Privacy Concerns: Perception Versus Reality

Peter Gray

SYNOPSIS

The privacy and security of consumer information have become significant public-policy concerns in the US and abroad. These concerns are receiving increased attention from Congress, state legislatures, the administration, domestic and foreign regulators, privacy advocates, and the media. With such exposure, the political temptation to enact legislation to protect consumer privacy and security becomes hard to resist. Under the assumptions that consumers are powerless to protect their privacy and businesses do not have the will to do so, some may view legislation and regulation as the ideal solution, rather than a last resort. But enactment of legislation to protect consumer privacy and security can profoundly affect both online and offline information businesses, including the financial-services industry, and may have unintended consequences. This chapter focuses on key privacy and security concerns, the role of self-regulation, the rationale offered for public-policy changes, the role of consumers, the European influence on US privacy policy, and the current trend towards more regulation.

INTRODUCTION

Privacy protection has been a public-policy concern for decades. However, rapid changes in technology, accelerated public acceptance of the Internet and electronic commerce, and the development of more sophisticated methods of collecting, analyzing, and using personal information have made privacy a major socio-political issue in the US, Europe, and other areas. Privacy issues increasingly have attracted the attention of the media, politicians, government agencies, businesses, and privacy advocates. In addition, the public has become increasingly sensitized to the protection of their personal information.

Nonetheless, many consumers balance their privacy preferences against other values and interests. Their actual behavior in the marketplace continues to demonstrate their willingness to trade off various degrees of personal privacy for discounts on merchandise, free products and services, points, and other benefits.

Critics of current information and data-protection practices frequently point to opinion polls, consumer surveys, and privacy violations by businesses and governments to demonstrate the erosion of personal privacy. For example, a 1998 survey by Privacy and American Business showed that 81 percent of Internet users expressed concerns about potential threats to their personal privacy while online. Over 70 percent were worried about unauthorized access and use of their e-mails, web-site tracking, and personal profiling.[1] Based on such findings, it has generally been assumed that many people are reluctant to use the Internet for online shopping.

National privacy surveys by Lou Harris and Associates and Opinion Research Corporation over the last 20 years also show a rising trend of public concerns about personal privacy.[2] Politicians and privacy advocates cite the results of such public-opinion polls and anecdotal examples of privacy violations to promote stronger consumer-protection legislation and regulations.

Growing media coverage of privacy abuses further attracts the attention of legislators, regulators, and the public. Indeed, many recent news stories give the impression that personal privacy no longer exists. For example, recent articles highlighted accusations that the IRS sent personal tax data to lenders via e-mail; states sold driver's license photos; banks sold customer information to marketers; and companies compiled massive databases of personal shopping habits without the knowledge and consent of consumers.

When stories like these give the impression that consumers are powerless to protect their own privacy, they provide momentum behind legislative proposals to try to restrict the collection and use of personal information. But such legislation may

curtail cross marketing, data mining, customer profiling, and other activities that could benefit consumers and businesses.

Businesses have adopted a number of strategies to reassure their customers and forestall the most onerous versions of "privacy protection" legislation. They are adopting privacy policies and displaying privacy seals on their web pages. Software vendors are promoting new privacy-protection systems. US businesses and the federal government continue to pursue international negotiations to prevent disruptions of cross-border data flows. Yet class-action lawsuits also are being filed against companies for alleged privacy violations.

Is all this effort and expense merited, or are we suffering from P4 (Preoccupation with Protecting Personal Privacy) syndrome?

Unfortunately, with all the emphasis on privacy protection, much less is known about consumers' attitudes and behavior toward information security. How concerned are consumers about hackers who might gain unauthorized access to their financial accounts or personal files? Do consumers approve or disapprove of security measures, such as unique identifiers in computer chips and software that help authenticate computer users? Do consumers agree that personal-security identifiers can help to prevent fraud and systems intrusions, and that increased security measures can enhance their privacy by better protecting personal information?

