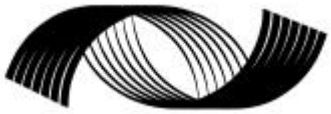


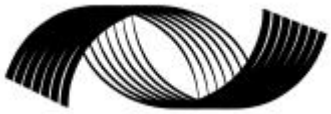
J O I N T C E N T E R
AEI-BROOKINGS JOINT CENTER FOR REGULATORY STUDIES

Balancing Costs and Benefits of New Privacy Mandates

Robert E. Litan

Working Paper 99-3

April 1999



J O I N T C E N T E R

In response to growing concerns about understanding the impact of regulation on consumers, business, and government, the American Enterprise Institute and the Brookings Institution have established the new AEI-Brookings Joint Center for Regulatory Studies. The primary purpose of the center is to hold lawmakers and regulators more accountable by providing thoughtful, objective analysis of existing regulatory programs and new regulatory proposals. The Joint Center will build on AEI's and Brookings's impressive body of work over the past three decades that has evaluated the economic impact of regulation and offered constructive suggestions for implementing reforms to enhance productivity and consumer welfare. The views in Joint Center publications are those of the authors and do not necessarily reflect the views of the staff, council of academic advisers, or fellows.

Abstract

Growing concerns about privacy have prompted policy makers to give more attention to buttressing existing statutory privacy protections. In this article, I lay out the case for taking a balanced approach to new legislation: one that weighs the benefits of the free flow of information against possible threats to privacy in certain circumstances. Using this balancing framework, I suggest that narrowly targeted legislation aimed at enhancing protections of sensitive medical and financial information is appropriate. In addition, there is a case for a limited across-the-board requirement that merchants–whether on or off line–notify consumers of their information policies and afford them an opportunity to opt out of having personally identifiable data forwarded to third parties for marketing purposes.

Balancing Costs and Benefits Of New Privacy Mandates

Robert E. Litan

We are said to live in an "information age." If so, it is not necessarily because more "information" is collected, analyzed, used or generated today than in earlier times–although that certainly is true. Instead, it is because computers, fiber optic cables and the Internet in particular enable information to be transferred much more quickly from one location to another and to be found with more far more ease than before.

The advances in information technology have been widely hailed as ushering forth a virtual revolution in the way people relate to one another and conduct business. But the information age also has unleashed a vigorous debate in this country and abroad over who can gain access to and use certain types of information–personal data about one's finances, medical history, shopping habits, and the like–and under what circumstances. Two widely respected surveys recently documented the strong public interest in privacy: one reported that 82 percent of Americans are concerned that they have "lost all control" over how their personal information is used by companies with whom they conduct business,[1] while the other indicated that 81 percent of Internet users have concerns about potential threats to their personal privacy while on-line.[2]

The rising concerns about privacy have been translated into policy in the U.S. and abroad. In 1998, federal laws were enacted that criminalized "identification theft" and fraud, protected children's on-line privacy, prohibited the federal government from requiring social security numbers to be placed on drivers' licenses, and prohibited the assignment of unique identifiers to health records. Many states added protections affecting data collected by health care providers, financial services companies, direct marketers, telecommunications companies, and on-line services. Meanwhile, in October 1998 the European Union began formally implementing its Privacy Directive, which not only mandates strong privacy protection for European citizens, but threatens to prohibit transfers of personal information about Europeans to other countries, such as the United

1. Harris & Associates and Westin (1998a).
2. Harris & Associates and Westin (1998b).

States, which various EU officials have stated lacks "adequate" protection of personal privacy.[3]

The U.S. Congress appears not to be finished considering privacy legislation. Left over from last session, and already showing signs of life in this session, are proposals for regulating on-line privacy practices, which would affect all types of businesses. Other initiatives target specific sectors–such as health care and financial institutions–and would impose new mandates relating to what uses firms in these sectors can make of the information they collect.

In this article, I suggest that policy makers should consider new privacy-related proposals within the same framework that has guided U.S. policy in this area over the past several decades: one that *balances* privacy interests on a case-by-case basis against the importance of ensuring the free flow of information. Indeed, the media have been instrumental in helping to shape public policies toward privacy. As discussed further below, recent examples include the exposure by the media of the sale of personal information by state motor vehicle bureaus without consumer consent and sale of prescription information by drug stores without the knowledge of their customers.

