, the customer is participating unless he or she opts-out by checking the "no" box. Opt-in can therefore be defined as when the customer decides to participate either by default or by proactively saying yes. Opt-out can be defined as when the customer decides not to participate, either by default or by proactively saying no.

Bellman et al. (2001) investigated the premise that customers would respond in the direction that required the least effort, following the path of least resistance. They examined two factors in a controlled experiment: (1) positive versus negative framing of the solicitation ("I want to participate" versus "I do not want to participate") and (2) whether the default answer indicated participation, no participation, or neither.

The authors conducted two experiments. The first was to investigate just the framing. They asked 134 Internet users whether they wanted to receive surveys about health issues. The question was framed in two ways: (1) the statement "Notify me about more health surveys" appeared and the customer had to proactively check a box in order to participate (opt-in presentation); (2) the statement "Do not notify me about more health surveys" appeared and the customer had to proactively check a box in order not to participate (opt-out presentation). The authors found that 48.2% participated under the opt-in format, while 96.3% participated under the opt-out format.

In the second experiment, Bellman et al. combined question framing with default box-checking. There were two factors in the experiment: framing of the question and action requirements in terms of box-checking. The framing question was asked in two ways: "Notify me about future health surveys" (positive framing) or "Do not notify me about future health surveys" (negative framing). The box checking could either be so that the null was to participate, not participate, or neither (box not checked). So for example the statement "Notify me about future health surveys" with the "yes" box checked would be a positive frame with the default being opt-in.

The results, depicted in Fig. 4.6, showed that positive framing and the no-action default increased participation rates. Figure 4.6 shows that if the customer saw the statement "Notify me about more health surveys" and the "yes" box was checked rather than the "no" box, 89.2% would participate. That is, only 11.8% would uncheck the "yes" box and check "no." On the other extreme, if the wording was negative, "Do not notify me about more health surveys" and the "yes" box was checked, indicating the customer would have to press "no" in order to opt-in, only 44.2% opted in.

Bellman et al.'s work is important because it shows the format of how customers are solicited for permission marketing is crucial for how many customers sign up. Wording the question in a positive way ("I want to participate") and having a yes box checked, can double participation rates over wording the question in a negative way ("I don't want to participate") and having a yes box checked for that. Interestingly, with a positive frame, the default checking of the "yes" box does not seem crucial. As Fig. 4.6 shows, wording the question positively yields 88.5% participation even if no box is checked, whereas asking the same question and checking the "yes" box as a default adds only slightly, yielding a participation rate of 89.2%.

A crucial next question is whether "manipulating" the customer into participating influences further response to the direct marketing offers to follow. That is, perhaps positive wording with a yes default yields the most

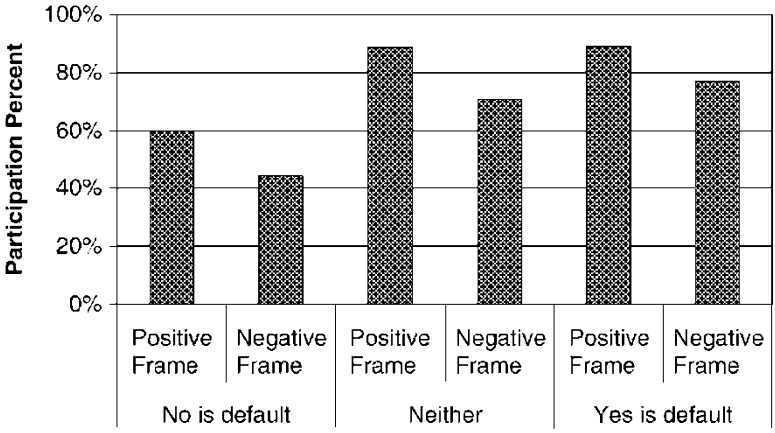

Fig. 4.6 Customer decisions to participate in permission marketing as a function of framing and default action. (**a**) Positive frame means the solicitation was worded "Notify me about more health surveys"; negative frame means the solicitation was worded "Do NOT notify me about more health surveys. (**b**) "No is default" means the box was checked that would indicate not to participate. "Yes is default" means the box was checked that would indicate participate. "Neither" means that neither box was checked (From Bellman et al. 2001).

customers, but many customers were essentially defaulted into participation, and they won't respond well to future direct marketing efforts. Whereas the customers who saw a negative wording with a default indicating non-participation had to take action in order to participate, and hence might be better responders further down the line. This is an important area for future investigation.

Another aspect of permission marketing is the need for companies to educate the customer – to spell out exactly what CRM is, and why the trade of privacy for database marketing is worth it. Customers seem to accept that financial institutions such as banks need to know their credit history. The view is that free flow of information lowers risk and keeps interest rates down. As a result, it helps the economy. The same argument needs to be made regarding other products – the free flow of information helps companies keep their marketing costs down, tailor appropriate services, and target price discounts. Customers need to "buy into" this notion and be willing to provide the data to make it happen – on a permission basis. In summary, in order for permission marketing to be profitable, it needs to be *marketed* to the customer.