Some people may consider security and privacy as separate matters; others may view them as related elements of personal-data protection. We do not have enough evidence to indicate if consumers are willing to trade off aspects of personal privacy for greater security, or whether such trade-offs are necessary. Even if we did, there never will be a single, easy solution to privacy and security protection. Instead, privacy and security preferences can best be achieved through a combination of company and industry initiatives, consumers' actions to protect themselves, enforcement of existing laws and regulations, and, if truly necessary in some cases, enactment of new laws and regulations.

In the US, the scope of data-protection laws and regulations varies by industry and geography. For example, the financial-

services industry is already covered by a variety of privacy-protection laws and regulations that apply domestically and overseas. However, the growing convergence of diverse financial institutions has raised new concerns about sharing of personal information internally and with third parties. The recent political push for more sweeping regulatory solutions to privacy concerns also has focused on several other relatively-unregulated sectors of the information economy: medical and health records, information gathered on the Internet, and data files collected and administered by many state and local governments.

THE ROLE OF PRIVACY SELF-REGULATION

The private sector, quite naturally, prefers a self-regulatory approach to privacy protection. But the US government increasingly has urged industry to develop meaningful ways to provide consumers with better privacy-disclosure policies and greater consumer control over personal information. Companies are being prodded to develop mechanisms that protect information security and data integrity, and to strengthen and enforce their existing privacy policies.

The private sector has responded with a variety of self-regulatory initiatives in an attempt to forestall potentially onerous legislation or regulations that could impede both offline and online business opportunities. For example, the Direct Marketing Association, which offers consumers the opportunity to opt out of mail and telephone solicitations, expanded that program to include Internet solicitations. Many trade associations have developed privacy guidelines or best-practices for their members. A growing number of companies that collect information about consumers in their databases have adopted their own privacy audits and standards, and they disclose their privacy policies and practices in print and on their web pages.

The Better Business Bureau developed the BBB*Online* Privacy Program to verify, monitor, and review company privacy policies and practices; provide a consumer dispute-resolution mechanism; award web-page seals to companies that comply with good privacy practices; and provide educational programs.

TRUSTe and the American Institute of Certified Public Accountants also offer privacy-assurance programs to companies that meet their privacy standards. In addition, new technological solutions are being applied to better protect consumer information.

THE RATIONALE FOR PUBLIC POLICY

In the privacy arena, the rationale for US public policy appears to be based on a series of assumptions that rely heavily on public-attitude polls, media exposure of abuses, potential threats to personal privacy, laws and regulations of other countries, and the misinterpretation of statistical data and anecdotal information. The best illustration of this phenomenon can be found with respect to the Internet and online-privacy protection. Consider the following assumptions and compare them to the reality of the marketplace:

Assumption: Consumers are universally concerned about the privacy of their personal information, both offline and online.
Reality: Some people are more privacy-sensitive than others. Some care most about protecting sensitive information, like their medical records. Others don't seem to care, and they are willing to trade personal information for free or low-cost products and services, greater convenience, and other benefits.

Assumption: Consumers consider privacy as more important to them than convenience, security, reliability, value, choice, customer service, speed of access, and other benefits.
Reality: Individuals have a hierarchy of needs and preferences, which may change over time. For example, a consumer seeking the lowest-cost airfare available may be willing to divulge a degree of personal information in order to get the ticket. Someone who pays bills online may value the security and reliability of that service more highly than privacy. While the opportunity for lower costs remains a primary reason why millions of investors have opened online brokerage accounts, security and service availability are important, too. In the case of researchers surfing

the Web, they may be primarily interested in obtaining greater bandwidth to speed access to, and retrieval of, information, with little or no concern about privacy.

Assumption: Consumers who say they are concerned about their privacy won't surf the Internet or shop and buy online.
Reality: People often behave and act differently from what they say or believe. This particular example of cognitive dissonance may help to explain the discrepancy between public-opinion polls, which point to privacy concerns as a major deterrent to Internet use, and explosive growth in consumer online shopping and purchasing. According to Forrester Research Inc., the number of US households on the Internet grew from 5.8 million in 1994, to 38.8 million in 1999, and the company forecasts 59.8 million online households in 2003.[3] Jupiter Communications reported that the number of US online buyers grew from 18.8 million in 1998, to 28.8 million in 1999, and it predicts 85 million buyers by 2003.[4]

Assumption: Most consumers are worried about unauthorized access to their e-mail messages.
Reality: Despite the availability of various methods to ensure the privacy of their electronic communications, most people don't attempt to encrypt their messages or use anonymous identities. Their actual behavior demonstrates a clear lack of public concern over the privacy of e-mail messages.

