Managing Global Privacy*

Anne Stanley

September 2002

Summary: On May 7, 2002, Dr. Benjamin Robinson, chief privacy officer for MasterCard International, led a workshop on managing global privacy for the Payment Cards Center of the Federal Reserve Bank of Philadelphia. Robinson described how changing business practices, industry consolidation, electronic commerce, and economic trends have positioned consumer privacy as a key issue in the financial services sector that must be managed. He discussed various privacy initiatives in other countries and compared them to the environment in the U.S. This paper summarizes the workshop discussion and is supplemented by additional research by the author.

*The views expressed here are not necessarily those of this Reserve Bank or of the Federal Reserve System.

FEDERAL RESERVE BANK OF PHILADELPHIA

Ten Independence Mall, Philadelphia, PA 19106-1574• (215) 574-7220• www.phil.frb.org

Managing Global Privacy

A Payment Cards Center Discussion Paper*

Federal Reserve Bank of Philadelphia

Anne Stanley

September 2002

Summary

On May 7, 2002, Dr. Benjamin Robinson, chief privacy officer for MasterCard International, led a workshop on managing global privacy for the Payment Cards Center of the Federal Reserve Bank of Philadelphia. Robinson described how changing business practices, industry consolidation, electronic commerce, and economic trends have positioned consumer privacy as a key issue in the financial services sector that must be managed. He discussed various privacy initiatives in other countries and compared them to the environment in the U.S. This paper summarizes the workshop discussion and is supplemented by additional research by the author.

*The views expressed here are not necessarily those of this Reserve Bank or of the Federal Reserve System.

PRIVACY AT MASTERCARD

Robinson briefly described MasterCard's privacy policy and the following statement of objectives:

MasterCard conducts its business and encourages its members to use the following general concepts in formulating their individual privacy and information management policies:

- *Recognize the interests and concerns of the consumer;*
- *Develop procedures to safeguard those interests;*
- *Maintain accurate record-keeping procedures;*
- *Disclose personal information only if the consumer is informed; and*
- *Remain flexible.*

In his role as chief privacy officer, Robinson oversees and coordinates MasterCard's privacy-related activities. This includes evaluating privacy risks, managing the ground rules for conducting privacy audits, ensuring that MasterCard is compliant with current laws, and serving as a media and government liaison.

DEFINITION OF PRIVACY, SECURITY, AND CONFIDENTIALITY

The concept of privacy is often confused with the related issues of security and confidentiality. Robinson defines privacy as "the state of freedom from unauthorized intrusion and the expectation that confidential personal information revealed in a private place will not be disclosed to third parties." In distinguishing privacy from security and confidentiality, he noted the following characteristics.

Privacy is:

- The right to have confidential and personal information protected from intrusion by the public; and
- The right of the individual to control disclosure of that information.

Security is:

- Having one's personal information protected from espionage, theft, or attack; and
- Using mechanisms to prevent unauthorized disclosure of information.

Confidentiality is:

- Trusting wholly and having faith in the professional to whom one might entrust private information; and
- Imposing on a trusted party the duty to prevent further disclosure of information.

The following example from the web site of PrivaComp, a company specializing in informing medical patients of their privacy rights, illustrates these three related concepts:

> *"If Mary has a burglar alarm in her house, she has employed a* security *mechanism. When Mary decides to leave home for the weekend, she sets the alarm and activates security. When Mary asks John next door (but not Jane down the street) to check on the pet hamster, she gives John her alarm security code. Mary has chosen to give access to John. Mary has exercised her right to* privacy. *When Mary authorizes John, and only John, to enter her home, Mary trusts that John will not bring someone else (such as Jane) inside Mary's home or give someone else the security code. The issue is one of* confidentiality*, i.e., trusting that John will keep Mary's home off limits to others."* [1]

Putting these definitions into the context of a commercial environment, Robinson noted that "the objective of privacy in a business environment is to protect data subjects from misuse of personal information, the objective of security is to protect data from unauthorized access and alteration, and the objective of confidentiality is to protect companies from misuse of sensitive information." Privacy, deals with social, ethical, and legal concerns; security deals principally with technical and organizational issues; and confidentiality focuses on commercial and legal concerns.

RECENT LEGISLATION

The concept of privacy is not specifically addressed in the Constitution, and there is no single law or statute that governs financial privacy. However, a number of separate federal and state statutes regulate different components of the financial privacy issue. One of the more relevant statutes, the Fair Credit Reporting Act (FCRA), was enacted in 1970 and amended in 1996. The FCRA regulates credit reporting agencies and the information they maintain on consumers. It also addresses the exchange of certain information among members of the same corporate family (referred to as "affiliate sharing"). Basically, the FCRA states that affiliated companies may share among themselves any information that consists of the transactions or experiences between one of the affiliates and the consumer to whom the information relates. The information can be shared either directly between the two affiliates or through a central database. The FCRA also allows affiliates to share any other information provided, as long as it is clearly disclosed to the consumer that this information is being shared and that the consumer is given an opportunity to opt out of the sharing before it takes place.