Using this balancing framework, I argue here that there is a case for additional, but narrowly targeted legislation aimed at enhancing protections of sensitive medical and financial information. In addition, there is a case for a limited across-the-board requirement that merchants–whether on or off line–notify consumers of their information policies and afford them an opportunity to opt out of having personally identifiable data forwarded to third parties for marketing purposes. Such targeted measures would help promote consumers' confidence in dealing with business, and like the Fair Credit Reporting Act (FCRA) and certain other privacy legislation already enacted, help expand retail markets (especially electronic commerce) and thus generate a "win-win" for *both* consumers and business.

Existing Privacy Protections in the United States

3. For a thorough study of the implications of this Directive, especially if the EU decides that one or more sectors of the U.S. economy lack adequate privacy protection, see Swire and Litan, (1998).

Few would dispute the ability of sellers to use information they may collect from buyers to complete transactions or provide services. For example, banks need to know the payees and amounts of checks in order to keep track of customers' deposit balances. Medical providers need to know highly sensitive health information in order to deliver quality health care.

The information sellers collect from buyers also can be and often is very valuable to other organizations that want to target their marketing to individuals with certain buying habits. Similarly, customer data can be useful to other entities in screening the credit-worthiness of potential buyers or borrowers. Indeed, the customer information that firms acquire in the course of doing business can be one of the most valuable assets on their balance sheets, which some may closely guard while others may sell or share with third parties, subject to applicable constraints. For example, U.S. financial service firms are required by law or regulation to protect the confidentiality of customer information. In addition, access to customer bases can be especially critical for smaller businesses, which cannot afford the expenses of mass marketing, but instead seek to target their marketing to groups of consumers whose names and address are possible to assemble only if customer information can be easily exchanged.

The debate over privacy arises, however, because many individuals may not want information about them so freely transmitted to third parties without their consent. What should the law say about whether and how personal data collected for one purpose may be transferred to third parties for other purposes? Should it make a difference what kind of information it is, what types of third parties gain access to it, and what those other purposes might be?

U.S. law at both the federal and state levels historically has taken a balanced approach to addressing these questions, adding legal protections over time where policy makers judge the benefits of legislating outweigh the costs of not doing so. As a result, explicit legal privacy protections here are selective and are aimed at specific types of sensitive information and parties who may acquire it in the normal course of conducting business.

Chart 1 summarizes the provisions of the substantial number of privacy-related federal statutes that are already on the books. These protections cover financial

information collected by credit reporting agencies and financial institutions, histories of video rentals and cable television subscriptions (which may contain sensitive information about personal viewing habits), abuses by telemarketers, and certain information collected by the government. Most recently, the Congress enacted legislation to make it a criminal offense to steal an individual's "identity" by gathering his or her personal information (such as a credit card or social security number). The new identity protections buttress preexisting provisions granting victims the right to civil remedies against financial institutions that improperly release financial records.

Federal privacy laws are reinforced or supplemented by state laws. A number of state constitutions contain express provisions protecting privacy. State common law has developed protections relating to financial information (especially account balances). Some state privacy statutes deal with specific subjects, regulating information disclosure by credit reporting agencies and credit card companies and requiring consumer consent relating to electronic funds transfers.

A common theme that implicitly runs through both the federal and state laws is that the protections are targeted at specific types of information and providers where a balancing test can be reasonably construed to warrant government intervention. For example, the costs of allowing individuals to gain access to their credit bureau files clearly would seem to pale compared to the harm that incorrect entries can cause affected individuals, who may be denied credit as a result. Current law understandably, therefore, allows consumers access to information held about them by credit bureaus and the opportunity to correct any mistakes. Similar logic supports other statutes that punish identity theft and limit the disclosure of sensitive television viewing patterns.

A balancing test produces a different outcome in other instances where regulation is not present. For example, a department store data base that contains the wrong addresses of some consumers, or even incorrect data regarding their purchasing patterns, would seem to pose relatively little risk of harm to consumers when used by the store itself, or even if shared with third parties. The worst that might happen is that some consumers would receive unwelcome mail or telephone solicitations (which by law they can stop), while others would be denied that opportunity (and thus conceivably miss out on a particular "good deal" that they otherwise might enjoy). Against these potential

harms is balanced the potential benefit to third parties of being able to use the data base (perhaps with some errors) to finely tune its marketing campaign and thus reduce its marketing costs, a result that benefits both marketers and consumers alike. Thus, the fact that current law does not require affirmative customer consent to the sale of such data also seems appropriate.

Is There A Need for Additional Government-Mandated Protection?

