

FRIED, FRANK, HARRIS, SHRIVER & JACOBSON

A PARTNERSHIP INCLUDING PROFESSIONAL CORPORATIONS

1001 Pennsylvania Avenue, N.W., Suite 800
Washington, D.C. 20004-2505
(202) 639-7000

A Presentation by:

Thomas P. Vartanian*

**Corporate Executive Board Platinum Initiative 2001: Privacy & Business
Practice**

“In and Out of Court: The Legal Perspective on Privacy & Commerce”
Washington, DC, January 23-24, 2001

Internet: VARTATH@FFHSJ.COM

21st Century Banking Alert™ Page on the World Wide Web at

<http://www.ffhsj.com/bancmail/bancpage.htm>

A Dow Jones Business Directory Select Site

© 2001 Fried, Frank, Harris, Shriver & Jacobson. All Rights Reserved.

**The Quest for a Data Protection Theology: Balancing the Blessings and
the Costs**

By Thomas P. Vartanian

Privacy is in style. Well it should be, given the problems that have been documented by the media. The current edition of “privacy” has emerged from the inner core of the Internet movement and today occupies a position of great social, legal and political prominence. Ironically, our concern for the control and use of information about us as consumers is becoming the dominant issue for us as business people.

But, what has changed in the last several years that has produced the hundreds of draft pieces of federal and state legislation that attempt to protect information about consumers?

First, it is important to understand the parameters of the debate. I believe that there is far too little understanding of what “privacy” entails. The concept of privacy is not new.[1] Neither is it a byproduct of the Internet. There is nothing substantially novel about the information that can be collected through the Internet. Data collection methods have been around for decades, as have databases that are chock full of every minute fact about consumers.[2] Sun Microsystems Scott McNealy understood that when he suggested that consumers “have zero privacy” and need to learn to “get over it.”[3] While that view may be harsh, it makes the point: there have been and are enormous

amounts of information about each of us that is publicly available and wanting to change that reality won't necessarily do so.

What Should Businesses Do?

Before we proceed in this analysis, permit me to make three suggestions:

1. The word "privacy" should be removed from the lexicon of American business conduct and law.[\[4\]](#)
2. American businesses should collectively and proactively educate the public on the benefits of data collection, use and distribution.
3. American businesses should encourage strong laws and swift enforcement with regard to commercial abuses of personally identifiable information about consumers.

It's About Data Protection

The overarching obligation for businesses in this area should not be characterized as preserving a customer's privacy. Privacy is too broad and too subjective a concept for companies to deal with. An individual's perception of his/her right of privacy scans a wide spectrum of rights, ranging from the right not to be bothered by telemarketers during dinner, to the right to have an abortion.[\[5\]](#) Given the breadth of this issue and the emotions that it raises, businesses cannot, per se, be in the business of protecting a consumer's right of privacy.[\[6\]](#)

The issue is more properly framed as one of data protection. While Americans may not always want to admit it, the Europeans have it right on this one. The now famous (or infamous) 1995 European Union Directive controls the "processing of data," which is a component of an individual's overall right of privacy.[\[7\]](#) After all, the movement of data is a concept that a business can effectively address: who can collect information, who controls the use of it and how may it be distributed? Those are questions that American businesses and their regulators can understand and to which they can respond.

The Frictionless Society: Whose Information Is It?

So why has the issue of data protection come into such sharp focus in the last few years? I believe that the successful growth of the Internet for commercial purposes has created the momentum behind this issue by removing the "friction" in the data collection and distribution system. In short, the friction, which used to make it clumsy and expensive to collect and transmit paper documents, and even electronic documents on proprietary systems, has been eliminated by Internet technology. So, now, a keystroke may be the triggering event that packages and dispatches information about an individual or group of individuals to every corner of the planet. This frictionless environment has resulted in a "whose information is it anyway?" syndrome. Since information can now be collected and distributed at the speed of light, data has become much

more valuable, and its use or abuse much more powerful and frightening to those who are the subjects of the data. Therefore, now more than ever before, political and economic power derives from the control or “ownership” of data.

It is critical to recognize that as we sit here in the year 2001, our legal system has not arrived at a consensus on a fundamental legal question that affects the issues we are grappling with: “Who owns the data about an individual?” That, after all, is what the current controversy is really about. Those who argue that no one should be able to collect, use or distribute information about them without their permission, are essentially saying that they own the data about themselves, no matter how it is created. They want to control the use and distribution of it, or at least share in the profits that are derived from the commercialization of such data. After all, many people seem to be willing to barter information about themselves in return for something of value. Certainly, this is the principle that supports those who would argue that the distribution of personal data for purposes other than that for which it was collected should occur only when someone “opts in” to a data collection system.