Passage of the Financial Services Modernization Act, also known as the Gramm-Leach-Bliley Act (GLB), in 1999 further fueled the debate on consumer privacy because it applied to all "nonpublic" personal information about a consumer, not just the consumer information included in loan-related transactions and experiences primarily regulated by the FCRA. This distinction between GLB and FCRA is important to understand because the GLB granted permission to financial institutions to disclose nonpublic personal information to nonaffiliated third parties.

The general rule of GLB is that a financial institution may not directly, or through an affiliate, disclose any nonpublic information (NPI) to a nonaffiliated third party, other than through a joint marketing/service provider agreement or as permitted by law, unless the financial institution:

- Has provided to the consumer an initial privacy notice;
- Has provided to the consumer an opt-out notice; and
- Has given the consumer a reasonable opportunity to opt out.

Opt-out notices must be clear and conspicuous, and they must accurately reflect the institution's privacy practices and policies to the consumer. Also, these notices must be provided when the relationship with the consumer is established, then annually throughout the duration of the consumer's contact with the company.

The first annual mailing of privacy notices required by GLB was in July 2001. According to a *Wall Street Journal* article, "Fewer than 5% of recipients mailed them back, despite surveys showing one third of Americans value privacy above all else. In many cases, the problem was simple: The fliers were incomprehensible — intentionally so, some consumer advocates say."[2] It should be noted that in their initial privacy notices, most financial institutions used the "safe harbor" language provided by the government, which was not "reader friendly." In response to the criticisms, regulators and industry participants who have been working to improve the notices are considering a range of alternatives, including:

- Reducing or eliminating technical jargon;
- Using headings;
- Using examples;
- Using bulleted lists and/or numbering; and
- Testing with various audiences.

The most recent legislation that affects financial privacy is the USA Patriot Act of October 26, 2001. Motivated by the events of September 11, the act empowers the government to fight money laundering and prevent terrorists and others engaged in unlawful activities from misusing the U.S. financial system. Reaction from the financial services community was relatively mute following passage of the law and generally supportive of subsequent money-laundering proposals. The response from the industry following the July 10, 2002, release of proposed Treasury regulations under Section 326 of the act suggests that blanket support for all aspects of the legislation may be wearing thin. At issue are a number of potentially burdensome requirements, including the collection and maintenance of **all documentation related to opening accounts**. For institutions that increasingly rely on remote establishment of accounts, compliance represents a real challenge. Think of the credit card world where there is rarely, if ever, physical contact between the issuing bank and the customer. In the July 18, 2000, issue of the *American Banker*, L. Richard Fischer, a partner at the Washington law firm of Morrison and Forester, notes, "It will be a very, very substantial and often adverse change in the operating procedures of most financial institutions."[3]

Public reaction to the act has, to date, been similarly subdued. Surely much of this reflects support for the "war on terrorism" but perhaps also suggests limited appreciation for the largely unfettered access to consumer financial information now available to the government. As noted by Linda Punch in a recent article in *Credit Card Management,* "The American public's sanguine attitude about access to financial files may be short-lived, if the government misuses the privilege." [4]

Recent privacy legislation has followed a somewhat circular path. Initially, there were no restrictions on the sharing of consumer information. The FCRA regulated consumer reports disclosed by credit reporting agencies and monitored the sharing of public information between affiliates. GLB addressed the sharing of nonpublic information between nonaffiliates and imposed privacy-disclosure and other obligations on financial institutions involved in this practice.

Both of these acts could be viewed as increasing the protection afforded consumers' personal information. However, the Patriot Act now allows government agencies to access information from financial institutions without the consumer's knowledge or permission if certain suspicious activity is observed. Obviously, this act is a response to recent events and, to date, has been broadly supported. However, over time, it could also be viewed as decreasing the protection of consumers' personal information and, ultimately, be subject to further refinement.

PRIVACY & REPUTATIONAL RISK

A Case Study: DoubleClick

While legislation and regulation set important standards for the protection of personal information, public opinion is often a more powerful enforcement vehicle. The story of DoubleClick provides a telling example of the power of public opinion about the issue of privacy. DoubleClick is the largest online advertisement company in the United States. The company provides sites that belong to its network with advertisements to display, then monitors the consumers who **respond to an ad** from these sites through the use of cookies. Cookies are pieces of text that a web server can store on a consumer's hard drive so that a web site will recognize the consumer's computer on return visits and "remember" the consumer's preferences. The information recorded by the cookies can then be placed in a database.