4.4.4 Customer Data Ownership

The aim of customer data ownership is to grant the customer control of his or her data. There are two ways this can be done. First is to provide customers

with access to their data and the right to change it (Zwick and Dholakia 2004). Cespedes and Smith (1993) early-on recommended consumer access to and control over their information. Zwick and Dholakia mention Amazon.com as a case in point, where customers can learn the reasons for recommendations Amazon makes, and update or add to their preference data in order to improve the quality of these recommendations. This essentially makes the customer an active participant in the estimation of predictive models-the data provided by the customer increase the accuracy of the recommendation engine used by Amazon. So this form of customer data ownership should result in higher response rates.

Another form of customer data ownership is to let customers house their data on their computers. Watson (2004) envisions a system of "Customer-Managed Interactions" (CMI) whereby customer compile their own data on preferences and behaviors regarding various product categories. They then submit their data to companies and ask for tailored offers. For example, the customer might maintain a database on his or her travel history, vacation preferences, etc. When it comes time to take a vacation, the customer sends the data to various travel agencies who then compile a product recommendation and offer for the customer. Essentially, this system brings the "request-for-proposal" (RFP) system used in government and B2B sectors to the realm of database marketing.

Data ownership addresses several concerns related to privacy. It addresses data security, secretive data collection, and none-of-your-business and violation attitudes. In addition, it makes the nature of the exchange-information for better service and more appropriate offers-more clear. One concern is that providing customers with ownership of their data can be costly. As with permission marketing, the question of whether it increases sales and profits depends on how many customers want to participate. It does appear to address the ethical concerns with database marketing, because customers know exactly what data are being housed in the company.

4.4.5 Focus on Trust

Bart et al. (2005) as well as other work discussed in Sect. 4.2 identify the intermingling of trust and privacy. How exactly to combine trust and privacy in a database marketing context is a fertile area for future research (e.g., see Peppers and Rogers 2005a). Trust addresses concerns about junk mail and spam, third-party access, data security, and fears of violation. However, its main promise is to define the DBM exchange equation – the customer trusts that by providing the company with better data, he or she will be better served. The result, as indicated by Bart et al.'s work, is higher sales levels. Customers who trust companies tend to buy more from them.

Cespedes and Smith (1993) suggest a three-faceted approach to engendering trust: (1) obtain clear and informed consent regarding the use of a customer's data, (2) acknowledge corporate responsibility for information accuracy and allow customers to access and edit their data, and (3) categorize customers based on behaviors rather than personal characteristics. The third recommendation is particularly interesting. Customers will perceive as fair a system that provides heavy users with special offers, but less likely to believe a system is fair if it provides customers of certain income groups with special offers. Perhaps the key theme of Cespedes and Smith is *transparency* – transparency in how the data are used, what data are collected, and access to the data.

Bart et al's (2005) rating scales for privacy involve transparency, reflected in phrases such as "easy to understand" and "clearly explains." The fact that this measure links so strongly to trust shows that transparency is crucial for establishing trust. Our review in Sect. 4.3.1 suggests current practice entails vaguely worded privacy policies. One possibility would be for companies to adopt a standard format for stating policies that makes clear where the company stands on the three crucial issues: what data are collected, do third parties have access to the data, and can the customer opt-out.

Additional recommendations for engendering trust include: make it part of the corporate culture; engender the attitude among the entire company that they need to do all that's possible, not merely all that is required, to ensure customer privacy (Peppers and Rogers 2005b); and publicize customer trust ratings obtained via surveys – e.g., a recent survey found eBay, P&G, Amazon, and HP among the most trusted companies (McClure 2004).

4.4.6 Top Management Support

The European Directive requires companies to create top management positions and empower the occupiers of these positions to ensure privacy within their company. It appears that more and more US companies are creating the position of Chief Privacy Officer (Clampet 2005b). For example, the CPO at Pfizer is needed simply to deal with the regulatory environment created by HIPAA (Corr 2004).

Top management support potentially can address all privacy concerns, because top management can enhance the implementation of software, compliance with government and self-regulation, permission marketing, data ownership, and taking the steps to engender trust. Milberg et al. (2000) measure "corporate privacy management environment" using a number of items, including "how important to the senior management of your organization is information privacy?" They find that the corporate privacy management environment is negatively associated with whether managers

perceive privacy problems within the company. So at least company executives believe that top management support decreases privacy concerns. However, further research is needed to see whether customers see this link.

While the above suggests that top management support can address concerns, it is costly in that it increases personnel costs, and raises concerns about organizational bureaucracy. It hopefully would help resolve ethical dilemmas, because the CPO could make these issues more salient and more openly discussed within the company.

4.4.7 Privacy as Profit Maximization

One view is that the customer database is a competitive advantage for many companies, because it teaches them things about customers that no other companies know, and hence enables them to serve them better. It therefore behooves companies to protect this core competence by not sharing information.