The balancing approach is not and should not be static. As technology and markets change, new problems emerge, shifting the balance between the costs and benefits of adopting new mandates. The calls for new privacy legislation or regulation have concentrated on three areas.

Medical Data: Medical information represents one of the most sensitive categories of personally identifiable data. Indeed, the law carves out a special privilege in litigation for information conveyed by patients to their physicians. To be sure, the sale of health information to pharmaceutical and possibly other health related companies might facilitate the marketing of health products to consumers. But these benefits seem small in relation to the large costs that many individuals could suffer by having their health status and sexual preferences, among other types of sensitive data, widely distributed. It is only appropriate, therefore, that the law restrict the use of medical information by health care providers–doctors, hospitals, HMOs and the like–who obtain it in the normal course of providing treatment and those who require such information to process payments and effect reimbursement.

Congress has been considering proposals to do precisely that: to ensure that personally identifiable health data cannot be sold or transferred to third parties without the patient's explicit consent. Senator Robert Bennett, in particular, has played a leading role in the Congress in crafting medical privacy legislation (S. 2609 in the last Congressional session). In his 1999 State of the Union address President Clinton called for Congress to act in this area. It is conceivable that medical privacy legislation could get mixed with the more controversial proposal by the Administration to legislate a

"patient bill of rights." If so, and if no compromise is reached on the broader bill, Americans deserve at least a more targeted bill aimed at medical privacy.

Financial Data: Despite the numerous provisions in current law that already protect sensitive financial data, two new concerns have arisen.

On one issue, there is clear consensus that new legislation is needed. Closely related to the problem of identity theft is that some individuals or organizations apparently have found ways to obtain data from financial institutions under "false pretenses"–claiming to be a customer when in fact that is not the case. Representative James Leach, the Chairman of the House Banking Committee, has introduced legislation this year (H.R. 30) making it a criminal offense to gain financial information by false pretense and granting civil enforcement authority to the Federal Trade Commission and the banking regulatory agencies. Not waiting for such legislation to pass, banking regulators last year notified banks that they would review measures they have taken to minimize the chances that their customers could be victims of false pretense data gathering.

Congress also has displayed significant interest in information sharing by financial institutions. Legislation introduced by Senator Paul Sarbanes (S. 187) would give customers the opportunity to ask their financial institutions not to disclose to affiliates certain financial information not already covered by the opt out requirements of the FCRA: deposit account balances, transactions histories (including amounts and dates), maturity dates of certificates of deposit, securities holdings and insurance.[4] Consumers would have to *opt in*–that is, provide their affirmative consent–for financial institutions to share this information with third parties that are not affiliates. The Sarbanes bill would also require financial institutions to notify consumers of their policies on information disclosure, to give consumers access to information held about them, and an opportunity to verify its accuracy.

Financial modernization legislation adopted by House Banking Committee in March 1999 takes a more limited approach to mandating financial privacy protection. This legislation requires financial institutions to notify consumers of their privacy

4. S. 187 is co-sponsored by Senators Dodd, Bryan, Leahy, Edwards and Hollings.

policies, while prohibiting them from sharing medical data with affiliates or with outsiders without the consumer's consent. The latter provision essentially would codify the decision by the Federal Reserve Board approving the Citibank-Travelers merger on the condition that Travelers not share medical data with the rest of the organization. In late March, the Comptroller of the Currency issued guidelines which closely track the approach adopted by the House Banking Committee, while affording banks flexibility in deciding how to provide the notices and opportunities for consumers to opt out.

In considering these proposals, it is important to bear in mind that the Fair Credit Reporting Act already tightly regulates the data held by credit reporting agencies and requires financial institutions to offer the opportunity to their customers to opt out of having their credit-related financial information shared with affiliates. The Electronic Funds Transfer Act, meanwhile, requires banks to notify their customers of the circumstances under which their account information will be disclosed to third parties. As to rights of access, current law already requires banks to provide account information to customers so they can verify it. Indeed, what consumer would do business with a bank or a securities firm, for example, that did not routinely mail out statements showing their customers' funds balances?

Policy makers should also be aware of consumer benefits of various types of information sharing before rushing to legislate new restrictions. When banks share customer data with their affiliates, they facilitate the delivery of bundled services to consumers: comprehensive account statements, quicker loan processing, and so forth. In addition, information sharing allows diversified financial organizations to spread marketing costs across multiple products and services. In competitive markets, lower costs lead to lower prices. Consumers also benefit when banks share information about them with unaffiliated third parties, which can then target marketing campaigns to those consumers most likely to be interested in purchasing particular products or services. Furthermore, banks often disclose information to third parties–affiliates and non-affiliates–to facilitate the detection of and protection against fraud. Indeed, individuals who are most likely to defraud a third party are strong candidates for opting out or refusing to opt in to information sharing by the bank.