Said in a more legalistic way, is the data about us a “commodity” to which property rights can attach, and if so, whose rights attach? When a consumer fills out the warranty card for a new toaster or DVD player and volunteers information about themselves to the manufacturer, the law does not generally tell us who owns that data. That is the fundamental legal question, which perhaps advocates from neither side really want expressly answered, unless they can be assured that the answer is a complete affirmation of their position.^[8] The middle ground between those who would argue that such data belongs to the businesses that collect it, and those who believe that it belongs to the individual who provided it, is a policy that requires businesses to announce the means of collection, how the data will be used both internally and externally and then adhere to their self-imposed parameters of conduct.^[9]

But, let’s not forget Scott McNealey’s point. Data about consumers has long been unleashed and used for a variety of commercial purposes, and getting that toothpaste back in the tube is a complex exercise. McNealey’s comments do, indeed, frame the issue for us. The question is not how we can restrict the collection, use and distribution of data so that databases are not created that pose a threat to the well-being of people. Those databases are already in existence and are not likely to be eradicated. The issue is how to prevent the “abuse” of that information and those databases.

The balancing of interests here gets very difficult. If businesses are not permitted to use the data that they collect on the purchasing habits of their customers to streamline their own marketing, ordering, shipping and distribution operations, there may be a loss of efficiency. Indeed, economic theory tells us that if our laws try to affect the collection and legitimate use of information, there may be significant economic impacts on the business environment.^[10] In short, there has been a high level of information transparency in the American economy that appears to have lubricated it and provided a certain level of efficiency. To the extent that laws seek to remove that transparency from the system, it seems reasonable to assume that the increased uncertainty in the system will require

businesses to pay more to achieve the same results. That is not to say that information should not be protected. It is to suggest that there is a balancing of factors that must occur.

Dealing with the Practical Problems of Data Protection

There are dozens of federal laws, numerous state laws, and a growing number of international laws^[11] that purport to either restrict the collection and use of data, or protect some right in the confidentiality of the data. The most comprehensive private sector directed data protection was recently enacted in Title V of the Gramm-Leach-Bliley Act.^[12] But, dozens of other federal laws bear on the topic, including the Fair Credit Reporting Act,^[13] the Right to Financial Privacy Act,^[14] the Electronic Communications Privacy Act,^[15] the Computer Fraud and Abuse Act,^[16] the Privacy Act of 1974,^[17] the Driver's Privacy Protection Act,^[18] and the Video Privacy Protection Act.^[19] Yet, there is no clear, private right of action regarding one's financial privacy in federal law.^[20]

There are still many business sectors that are generally not subject to federal or state law requirements regarding the handling of customer data. However, as a matter of evolving industry customs and practices, a wide range of companies, particularly those that have embraced electronic commerce and the Internet, have voluntarily adopted data protection policies. Where companies have taken this approach, they must ensure that their "data protection" policies are scrupulously followed throughout the business. But, this, as you may already know, is easier said than done, particularly in large, global companies that have hundreds of subsidiaries and divisions. This will require, among other things, an enormous training effort throughout the company. The data about a customer will, in some sense, need to be treated as military secrets, even if the punishment for disclosure differs.

But, permit me to predict the obvious: right or wrong, more and more laws dealing with data protection will be enacted on every level in every country, particularly in the absence of a convincing business case regarding the benefits of data collection. That will put a premium on the operational benefits of understanding (i) where data comes from at the point that it reaches the company, (ii) who has control of it while it is in the company, (iii) who controls how it is used and distributed, (iv) where it goes when it leaves the company, and (v) what restrictions and monitoring will apply with regard to third parties. In short, to get their arms around this issue, companies will need to create data flow charts and inventory lists which track the data throughout the company, from development to distribution or dissipation. While it may be easy to say this, it will be enormously difficult to do. Even more perplexing is what happens to data after the company no longer has sole control of it, for example, when it becomes the principal asset of a company in bankruptcy.^[21]

Data Tagging: "You're It!"

But this is only the tip of the informational iceberg. The only way that companies will be able to comply with the plethora of new data protection laws is to develop sophisticated technological "tagging" systems. Data will have been categorized in various different ways depending on how the company derived it

and how the consumer wishes it to be used. So, for example, a company may have data that was volunteered (e.g., a loan application submitted by the customer), experiential data (e.g., a customer's credit history) purchased (e.g., from credit bureaus), or collected from a consumer's Internet surfing habits (e.g., the use of cookies to track customer preferences). And, most recently, the data that a company may have might come from the data banks of its competitors (e.g., screen scraping).