Assumption: People have no control over their personal privacy in cyberspace, and they are powerless to protect themselves from privacy intrusions.
Reality: Consumers have a variety of ways to control their online privacy by using technological and other means to protect their personal information. They can disable cookies, encrypt messages, do business with companies that they trust, and use commercially-available privacy-enhancing software. They can also refuse to provide personal information, use anonymous identities, employ filters to block unsolicited commercial e-mail

(SPAM), and configure their browser setup and preference specifications with a pseudonym.

Assumption: Consumers will not do business with companies that don't have privacy policies or privacy seals posted on their web sites.
Reality: Most people want to deal with companies that they trust and in which they have confidence. Good privacy policies and practices are an important element of trust. But good value and product quality, company reputation, excellent customer service, fair and prompt dispute resolution, and other factors besides privacy are also important. Annual consumer-complaint surveys by the Federal Trade Commission and state consumer-protection agencies show that fraud, misleading claims, refund and billing disputes, service availability, and failure to deliver promised merchandise predominate. Consumer complaints about online or offline privacy violations are rare.

In conclusion, there is a critical need to examine the assumptions that tend to drive and shape privacy policy. Legislation and regulations are not the panacea for comprehensive online or offline privacy protection, and they should be used as a last resort. Instead, existing laws and regulations should be enforced, consumers should become better informed and empowered to protect their own privacy, and businesses should compete for the public's trust.

CONSUMER INFLUENCE AND CONTROL OVER PRIVACY

Consumers are increasingly aware that ubiquitous and more-powerful computers, sophisticated data-analysis software, and widespread access to the Internet make it easier for both legitimate and shady businesses, as well as government agencies, to collect, access, and use personal information. Consequently, consumers have become more assertive in demanding that their personal information be protected, and that they be given greater control over the collection and use of such information. The following examples illustrate the influence of the public and the

media on changing the privacy policies or practices of businesses and government agencies:

(1) South Carolina, Florida, and Colorado decided to sell 22 million drivers' photo images and personal data from their motor vehicle license files to Image Data, a private company in New Hampshire that is building a national database to help reduce identity theft, fraud, and other crimes. Media exposure and negative public reaction forced Florida to cancel its contract with Image Data; the Colorado legislature to consider a ban on the transfer of state motor vehicle records; and South Carolina to appeal its contract. Other states are considering imposing restrictions on sales of public information.

(2) Last year, federal banking regulators issued proposed anti-money-laundering regulations that would require banks to monitor customer accounts and report suspicious financial transactions to law-enforcement authorities. Privacy advocates warned the public that this was a government attempt to invade the privacy of consumers' confidential financial information. Consumers responded by sending thousands of e-mails to legislators and other policymakers. As a result, federal banking regulators decided to scrap the proposed rule.

(3) Intel's Pentium III computer microchip contained a processor serial number that was designed to combat online fraud, improve the security of e-mail messages, and limit computer theft by enabling web-site operators to track or trace consumers' online activities. Under the threat of a consumer boycott and negative publicity, Intel changed its software to permit users to deactivate the identification feature.

(4) Microsoft imbedded a unique serial number into its software that identified an individual computer user, the computer being used, and documents created on the computer in order to help the company diagnose and solve users' problems. Under pressure from privacy advocates, Microsoft agreed to modify its software to prevent the automatic transmission of personal information without proper customer authorization.

(5) RealNetworks used its software to collect users' personal information and music preferences online, without their knowl-

edge or consent. Extensive media coverage and public criticism caused the company to change its procedures and software to avoid tracking customers without their consent. The company faces a series of class-action lawsuits alleging violations of various state and federal laws by not complying with its own stated privacy policy.