At bottom, therefore, Congress should proceed cautiously before mandating new financial privacy protections. The House financial modernization bill seems to strike a sensible balance, requiring notice and limiting the disclosure of sensitive medical data. If Congress wants to go further by legislating an opt-out consent provision for information sharing among affiliates, it should be limited only to data used for *marketing* purposes (and thus not frustrate the workings of credit markets or the ability of companies to detect and combat fraud).

***E-Commerce*:** Privacy concerns have been perhaps most visible in connection with the use of the Internet. In June 1998, the Federal Trade Commission reported the results of its survey of commercial web sites and found that only a small minority even informed potential consumers of their privacy policies. Shortly thereafter, the Commission, the Clinton Administration, and several members of Congress warned private industry that unless it soon developed a workable system of self-regulation that had enforcement "teeth," legislation mandating privacy protections could follow.

Although some legislators have expressed disappointment with the speed of industry's reaction to these warnings, the reality is that much has happened since the release of the FTC's survey. Many more web sites, especially the large commercial sites, now have privacy policies visibly displayed (or hyperlinks to the same effect) on their home pages–a fact that can be verified by going to the ".com" sites of many widely recognized banks, securities firms and insurance companies, retailers and other service providers. The FTC has authorized a new survey of websites which should confirm this to be the case.

Both the private sector and the Clinton Adminstration support a self-regulatory approach to on-line privacy protection. Nonetheless, the Administration is urging industry to develop meaningful ways to provide consumers with more information about companies' privacy practices, greater choice about how information will be used, and access to personal information. The business community also is being urged to develop ways to protect the security of information and the integrity of the data they collect, as well as to enforce privacy policies.

The private sector has responded with a variety of self-regulatory initiatives in an attempt to forestall potentially onerous legislation or regulation it believes could impede the growth of e-commerce. For example, the Online Privacy Alliance of companies and trade associations has issued privacy guidelines to its members. The Better Business Bureau has developed its BBB Online privacy program to verify, monitor and review company privacy policies and practices, to provide a way of resolving consumer disputes, to award web page seals to companies that comply with good privacy policies, and to provide education programs. The banking industry, in particular, has made great strides in providing notice to Net users of how information they provide will be used by their banks.

The term "self-regulatory" is actually somewhat of a misnomer, because in fact, all privacy representations of alliances like this as well as those of individual firms are subject to enforcement by agencies of the federal and state governments under existing law. The FTC, for example, has authority to sue companies for "unfair and deceptive" practices if they do not adhere to their announced policies. The FTC has used this authority in the case of Geocities (which advertised its unwillingness to sell customer data to third parties and then went ahead and did it anyway). States can also sue under similar theories.

Cynics may say that companies have joined self-regulatory efforts only because they fear the enactment of formal regulation or legislation instead. To be sure, this has been one motivation for some companies' participation. But equally, if not more important, is the fact that it is in the *self-interest* of companies doing business on-line to announce and adhere to privacy policies that serve the interests of consumers. Individuals who fear using the Net because the information they supply to on-line dealers will be transmitted freely to other parties will not buy the products and services that on-line merchants want to sell. Companies having an interest in making money clearly have an economic incentive to respond to these fears.

That many seem to have taken their time in doing so is, in part, a reflection of the fact that just twelve months ago e-commerce was very much a novelty. Many companies did not expect it to take off as fast as it has. Now that many consumers are flocking to the Net to conduct business, companies realize the importance of having a major web-

presence while consumers increasingly are aware of the importance of doing business only with firms that have a clearly announced privacy policy. In short, the growth of e-commerce and the increased attention firms are paying to on-line privacy protection are mutually reinforcing trends.

The importance of the media as an on-line privacy watchdog also must be underscored. Newspaper and television stories can place a powerful spotlight on practices that are widely regarded to threaten privacy. When that has happened, these practices have been quickly changed. For example, Lexis/Nexis quickly abandoned its plan to introduce its P-trak locator service (which provided such personal information as mothers' maiden name to subscribers) after the initiative was made public. The same was true when the media revealed that AOL was planning to release its customer lists to telephone marketers (despite earlier assurances not to do so) and when Giant Food and CVS announced plans to sell to third parties drug prescription data provided by customers. Most recently, faced with a potential consumer boycott of its products, Intel immediately backed down from introducing a new version of its pentium computer chip that would have tracked the websites visited by computer users. The media have also disciplined governments as well. During the past few months, authorities in Colorado, Florida and South Carolina backtracked on plans to sell drivers' license photos after they became public and residents flooded state offices with complaints.