All this data may have been collected subject to different privacy policies, and the consumer may decide to opt-out with respect to the use of some information for some purposes, or opt-in with respect to other situations. Add the fact that there is nothing that prevents a consumer from changing his or her mind periodically about opt-outs and opt-ins, or that they may choose to do partial opt-outs or opt-ins, and it very quickly becomes apparent that data tagging is a monumental technological challenge.^[22] Translation: a significant new cost that businesses will have to incur.

Use Versus Abuse

It is only after you have thought through these issues in a real live corporate setting and tried to develop systems to deal with them and satisfy the law that you begin to understand that there is a cost to over-regulating in this area. Perhaps it is as significant as under regulating in an electronic environment where data may be up for grabs. But, unless we strive to maintain the difficult and complex balance that the data protection issue requires, we may create an environment where compliance is just not practical or possible given the way that business is conducted in this country.

Should the inevitable regulation of data transmission, coming as it does in the middle of the information game, seek to affect every aspect of the collection and use of it? Or, should it attempt to modify, as efficiently as possible, a system that has proven generally to be fair, and regulate toward the elimination of data abuse? In the latter category, data abuse, I include the improper use^[23] of personally identifiable information: (i) for financial gain; (ii) discriminatory purposes; or (iii) impersonation.

The problem with the approach that attempts to prevent abuse is that electronic information does not move only linearly in a static fashion. Today, data is constantly in motion, so companies both receive and dispense data in geometrically compounding fashions. So while data may be collected for a legitimate business purpose, unless its distribution is controlled, it can easily end up in the hands of someone who has what a consumer believes is an improper intent with regard to it. In fact, in this constantly moving world of information, it seems reasonable to expect that data laundering is likely to become a more prevalent problem as unscrupulous individuals and illegitimate businesses move improperly acquired information into the legitimate commercial flow of data. Does that mean that the possibility of improper distribution of data suggests that the individual should always control the right of distribution?

The Rubicon of Data Aggregation

All of these difficult issues seem to collide in the practice known as data aggregation or screen scraping. Here, one entity provides the individual with a

single website where all of his or her financial or other specialized data is maintained. The practice is generally described politely as “aggregation” when the data hosts give their permission, and “screen scraping” when they are not consulted prior to the data being collected and reassembled elsewhere.^[24] This latter practice raises interesting issues under various computer and intellectual property laws. How is it that one company can enter the computer data base of another and collect information about a customer, display it on a page it maintains, and then perhaps, add certain amounts of functionality to permit the consumer to conduct transactions from the aggregator’s site?^[25] But, then again, isn’t the aggregator just an agent for the consumer who could, given the time, do the same thing with the data?^[26] The complex legal and business issues in this tri-partite relationship between the consumer, data aggregator and data provider will inevitably be resolved through agreements, convention, technology or law, simply because data aggregation and the future that it portends benefits all of these parties.

Technological developments which facilitate data aggregation and innovative products like it underscore the way that technology and the law regarding data protection are clashing. Remember, all of the information that is aggregated has come from companies who themselves collected it pursuant to a privacy policy that had been disclosed to the consumer. And much of that information may have been provided on an opt-out basis, which is not dissipated by the fact that the data moves into the hands of a new entity, notwithstanding the consumer’s acquiescence. Clearly, aggregators will have to provide their own preemptive agreements with consumers to dictate the principles upon which they can collect and use this derivative data, but the history of the Internet is that technology multiplies issues because of the efficient distribution models that it creates.

The Battle Plan

In order to begin addressing the enormous business, social, operational and legal issues confronting businesses by virtue of the development of data protection laws and customs, companies need to have a defined battle plan. That plan should be based upon and include:

1. A clear understanding of the laws and regulations that apply, under what circumstance they apply, and what the global jurisdictional implications of such applications are.
2. The creation of a company philosophy with respect to the collection, control and distribution of customer data that is consistent with its corporate culture and capabilities.
3. The development of a comprehensive inventory of all methods by which nonpublic personal information is obtained.
4. An understanding of all means, channels and circumstances by which nonpublic personal information is disclosed to third parties or to affiliates.

