44

HUNTON& WILLIAMS

200 PARK AVENUE
NEW YORK, NEW YORK 10166-0136

TEL 212 • 309 • 1000
FAX 212 • 309 • 1100

MARTIN E. ABRAMS
DIRECT DIAL: 404-888-4274
EMAIL: mabrams@hunton.com

FILE NO: 59007.7

May 1, 2002

Via E-Mail and Fax

Regulations and Legislation Division
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, D.C. 20552

ATTN: Study on GLBA Information Sharing

Dear Sir or Madam:

This letter is submitted by the Center for Information Policy Leadership at Hunton & Williams in response to the request for comments published by the Department of Treasury in the Federal Register on February 15, 2002. Thank you for the opportunity to share our views with you on these important topics.

Marty Abrams, the principal author of these comments, is the Executive Director of the Center for Information Policy Leadership.[1] He is joined in these comments by Lisa Sotto, a partner with the law firm of Hunton & Williams and head of the firm's Regulatory Privacy Practice Group. These comments do not necessarily reflect the views of Hunton & Williams or its clients.

These comments describe the reasons that financial institutions share customer information with affiliates and nonaffiliated third parties. The comments also explore the benefits gained by financial institutions and their customers from such sharing of information, and discuss how the flow of personal information creates value for both financial institutions and their customers.

[1] Mr. Abrams also serves as Senior Policy Advisor to the law firm of Hunton & Williams. He is not a lawyer.

I. Data-Sharing Preceded the Computer Revolution

Merchants have always worked to understand their customers. They have used knowledge about their customers to offer better products targeted to the customers' varying needs and interests. They have developed new products and services to meet their customers' changing lifestyles. Consumers, likewise, have always valued highly-personalized customer service.

At the beginning of the twentieth century, merchants began to share information with other merchants in the same community on how consumers paid their bills. This knowledge allowed the merchants to confidently extend credit for consumer durables. Eventually, these bilateral relationships evolved into cooperatives that became the nation's first credit bureaus.

Several years later, early mail order merchants began trading customer names with each other. These merchants understood that a larger overall market would result from sharing customer names, and this increased customer base would more than offset the risk that a competitor would wrestle away an existing customer. These merchants understood that a growing marketplace would best serve their interests.

II. The Evolution of Computer Technology and Privacy Law

A. The Evolution of Computer Technology

Today, we take computers and the Internet for granted. In fact, the technology that drives the current marketplace has existed for only about forty years, and the Internet age is less than a decade old. The technological revolution began at the end of World War II. By the 1960's, mainframe computers had been developed that could solve single business problems. These systems and the data they processed were inextricably linked. The idea of sharing data between applications, much less organizations, was impractical.

In the 1970's, businesses took greater advantage of technology to improve industrial processes such as design, manufacturing and shipping. The introduction of microprocessors led to the development of "personal computers" and, in the 1980's, the invention of networking technologies allowed the distribution of computing power across organizations. The desire to share data between applications began to grow, and businesses began to depend on the increased knowledge.

In the 1990's, predictive sciences were applied to a broad range of business processes. As data storage became less expensive, there was more data available to apply to problems we needed solved. The explosive adoption of the Internet as a consumer (rather than as an academic or commercial) medium made the powers of both data and surveillance visible to the American public.

On the corporate front, we witnessed the emergence of data warehouses and customer relationship management tools that served multiple applications. For example, cataloguers discovered that they could integrate their sales and customer service databases. A marketer might thus discover that the customer who bought $2,500 worth of clothing actually returned most of it. Having a 360-degree view of the consumer helped organizations understand exactly who their best customers were.

B. The Evolution of Privacy Law

Three trends emerged in the 1970's. First, the Fair Credit Reporting Act ("FCRA") established that different applications of information required different rules based on the potential harm that could result from the application. Second, we realized that government use of data was highly-sensitive and required particular safeguards to protect data subjects. This realization led to the enactment of the Privacy Act. Third, businesses began to understand that it was good practice to allow consumers to choose not to receive sales communications if they so desired. In response to this trend, the Direct Marketing Association established its first consumer preference service. These three trends continue to be relevant today, and the first is particularly relevant to these comments.