(6) DoubleClick has been criticized by privacy advocates for tracking advertising click-throughs and profiling consumers who surf the Web. Negative publicity and the threat of legal action caused the company to change its privacy policy to allow consumers to opt out of profiling.

The above examples illustrate how the public, media, and privacy advocates effectively expose and oppose perceived threats to personal privacy. The Internet and modern communications systems are shifting market power toward consumers, who can decide just how much privacy they want. This market power may be expressed through competitive pressure against private companies to preserve market share, retain customers, maintain their reputation, and enforce their own promises. However, to the extent that consumers have insufficient market alternatives to government activities that threaten their personal privacy, they must rely on political power to protect those interests.

BALANCING PRIVACY CONCERNS WITH THE BENEFITS OF INFORMATION SHARING

Companies increasingly have the ability to customize their products and services to suit the individual consumer. In meeting the specific needs of individuals, however, companies often must tailor their marketing efforts based on consumers' personal information about their shopping habits, likes and dislikes, as well as demographic and other characteristics. Yet at the same time, consumers can and should decide the degree of personalization or anonymity they want from marketers.

For example, online behavioral tracking allows companies to know about consumers' interests and preferences, so they can target products and services that meet specific needs. Collaborative filtering software can be used to compile customer tastes

and purchasing behavior, segment consumers into like-minded groups, and use the preferences of some to predict the buying inclinations of others in the group.

The benefits of such methods of market analysis to both consumers and companies are clear. Consumers do not get deluged with unwanted ads and solicitations, and companies save money by targeting their messages to a receptive audience rather than to people who are unlikely to want or need their products or services. Furthermore, use of such software actually *reduces unwanted intrusions* on consumers' privacy.

To help assuage consumer concerns about online security, various electronic authentication methods have been developed to allow buyers, sellers, and other parties to verify each other's identities and to ensure that electronic messages, documents, or communications have not been altered or tampered with during transmission. Electronic authentication techniques can provide a greater level of user confidence in transacting over the Internet. Such techniques also have the potential to reduce online fraud, unauthorized access to personal information, and network security breaches. This technology enables consumers and businesses to conduct many different types of electronic transactions—including the purchase and sale of goods and services, as well as the payment, receipt, and settlement of funds—more quickly, easily, and securely than paper-based transactions.

In conclusion, the common assumption that consumers are powerless to protect their own privacy and security should be challenged. Consumers who are concerned about their privacy or security can and do take action. Businesses tend to respond quickly to both consumer sentiment and market competition. Government responses may not be as immediate, but they are tuned more to the buildup of sufficient political pressures.

EUROPEAN INFLUENCE ON US POLICY

The European Union (EU) adopted a comprehensive data-protection directive in 1995, effective in 1998. The directive includes a prohibition on the transfer of personal information from EU-member countries to other countries that do not pro-

vide European consumers with an "adequate" level of privacy and security. The European standard for adequacy is generally stricter and more comprehensive than that of the US and most other countries. Therefore, if certain industry sectors are considered to have inadequate data-protection safeguards in place, multinational companies with offices in Europe could be blocked from transferring information on European citizens to the US and other countries. Such blockages could affect Internet, intranet, and extranet transactions, as well as computer records and paper-based information on consumers. If enforced, the directive could seriously impede both electronic and traditional commerce activities. Meanwhile, authorities in the US, Latin America, and Asia are considering data-protection legislation modeled on the EU directive.

Government officials from the US and EU have been negotiating in an attempt to avoid blockages of data flows and disruptions to trade and e-commerce, so enforcement of the directive has been delayed to give the parties time to consider alternative solutions. The US Department of Commerce has developed a safe harbor concept that would protect US companies from data-flow blockages if they agree to adhere to prescribed privacy principles. But an agreement with the European Commission, representing the EU, and the US has been elusive, and some European countries may decide to enforce their privacy laws and penalize companies that violate them. In any event, the directive has raised the sensitivity of US policymakers to protecting the privacy and security of US consumers, and legislative and regulatory initiatives to do so can be anticipated. Meanwhile, to avoid disruption of their operations in Europe, US multinational companies are developing contractual approaches to data protection that comply with European laws.