5. Whether each disclosure to a third party or affiliate is subject to federal, state or international law, and opt-out or opt-in requirements.
6. A compilation of the actions, such as computer reprogramming and changes in operational policies, necessary to effectuate and modify, as necessary, the use of data consistent with the options that customers have by law, contract or policy.
7. The creation and modification of agreements with third party vendors, data processors or technology partners, which have access to nonpublic customer information, so that there is a consistent use of data at all points in the chain of collection, control and distribution.
8. A current evaluation and listing of the information-sharing relationships with affiliates, particularly with respect to the affiliate sharing opt-out notification required under the Fair Credit Reporting Act.
9. Procedures that assure that affiliates will comply with applicable limitations on the use of nonpublic personal information that is provided to them by the company.
10. An understanding of the types of “customer” and “consumer” relationships that trigger disclosure, record keeping and substantive obligations on the company’s part.
11. Legal and technological procedures as to how data protection compliance will be assured in each type of relationship and each type of delivery channel.
12. A reevaluation of data protection strategies, particularly in light of the increasing threat of unauthorized third party intrusion.
13. Regular monitoring of legislative developments and participation in the process.
14. A clear and consistent offensive and defensive approach to data aggregation.
15. The centralization of responsibility for company-wide compliance and responsiveness.

Conclusion

What is it that businesses can do to achieve a sense of balance as the data protection phenomenon unfolds? So far, they have not done a great job at making the case for the economic, operational and marketing benefits that accrue to consumers through the legitimate collection and use of personally

identifiable data. Until that occurs, it will be difficult to explain the costs and disadvantages that consumers will incur as data protection laws increase.

* _____
Thomas P. Vartanian is a Partner in the Washington office of the New York law firm Fried, Frank, Harris, Shriver & Jacobson and head of its Electronic Commerce and Technology Transactions Group www.ffhsj.com/bancmail/bancpage.htm. He is an Adjunct Professor in the graduate law program at Georgetown University Law Center, where he teaches a course on 21st Century Banking issues. Mr. Vartanian is also Chair of the American Bar Association's Committee on Cyberspace Law. He is co-author of two recently published books entitled *21st Century Money, Banking & Commerce* and *The Management of Risks Created by Internet-Initiated Value Transfers*.

[1] In 1890, Samuel Warren and Louis Brandeis first identified the right to privacy. They concluded that "[i]t is the unwarranted invasion of privacy which is reprehended, and to be, so far as possible, prevented." Warren & Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 213 (1890). Common law privacy gradually evolved to mean the right to enjoy life -- "the right to be left alone." *Id.* at 215.

[2] Recent developments suggest that information collection and sharing has reached the next level. A group of technology companies, including IBM, and their financial services partners have introduced an Internet standard that gives companies a common platform for exchanging information about customers. *A New Privacy Flash Point, Courtesy of IBM*, Am. Banker, Jan. 3, 2001, at 1.

[3] See John Markoff, *Growing Incompatibility Issue: Computers and User Privacy*, N.Y. Times, March 3, 1999, at A1.

[4] Unfortunately, most statutes, such Title V of the Gramm-Leach-Bliley Act, use the word "privacy" when they really mean to deal with "data protection." Gramm-Leach-Bliley Act, Pub. L. No. 106-102, tit. V, 113 Stat. 1338, 1436 (1999).

[5] See *U.S. West v. Federal Comm. Comm'n*, where the Tenth Circuit said:

The concept of privacy, though, is multi-faceted. Indeed, one can apply the moniker of a privacy interest to several understandings of privacy, such as the right to have sufficient moral freedom to exercise full individual autonomy, the right of an individual to define who he or she is by controlling access to information about him or herself, and the right of an individual to solitude, secrecy, and anonymity. See Fred H. Cate, *Privacy in the Information Age* 19-22 (1977); Joseph L. Rosenbaum, *Privacy on the Internet: Whose Information Is It Anyway?*, 38 *Jurimetrics J.* 565-67 (1998). (Footnote omitted.)

182 F.3d 1224, 1234 (10th Cir. 1999).

[6] Indeed, the Tenth Circuit stated in *U.S. West* that "privacy is not an absolute good, because it imposes real costs on society." 182 F.3d at 1235.

[7] EU Directive 95-46 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Oct. 24, 1995).

[8] The *U.S. West* case held that companies have a property right in records created in the course of their business and that certain uses of it are constitutionally protected.