In June 1999, DoubleClick purchased Abacus, the nation's largest consumer database company and gained access to 88,000,000 profiles. These profiles contained information about the spending habits of consumers derived from their more than 2 billion offline purchases. By January 2000, DoubleClick had assembled detailed profiles of 100,000 specific users and were planning to match their online navigational histories, obtained from the cookies, with the offline purchasing information in the Abacus database. At that time, no government or industry privacy standard prohibited this type of activity. However, by January 28, 2000, DoubleClick was hit with its first lawsuit, which challenged the circumstances under which names can be associated with anonymous user activity across web sites. The FTC notified DoubleClick that it was investigating whether the company had engaged in unfair and deceptive trade practices. The market reaction was swift: By March 2000, DoubleClick's stock had lost one-third of its value. The company quickly reversed its plan and released the following statement by Kevin O'Connor, CEO of DoubleClick: "We commit today that until there is agreement between government and industry on privacy standards, we will not link personally identifiable information to anonymous user activity across web sites." [5]

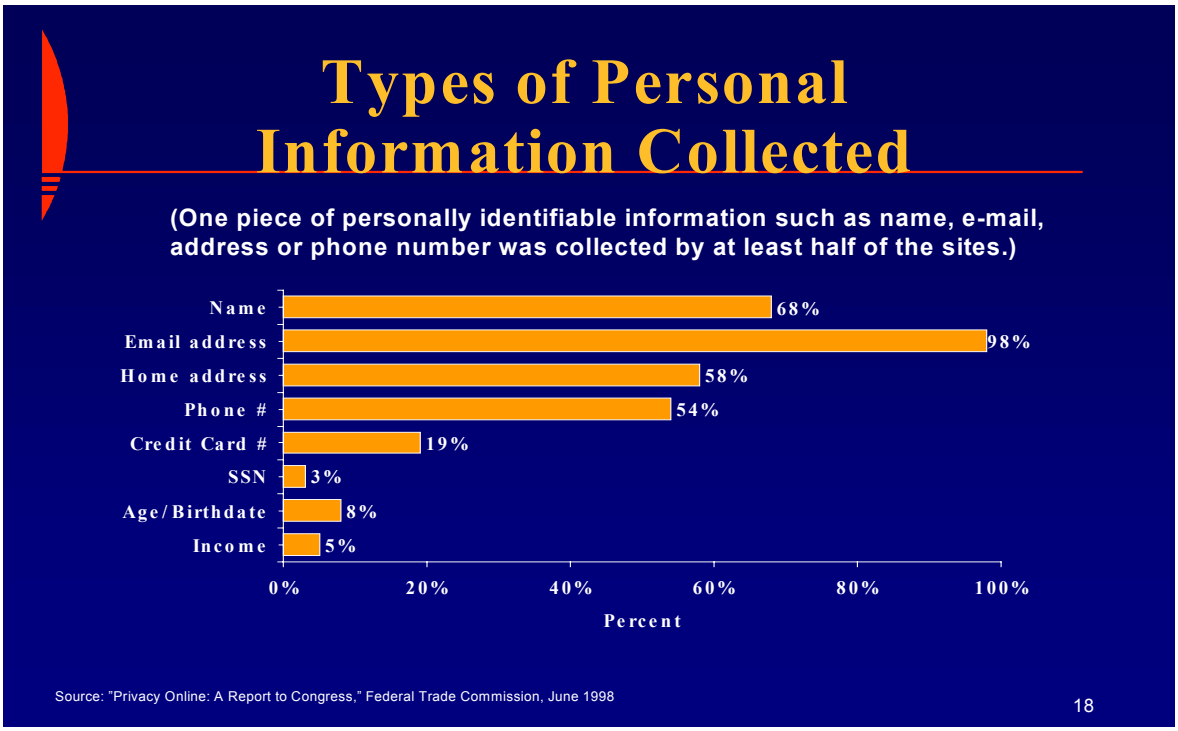
PRIVACY AND THE INTERNET

Since the DoubleClick example relates to the Internet, it illustrates the way this new technology has further complicated the privacy debate. In general, Robinson believes consumers' fears about the Internet stem from their sense that they lack control over their personal information and from their discomfort with available government protection.

A *Pew Internet & American Life Poll* conducted in May-June 2000 found that:

- 84 percent of Internet users fear that strangers will get their personal information; and
- 27 percent of Internet users fear that someone unintended will read their e-mail.[6]

These fears, in part, are fueled by the fact that most web sites collect personal information. In 1998, the FTC surveyed 1402 commercial web sites to see what type of personal information they were collecting and what percent of these sites also provided access to their privacy policies and information-collection practices online. From the 674 sites that responded, the FTC found that 92 percent collected at least one type of personal information and just 14 percent had a privacy policy posted on their site. The graph below, which is taken from the FTC's publication, *Privacy Online: A Report to Congress*,[7] shows the percent of sites in the sample that collected various types of personal information:



In the intervening years Internet merchants have almost all adopted and display privacy policies, but Robinson contends that the FTC's findings about consumer fears remain largely true today. Specifically, the FTC report noted that "research indicates that consumers have less confidence in how online service providers and merchants handle personal information than they have in how traditionally offline institutions, such as hospitals and banks, handle such information."[8]

Robinson explained that some consumers have devised their own form of privacy management on the Internet by providing false personal information and secondary e-mail addresses to avoid giving real information to a web site. According to Robinson, finding a solution to this perception problem is a major challenge to increasing commercial applications on the Internet and, by extension, increasing the use of payment cards in this new environment. As noted in the FTC report, "Findings suggest that consumers will continue to distrust online companies and will remain wary of engaging in electronic commerce until meaningful and effective consumer privacy protections are implemented in the online marketplace. If such protections are not implemented, the online marketplace will fail to reach its full potential."[9]

Since 1998 the bank card associations and other industry participants have made major strides meeting this challenge, and credit cards are the dominant payment vehicle in the growing Internet marketplace. Strict privacy policies, secured communication systems, anti-fraud detection technologies, and various customer authentication schemes have all served to increase consumer comfort with Internet shopping and the use of payment cards in this environment. Nevertheless, the occasional report of merchant sites being compromised or the inadvertent disclosure of personal financial information continues to have a chilling effect on the public and is evidence that further work needs to be done.

INTERNATIONAL PRIVACY LAWS

Further complicating the financial privacy debate is the differing legal structures around the world. For many financial services firms, including MasterCard and its global-issuer members, privacy is an increasingly difficult issue. As an example, Robinson described the European Union's Data Protection Directive, which was effective October 28, 1998. The directive requires that when a firm in an EU country transfers sensitive personal data to a firm in a non-EU country, the non-EU country receiving the data must provide a satisfactory level of data protection or, in other words, be a "safe harbor." Unfortunately, according to Robinson, the definitions of "satisfactory level of data protection" and "sensitive personal information" are not clear, and their applications differ among other countries, particularly the United States. As a result, the United States is not in compliance with the technical terms of the directive, a fact that presents challenges for card issuers, for example, those operating in Europe but processing cardholder information in the U.S.

Robinson noted other differences between European and U.S. privacy law. Among them, the EU's directive has opt-in requirements for information sharing and covers all commercial entities processing any form of information that could identify a person. GLB, on the other hand, has opt-out requirements for information sharing and covers only firms dealing with financial services.

In recent years, efforts to protect personal private information have become a truly international priority. Since 1998, Canada, the UK, Italy, Hong Kong, South Korea, and Chile are among a number of countries that have enacted new or updated privacy legislation. Many European countries have followed the lead of the EU's Data Protection Directive and its emphasis on a "safe harbor" for the transfer of "sensitive" information. Other nations have modeled their privacy legislation on a set of principles developed by the Organization for Economic Cooperation and Development. These principles include provisions for notice, choice, onward transfer, security, data integrity, access, and enforcement.

CONCLUSION

Robinson concluded the workshop by emphasizing that, legal requirements aside, it is most important to monitor and respond to consumers' perceptions. How consumers perceive a firm's commitment to protecting their personal information has become a critical business issue. These attitudes are subject to change and will continue to evolve over time. In his book, *Financial Privacy and Electronic Commerce: Who's in My Business*, Robinson stresses the need for flexibility, noting that "privacy policy will have to focus on 'privacy tolerance' as a concept of consumer acceptance versus a clear definition of what is privacy. In essence, the public will dictate what is acceptable by the current trend of tolerance."[10]

ENDNOTES

[1] PrivaComp Page. <http://www.privacomp.com/secprivintr.html.>

[2]Russell Gold, "Mailing From Banks, Retailers Lets You Protect Financial Data, but It's Hard to Dechiper," *Wall Street Journal* (May 30, 2002).

[3]Rob Blackwell, "Launder Plan Criticized as Burdensome, Ineffective," *American Banker* (July 18, 2002).

[4]Linda Punch, "Cardholder Privacy, Post-Sept 11," *Credit Card Management* (February 2002).

[5] "Statement From Kevin O'Connor CEO of Doubleclick," Doubleclick Inc., March 2, 2000.

[6] Trust and Privacy Online: Why Americans Want to Rewrite the Rules, August 2000. <http://www.pewinternet.org/reports/>.

[7]*Privacy Online: A Report to Congress*, Federal Trade Commission (June 1998), page 25.

[8] *Privacy Online: A Report to Congress*, Federal Trade Commission (June 1998), page 3.

[9] *Privacy Online: A Report to Congress*, Federal Trade Commission (June 1998), page 4.

[10]Benjamin E. Robinson III, *Financial Privacy and Electronic Commerce – Who's in My Business.* (Writers Club Press, 2000), page 12.