THE TREND TOWARD GREATER PRIVACY REGULATION

Two key public-policy issues face lawmakers and regulators: Can the private sector be trusted to adequately protect consumer privacy and security? Or should government be trusted to impose stricter regulations to guarantee such consumer protection?

Those who advocate stricter regulation rationalize that it will cause more people to use the services of legitimate businesses and be protected from disreputable ones. They argue that more people will participate in electronic commerce if they have confidence that those who violate their privacy or security will be punished. Opponents of greater regulation say that heavy-handed privacy laws and regulations will stifle market opportunities and burden existing operations. Legislation designed to further protect consumer data may make some segments of the public, particularly those who are privacy sensitive, feel more secure. However, it may also disrupt the flow of information, and add to the cost of products and services for all consumers.

Congressional concerns over the privacy and security of personal information have led to passage and recent enactment of legislation that sets various privacy-protection goals, such as: protecting children who use the Internet; criminalizing identification theft and fraud; prohibiting the federal government from requiring Social Security numbers to be placed on driver's licenses; requiring consumer opt-in before personal information from driver's licenses and registration files can be used for marketing purposes; prohibiting the assignment of unique identifiers to health records; and protecting financial information. In addition, many states have enacted privacy laws affecting health care, direct marketing, telecommunications, financial services, and other areas.

Last year, Congress enacted the Financial Services Modernization Act, which applies broadly to banks, thrifts, credit unions, insurance and finance companies, securities firms, retailers, and others that offer consumer financial services. The legislation includes the following new consumer-privacy provisions:

- All covered institutions are required to clearly and conspicuously disclose to consumers their privacy policies on the sharing of nonpublic information.
- Disclosures on sharing of such information must take place when a customer relationship is first established, and annually as long as the relationship continues.

- Unlimited intracompany sharing of customer information is permitted, but customers must be given the opportunity to opt out of sharing personal information with third parties, with limited exceptions.
- The transfer of customer account numbers to third parties for marketing purposes is prohibited.
- States are permitted to enact stricter privacy-protection laws, so long as they do not preempt relevant provisions in the Fair Credit Reporting Act.
- Both federal and state regulatory authorities may enforce the privacy provisions of the act.
- The federal regulators are required to establish standards to ensure the confidentiality and security of customer information.
- The federal regulators are directed to study the appropriateness of information sharing between company affiliates, including the benefits and risks to consumers.
- Pretext-calling by information brokers who phone financial institutions to obtain customer information with the intent to defraud is prohibited.
- Remedies for violations of the act's privacy provisions are established.

Despite concerns over the privacy of their personal information, most customers who have an existing account relationship with a financial institution do not object to information sharing between different business units within a corporate family. In fact, customers often expect their financial institutions to know that they already have an account relationship when they apply for another financial product or service, or when they have an account inquiry or complaint. Furthermore, intracompany sharing of personal information provides a greater level of privacy protection for consumers, since third parties do not get access to customer data if the consumer chooses to opt out. By allowing financial institutions to directly offer their customers a wider array of products, less customer information is shared with third parties and personal privacy is enhanced.

As more consumers use the Internet to bank, pay bills, purchase insurance, shop online, save money, buy and sell securities, and engage in other financial transactions, financial-services companies are designing their web pages to offer a convenient, lower-cost way to access a wider range of financial products and services. For example, a customer seeking an online auto loan can also choose to buy auto insurance from the same source. An individual who wants to invest a sum of money can access a variety of choices among securities and get investment advice based on his or her risk profile. A credit-card holder who wants a mortgage may be able to get preferential terms or rates from the same company. Without the ability to share information between the bank, insurance, credit-card, mortgage, securities, and insurance affiliates of the financial-services company, consumers would not have the opportunity to take advantage of such benefits.