The media have several virtues as enforcers of privacy standards relative to government regulation. Publicity can and does lead to swift justice: often company policies change within a day or two of when information about a particular practice becomes public. If companies do not change their practices as a result of news stories, then that outcome provides an equally valuable market test of what the public is willing to tolerate. In either case, the results become evident far more rapidly than is the case with agency enforcement actions, especially given due process requirements that must be followed before violations can be remedied. To put it mildly, the current legal process is hardly well adapted to the on-line environment where "Internet time"–measured in days or even hours–is the governing standard.

Nonetheless, because so many consumers–even those who are already familiar with the Net–remain concerned about their privacy, it would be in the on-line business

community's own self interest to address those concerns with a simple statute requiring notice and opt out for use of information captured online for marketing purposes (indeed, as suggested below, there is a case for extending such a requirement to "off-line" merchants as well). The FTC can be charged with enforcing such a simple requirement with civil penalties.

A notice and opt out statute could easily do for on-line commerce what the statutory $50 limit on credit card liability for fraudulent use or theft of credit cards did for the credit card industry. In the case of credit cards, limited liability gave consumers confidence that they could use their cards without fear of ending up with huge liabilities. By the same token, if all consumers knew how on-line merchants would use their personal information and if consumers could opt out of having their name and other data forwarded to third parties for marketing purposes, many more consumers would gain confidence in using the Net for commercial transactions.

Why Not Go Further?

Rather than continue to regulate information disclosure in a selective and incremental fashion–as has been the case in the United States so far–some have argued that the U.S. law privacy law should be revised comprehensively, requiring among other things, mandatory consumer consent before any personal information may be disclosed to third parties and unqualified consumer access to all information that may be held about them.

Requiring consent on an opt-in basis in all circumstances would dramatically change the way goods and services are marketed in this country, whether "on" or "off" line. The same would be true for fund-raising by charitable and public interest organizations, many of which now purchase customer lists from magazines and other organizations (commercial and non-commercial). In all of these cases, if an across-the-board opt-in requirement were in effect, organizations would have to painstakingly build solicitation lists from scratch, a task that would be prohibitively expensive for all but the very largest commercial entities in the country. One result would be to raise barriers to entry by smaller, and often more innovative, firms and organizations. Furthermore, an

across-the-board opt-in requirement could make it more difficult for companies to authenticate customers and verify account balances, and thus frustrate the ability to counteract fraud.

To be sure, some individuals may benefit from having fewer solicitations aimed at them in a mandatory opt-in regime. But many other consumers would be harmed in one of several ways. Prices for many products and services would be higher, because competition would be reduced while fraud-related and marketing costs of existing, larger firms would be higher. In addition, some consumers who now receive unsolicited material by phone or mail and act on those solicitations would not be made aware of particular products or services that might interest them.[5]

What about providing consumers with an *automatic and unqualified* right of access and an opportunity to correct information that may be held about them (as is the case in the EU)? In fact, U.S. law affords this opportunity for credit information held by credit bureaus and for deposit account and credit account information maintained by financial institutions. In addition, members of the On-Line Privacy Alliance correction have agreed to afford "reasonable"–but not automatic–means of access and "appropriate" opportunities for customers to correct data.

Given the costs of any mandatory access requirement, it is important to distinguish between "automatic" and "reasonable" access to information, as well as "unqualified" and "appropriate" opportunities to correct. Medical or sensitive financial data clearly warrant giving consumers an automatic right of access and opportunity to correct (which they do have for financial information). But as discussed earlier, it is hard to make the same case for, among other things, customer name and purchasing data held by merchants in the ordinary course of business.