[9] This, in fact, has been the basis for several enforcement actions that have been brought. In 1998, the FTC filed the first Internet privacy action against GeoCities for allegedly misrepresenting how it planned to use information it collected and for violating its own privacy policies. See *GeoCities, Inc.*, Docket No. C-3849 (Aug. 1998) (consent order Feb. 12, 1999). At the state level, the Minnesota Attorney General filed a complaint against U.S. Bank, N.A., and others, alleging that the bank violated the Fair Credit Reporting Act and state law with regard to the bank's alleged sale of customer information to a telemarketing firm that markets membership service programs. See *Hatch v. U.S. Bank, N.A.* C.A. No. 99-872 adm/ajb (D. Minn. filed June 9, 1999) (stipulation of settlement June 30, 1999).

[10] As noted in *U.S. West*, Professor Cate lists a number of costs privacy imposes. Privacy facilitates the dissemination of false information; protects the withholding of relevant true information, such as when an employee fails to disclose a medical condition that would affect job performance; interferes with the collection, organization and storage of information that can assist businesses in making rapid, informed decisions and efficiently marketing products; and can interfere with the public's ability to access information needed to protect people. In short, privacy may lead to reduced productivity, higher prices and lost opportunities. *U.S. West, supra* note 5, at 1248 n.7; see also, Cate, *supra* note 5, at 28-30. See also Peter Swire, *Markets, Self-Regulation and Government Enforcement in the Protection of Personal Privacy Information* (1997).

[11] In addition to the EU, Canada has recently adopted extensive data protection laws. Personal Information and Electronics Document Act, C-6 (1999).

[12] Gramm-Leach-Bliley Act, *supra* note 4.

[13] 15 U.S.C. §§ 1681-1681u.

[14] 12 U.S.C. §§ 3401-3422.

[15] 18 U.S.C. §§ 2510-2521, 2701-2711.

[16] 18 U.S.C. § 1030.

[17] 5 U.S.C. § 552a.

[18] 18 U.S.C. §§ 2721-2725.

[19] 18 U.S.C. §§ 2710-2711.

[20] More than a dozen states provide for a common law right of privacy that attaches to an individual's financial records of financial institutions. See Donald A. Doheny, Sr. & Graydon John Forrer, *Electronic Access to Account Information and Financial Privacy*, 109 *Banking L.J.* 436 (1992); Roy Elbert Huhs, Jr., *To Disclose or Not to Disclose Customer Records*, 108 *Banking L.J.* 30 (1991); Thomas C. Russler & Steven H. Epstein, *Disclosure of Customer Information to Third Parties: When Is the Bank Liable?*, 111 *Banking L.J.* 258

(1994). Increasingly, banks have felt an increased ethical, as well as legal, obligation to safeguard their customers' financial records. See Cheryl B. Preston, *Honor Among Bankers: Ethics in the Exchange of Commercial Credit Information and the Protection of Customer Interests*, 40 Kan. L. Rev. 943, 970-71 (1992).

[21] Consider, for example, the Federal Trade Commission's efforts to prevent data collected under a restrictive privacy policy by Toysmart.com from being sold in connection with its bankruptcy. *FTC v. Toysmart.com*, C.A. No. 00-11341-RGS (D. Mass. filed July 10, 2000).

[22] Changes in consumer choices after data has already been transmitted are likely to create unique problems.

[23] The definition of "improper use" is, of course, what the controversy is all about.

[24] Fried, Frank, Harris, Shriver & Jacobson, *Screen Scrapers Hit Nerve at Financial Institutions*, 21st Century Money, Banking & Commerce Alert No. 2000-01-19 (Jan. 19, 2000), available at www.ffhsj.com/bancmail/banpage.htm.

[25] These issues were raised in a lawsuit filed in December 1999 by First Union Bancorporation against a firm that was engaged in aggregation. The lawsuit was dismissed several months later when the parties reached a settlement. It raised issues ranging from the conversion of intellectual property to violations of the Computer Fraud & Abuse Act. *First Union Corp. v. Secure Commerce*, C.A. No. 3:99CV519H (W.D. N.C. filed Dec. 30, 2000). In addition, *EBay v. Bidder's Edge*, has revised the theory of trespass against chattel with regard to the use of information from third party sites. *EBay, Inc. v. Bidder's Edge, Inc.*, C.A. No. C-99-21200RMW (N.D. Calif. May 24, 2000).

[26] In this regard, the aggregator may ask the consumer to agree to its appointment as agent or "legal representative" to collect the information on behalf of or and as the consumer. Aggregators may require consumers to warrant that the practice is permissible and assume all responsibility if it is not. Finally, some companies ask the consumer to execute a power of attorney (which can now be done electronically) in favor of the aggregator.