Notwithstanding such benefits, both federal and state legislatures are considering further restrictions on information sharing. For example, New York state is considering legislation that would require companies to get the consumer's prior consent (opt-in) before information may be shared with third parties. In addition, proposed federal and state legislation would require prior consent of the customer of a financial institution before information may be shared between company affiliates. Legislation has also been proposed to restrict data mining and consumer profiling, the collection and use of medical and health information, access to and use of public-record information, unsolicited commercial e-mail, and Internet privacy.

There is a clear trend toward more stringent regulation of consumer privacy and security, despite industry self-regulation efforts, the availability of new technology to protect consumers, and the public's ability to protect itself. While the generally-accepted practice of most businesses is to permit consumers to opt out of the collection and use of personal information, companies are moving toward obtaining consumers' informed consent, getting permission to market products and services, and providing the opportunity to opt in under certain circumstances.

Meanwhile, legislative precedents have been established for mandatory consumer opt-in requirements. The Communications Act of 1934, as amended by the Telecommunications Act of 1996, established an important opt-in precedent. Section 221 (47 USC 221) of the act permits a telecommunications carrier to disclose customer proprietary network information (CPNI) for marketing purposes only when the customer provides an affirmative, written request. The Federal Communications Commission (FCC) regulations to implement the CPNI provisions were subsequently vacated by the 10th Circuit Court of Appeals on First Amendment grounds, but the FCC plans to appeal the decision. Section 631 of the act (47 USC 551) protects cable-TV subscribers' privacy by restricting cable operators from collecting or disclosing personally-identifiable information without receiving prior written or electronic consent. To protect children from online predators, the Children's Online Privacy Protection Act of 1998 (PL 105-277) makes it unlawful for online services to collect or use personal information about a child for marketing or other purposes without obtaining parental consent. In 1999, the Driver's Privacy Protection Act of 1994 (DPPA), which permitted consumers to opt out before motor-vehicle-record information could be disclosed for marketing purposes, was amended to require consumer opt-in permission. And in January, 2000, the Supreme Court unanimously upheld the constitutionality of the DPPA. Thus, states may not disclose personal information from drivers' files without obtaining their affirmative consent.

What are the implications of this trend toward requiring companies to obtain consumer consent before they may use personal information? Most industry officials believe that both traditional and electronic commerce activities will be constrained, because experience demonstrates that most people will not provide advance consent to disclose personal information to marketers and other third parties. Consequently, consumers' opportunities to obtain new, improved, or lower-cost products and services may be lost. Personalized marketing will become more difficult and expensive, the volume of unwanted junk mail will increase, and market efficiencies will be reduced.

To cope with such threats, businesses must become more sensitive to both the privacy concerns of consumers and the political popularity of protecting the confidentiality of consumers' information. To avoid onerous restrictions on the collection and use of consumer information, businesses must demonstrate responsible behavior and convince policymakers of the costs of over-regulation.

CONCLUSION

Both privacy and security are politically popular areas of concern, with growing public awareness and activism in the US, Europe, and many other countries. Opinion polls indicating high levels of consumer privacy concerns and media coverage of privacy and security breaches make data protection an irresistible area for attention by regulators and politicians. Therefore, the temptation to legislate and regulate to protect the public often outweighs the consequences of restricting both offline and online commerce. Furthermore, legislation that is designed to apply to offline business operations may have a significant effect on online activities, and vice-versa. To deter enactment of restrictive legislation, the private sector must demonstrate that it is acting fairly and responsibly to protect consumer privacy and security.

The political bottom line is that the burden remains on business to show that additional data-protection laws or regulations should only be necessary to deal with specific abuses that cannot be cured by other means, or (perhaps) when private-sector actions truly fail to enhance consumer confidence adequately. Legislators should not rush to enact new proposals to protect consumer privacy and security unless the public benefits clearly outweigh the risks of not acting.

Finally, consumers have a crucial role to play. They should exercise greater control over their own privacy and security by only doing business with companies they trust, and they should employ technological and other means to protect the confidentiality of their personal information.

Notes

[1] Louis Harris & Associates and Dr. Alan Westin, "E-Commerce and Privacy: What Net Users Want" (1998).
[2] Ibid.
[3] "The Digital Economy Factbook" (1999).
[4] Jupiter Communications Survey (1999).