Chen et al. (2001) present a more nuanced viewpoint, that a moderate level of sharing customer data may be a profitable equilibrium in a competitive environment. Chen et al. examine the case where companies vary in their abilities to target customers. Chen et al. express this as knowing brand preference and willingness to pay – their theory is about targeting in terms of price. But the general point is that an important industry capability is how much different companies know about different customers. A main finding of Chen et al. is that industry profits are maximized when targeting is imperfect, i.e., when companies do not know the preferences of all customers. Chen et al. show that when companies do not know much about customers, they should share information to increase profits. But at a certain point this becomes self-defeating because extensively shared customer information promotes price competition (see Fig. 4.2, p. 31 of Chen et al.).

In summary, Chen et al. alleviate the fear that firms will share information *without bounds*. However, they would advocate a balanced sharing of information because "when the achievable targetability in an industry is low, it is important to share customer information. However, it behooves firms in an industry to develop self-regulations at an early stage to protect customer privacy so as to ensure win-win competition in the industry" (pp. 36–37).

Another viewpoint of privacy as profit maximization is that privacy is a company attribute and rating higher on that attribute increases sales and loyalty. In the words of Peter Cullen, CPO of Royal Bank, quoted in Thibodeau (2002), privacy "is one of the key drivers of a customer's level of commitment and has a significant contribution to overall demand," and "plays a measurable part in how customers decide [to] purchase products and services from us. It brings us more share of the customer's wallet."

4.5 Summary and Avenues for Research

In this chapter we have reviewed the nature of the privacy "problem," the consumer perspective on privacy, current industry practices, and potential solutions to the problem. Some of our major conclusions are:

- *Privacy is multi-dimensional.* It ranges from customer feelings of violation to inequitable exchange to a reluctance to have their data transmitted to third parties. The implication is that any measurement of consumer perceptions of privacy needs to be multi-dimensional, and any solutions to privacy concerns must address several dimensions (see Table 4.1).
- *Negative consumer attitudes toward privacy appear to decrease sales.* The evidence comes from three studies: George (2002) found that privacy attitudes influenced Internet purchase intent, Verhoef et al. (2007) found that privacy attitudes decreased use of the Internet as a sales channel, and Bart et al. (2005) found that privacy concerns lead to lower trust and lower trust in turn leads to lower sales.
- *Companies communicate their privacy policies.* This communication takes place at least on the web, and policies vary in terms of opt-in/opt-out/no option for data collection, the type of data collected, and whether the data is shared with third parties. The statements are often difficult to interpret although there seems to be a clear tendency for opt-out rather than opt-in, and providing no option at all is more common than opt-in.
- *There is an active market for sharing customer data.* This occurs through the direct sale of lists, customer list exchanges, and third party collectors of customer data. Customer concerns regarding the sharing of data are well-founded.
- *There is a growing regulatory environment with respect to privacy.* Europe has taken the lead in adopting a strict, highly protective policy, and American companies have scrambled to comply with it. The USA is less regulated, but there are specific laws with regard to children, the financial industry, the health care industry, and e-mail marketing. The indications are that more laws will be forthcoming.
- *There are several potential ways to address customer privacy concerns.* Including software solutions, government and self-regulation, permission marketing, customer data ownership, focus on trust, top management support, and privacy as a profit-maximizing strategy. These solutions collectively can address all customer privacy concerns. They hence offer ways to improve sales levels and ensure efficient targeting, in an ethical way.

The chapter suggests several areas for further research:

- *Which privacy dimensions are most crucial*? How does this vary by industry and customer? Are there customer segments?
- *More evidence on how privacy concerns detract from commerce*: We do have some evidence summarized above that suggests privacy concerns

decrease economic activity, but we need new studies especially with regard to the Internet.

- *What is the impact of regulation*? Is regulation a friend or foe of database marketing? Which is more effective, government or self-regulation, and under what conditions? A fascinating question is whether the do-not-call registry has provided advantages to large firms with large customer bases.
- *What would be the impact of a more transparent information environment for the customer*? If customers knew exactly what data were collected, exactly how they were used, and what decisions were made as a result, would this enhance participation in database marketing or cause too many customers to opt out? This is a crucial issue because probably the underlying fear of many CRM executives is that complete transparency, coupled with opt-in, would result in very little opt-in.
- *Does customer experience with database marketing diminish or enhance concerns for information privacy*? This is a very important issue because if experience diminishes concern, the privacy issue might possibly melt away over time. This issue has been studied with respect to the Internet. The evidence seems to be that experience diminishes concerns (George 2002; Bellman et al. 2004). However, this issue warrants deeper investigation.
- *What is the effectiveness of the various solutions proposed for addressing privacy*? Are some of the customer data ownership proposals feasible? What would be their impact? Is permission marketing the ultimate solution? That is, make it clear what companies want to do, market or communicate the value of what they want to do, and see who signs up? How effective would this strategy be?

In conclusion, privacy is an issue in flux and difficult to research, but it gets at the core of whether the database marketing premise of exchange – data and some loss in privacy for better products/services/offers – is viable as a long-term business model.