In 1970, Congress passed the FCRA in response to concerns about the accuracy and use of credit information. Most credit reporting agencies were still using manual systems, and credit reporting was conducted only on a local basis. Consequently, credit reports were not particularly accurate or current, and the data could be used for any purpose. The FCRA focused on actual and potential harms, limited the use of credit data, and gave consumers rights of access and correction. Each of these legislative fixes was proportional to the potential harm that needed to be addressed.

For the next twenty years, privacy laws followed the FCRA model and focused on the harmful application of information (not the control of information). Sector-specific laws like the Video Privacy Protection Act and the Children's Online Privacy Protection Act provided consumer rights in relation to specific uses of information by industry.

This application-focused approach shifted with the enactment of the Driver's Privacy Protection Act ("DPPA"). The DPPA not only restricted the use (application) of motor vehicle and drivers' license data but also sought to impose control restrictions by mandating an opt-out opportunity (and then, via amendment, an opt-in requirement) for the use of these public records for marketing. There was no indication, however, that the use of these records for marketing was harmful in itself. Thus, the law imposed controls even though there was no evidence of actual or potential harm to consumers. The DPPA sought to limit uses of information that were objectionable merely because consumers could not control those uses.

Title V of the Gramm-Leach-Bliley Act ("GLB") muddles the legal arena even further. GLB mandates notice, which is unrelated to any harm, without providing control. The Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") further complicates the equation. HIPAA essentially ignores the concept of targeting restrictions on information flows to specific harms. Instead, HIPAA focuses on notice and consent as a control mechanism. As a result, HIPAA will provide little actual privacy protection. The DPPA, GLB and HIPAA do not address the harmful application of data. Instead, they seek to allay the anxiety of living in an era where information drives all processes and the technology is available to all users. Unfortunately, legislation cannot relieve this anxiety.

III. The Application of Information and Information Flows

As discussed above, the business practice of sharing consumer information arose long before the advent of computers. Merchants have always shared information, offered personalized services, and made credit decisions. Today's processes for evaluating data are less subjective. An issue is isolated, and technology and data are applied to solve the problem. These processes tend to be more accurate, fair and safe. For example, credit scoring reduces discrimination in the lending industry. Credit scores are derived using reliable models; credit decisions are no longer made solely by individuals whose views inevitably are subjective. Robust information flows make these improved processes possible.

Additionally, consumers today have multiple financial relationships. A typical consumer will have a checking account, a savings account, a mortgage, an equity line of credit, a credit card, a debit card and a car loan. These relationships may be with the same bank, with related financial institutions, or with competing institutions. For each relationship, the relevant financial institution collected data directly from the consumer when the account was opened. That application information most likely was augmented by information from one or more credit bureaus. The financial institution probably used the data initially to verify the identity of the consumer and to qualify the consumer for the service requested. The financial institution then used the data for fulfillment, such as printing checks or issuing a credit card. Data also likely flowed across accounts, such as when the consumer's loan payment was directly debited from her checking account.

In the past, all the data was tied to the account, not to the consumer. As such, data-sharing was limited because it was difficult to match account data. Today, the systems either feed into a common data warehouse or are linked so the bank can obtain a complete picture of its relationship with the customer. Now, all account information for a particular customer at a particular institution can be viewed in one place. A customer benefits from having multiple relationships with a single financial institution because the institution can service all her accounts in a holistic manner. The customer can access information in a standard format, thus enabling the customer to easily manage multiple accounts, transfer funds, and receive consolidated

statements. The institution also benefits because it can better predict the products and services that would be of interest to its customer today and in the future. There are innumerable examples of benefits to both consumers and companies that result from the integration of systems and matching of data within an organization.

In this era of specialization, not every organization can offer every product its customers desire. To respond to consumer demand, some companies develop joint-product and joint-service relationships. Other companies supply data to third parties that can then offer their own products directly to the consumer. Much of the controversy over information flows relates to the transfer of consumer information to these third parties. In many respects, however, joint relationships are no different from the financial institution directly offering a product or service to the consumer. The consumer's receptivity to the offer will be directly related to the value of the product or service offered; the fact that it is offered jointly is of little consequence.

The flow of data to support a third party's product offering appears more problematic. In fact, consumer anxiety often stems from concerns about control rather than harmful uses or applications. These concerns are misplaced. History has shown that the early marketers who shared names created the consumer-driven, product- and services-rich market we have today in the United States. Furthermore, information flows create value for consumers by enabling them to receive the right offer at the right time, regardless of the origin of the offer. Incorrectly targeted offers are discarded, as they always have been. The consumer issue should not be control itself; instead, it should be whether the business applications have been harmful, fraudulent, deceptive or unfair.

IV. Benefits and Risks Derive From Applications

Consumer, corporate and societal benefits result from the applications created by information flows, not from the information flows themselves. Similarly, while these applications may create risk, the risk generally is tied to the application itself rather than the underlying information flow.

Research by Wirthlin International for the Privacy Leadership Initiative shows that consumers do not understand the relationship of information flows to the applications that generate value (such as the availability of instant credit) or risk (such as deceptive solicitations). Consumers demand the immediacy and value that comes from customer-focused (rather than account-focused) information systems. For example, many consumers routinely check account balances online, at their own convenience. This beneficial consumer option can translate into real savings for the financial institution if the consumer is able to resolve questions via email or a call to the bank's service center (rather than an in-person visit to the local branch). Information flows that permit immediacy, access and convenience typically are not visible to the consumer. The consumer simply is not aware that information flows are the foundation for the conveniences they demand from the organizations with which they do business.

V. Policy Implications

Each new business application requires new information flows. As noted above, these information flows form the foundation for all new consumer services. Successful applications create real value for both consumers and companies. Other applications that are not valuable to either consumers or businesses will be discarded by traditional market economics.

In addition, some applications of information will create risks for consumers and other applications simply may be inappropriate. The Center for Information Policy Leadership believes that the legislative and policy focus should be on these risky and inappropriate applications rather than on the underlying information flows themselves. Privacy laws should be drafted to focus on appropriate use (not control) of information, and should target harmful applications of information.

We recommend that, when setting policy in this area, policymakers first identify those applications of information that are harmful, deceptive or unfair. Once those applications are isolated, analysis should be conducted to determine which of these bad applications is already regulated by existing laws. For example, fraudulent applications and deceptive marketing practices are already regulated by existing law. Processes that are unfair may need to be specifically regulated. If a process (such as charging a consumer's account without unambiguous consent) is unfair, and that process is not otherwise regulated, the process should be addressed through legislation.

VI. Conclusion

As a society, we have learned a number of lessons from our evolution from a manufacturing-centered economy to an information-centered economy. We have learned that, when technology is developed, it will be applied generally to solve a problem. This application leads to a cycle of economic growth, and a need for more and better technology.

We have learned that today's amazing solution is the business process we will take for granted tomorrow. We have learned that we can no more anticipate tomorrow's applications of information than we can predict tomorrow's weather. We have learned that we do a better job of policing applications that we find inappropriate than we do policing either the data or the technology. In fact, we often have the legal tools already in place to police solutions we find harmful. For example, Section 5 of the FTC Act, prohibiting unfair or deceptive practices, has proven to be a powerful tool in assuring the appropriate application of information to business processes.

How do these lessons relate to issues of information-sharing and the benefits derived from such sharing of information? Information-sharing is merely the process of applying technology and

information to new applications. The organizational and consumer benefits are derived not from sharing the data but rather from having found a solution to a business problem. While consumer anxiety over information flows is real, legislating control over information will not relieve the anxiety. Instead, the anxiety should be addressed by regulating harmful applications of data and rigorously enforcing those regulations. By limiting the flow of information needed to create valuable solutions, we put a throttle on potential economic growth as well as on the ability of consumers, companies and society to benefit from rich and appropriate data applications.

Thank you for the opportunity to provide these comments. For more information, please contact Marty Abrams at (404) 888-4274 (mabrams@hunton.com) or Lisa Sotto at (212) 309-1223 (lsotto@hunton.com).

Sincerely,

The Center for Information Policy Leadership

The Center for Information Policy Leadership at Hunton & Williams

By: _____ LTS
Martin E. Abrams

By: _____
Lisa J. Sotto