In theory, it is possible that a regulatory agency could make these fine distinctions among different types of data and write rules prescribing what constitutes reasonable access and opportunity to correct for specific types of industries. But there comes a point

5. As a personal example, I am addicted to golf and discovered that by subscribing to one golf-oriented magazine, I apparently was put on the mailing list of numerous mail order catalogues and other golf magazines of which I otherwise would have been totally unaware. I have since purchased items from some of these catalogues and subscribed to other magazines as a result. Many other consumers have had similar experiences, I suspect. Otherwise, so many firms would not go to the trouble or expense of preparing and distributing these materials.

where one has to ask what is to be gained by regulatory micro-management and whether the benefits outweigh the costs of the private sector having to comply with another set of potentially detailed rules. The tradition in the United States has been to have the government step in only where there is a demonstrated demand to do so by the public and where that demand is not being satisfied sufficiently by the private sector. Before the Internet became a household word, there in fact was no groundswell for across-the-board access rights to any type of personal data held by companies. That may have changed with the increase in e-commerce, but as already noted, major on-line companies in the private sector have responded with a commitment to provide "reasonable" means of access and "appropriate" opportunities for correction of mistakes. As Geocities has discovered, these promises, in turn, are subject to enforcement by the Federal Trade Commission and the states, as well as by the media. This combination arguably is *more* effective in serving the privacy interests of individuals than relying on a single mission government agency to establish and enforce privacy standards, as is the case in Europe.

More broadly, there is a very real danger that any across-the-board privacy law could trigger unintended consequences that cannot be foreseen now but could easily emerge in particular circumstances. The events following a recent proposal by bank regulators requiring banks to investigate potential customers for nefarious backgrounds illustrate this point. This "Know Your Customer" (KYC) proposal was designed with very good intentions: to prevent banks from taking on criminals as clients, who would then use the bank to launder the proceeds of their criminal activity. Moreover, it seemed like a good idea until the regulators were flooded by thousands of comments from customers and banks fearing an invasion of their privacy. The bank regulators have since withdrawn the proposal (although banks are still required under current law to file "Suspicious Activity Reports" for activities of customers suggesting possible violations of laws or regulations). The KYC episode illustrates the dangers of implementing prematurely broad measures that can have unintended, adverse consequences.

One limited, but comprehensive federal privacy statute, however, could entail benefits that outweigh any costs (and any unintended consequences): an extension of the notice and opt out provisions already suggested for on-line firms to vendors doing business in the physical realm. The opt out opportunity would apply only to the sale or

transfer of information for marketing purposes. The FTC could be charged with suggesting ways in which the notices and opt out opportunities could be provided, much as the bank regulators have recently suggested for financial information. The legislation should make clear that the agency is to take a flexible approach, offering multiple means of compliance. The agency would also be charged with enforcing the provisions (rather than creating new private rights of action that could lead to further clogging of the courts).

In fact, many firms in this country already follow the practices that such a law would mandate. Nonetheless, there is a good case that a generic notice and opt out mandate would pass a balancing test. The costs to firms of providing notices would be small. So would the costs of opt out provisions, which typically are taken up by only small fractions of consumers given the choice. Against these rather small costs are potentially much greater benefits of providing assurances to consumers that they have some control over the information they supply to firms in the course of conducting business with them. For this reason, businesses are likely to benefit by enjoying the enhanced trust of consumers. Finally, and not insignificantly, a statute of this type should help defuse tensions that have arisen between the EU and the United States over the enforcement of the EU's Privacy Directive. A win-win-win proposition all around.

References

Louis Harris & Associates and Alan F. Westin. 1998a. *Privacy Concerns & Consumer Choice.* Washington, D.C.: Independent Survey.

———. 1998b. *E-Commerce and Privacy: What Net Users Want.* Washington, D.C.: Independent Survey.

Swire, Peter P., and Robert E. Litan. 1998. *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive.* Washington, D.C.: Brookings Institution Press.

Chart 1

Current Federal Privacy Statutes

Financial Information

Fair Credit Reporting Act of 1970	First federal act to govern information practices of credit reporting bureaus; requires financial holding companies to provide notice to consumers of disclosure policies and gives them an opportunity to opt out
1996 Amendments to the FCRA	Allows consumers to opt out of sharing of information by affiliates; prohibits institution from furnishing information to a credit reporting agency that it knows or consciously avoids knowing to be inaccurate
Fair Credit Billing Act	Creates statutory right of access to the credit file and a right to challenge the accuracy of the information contained therein
Electronic Communications Privacy Act	Protects against unauthorized interception of electronic communications
Electronic Fund Transfer Act of 1978	Requires notice by financial institutions of when and which account information will be disclosed to third parties
Fair Debt Collection Practices Act	Prohibits excessive and abusive debt collection practices, limiting access by debt collectors to debtors
The FTC Act	Requires bank supervisory agencies to establish separate divisions of consumer affairs to handle complaints about unfair and deceptive practices; also has authority for the agency to enforce an institution's disclosed privacy policy
Right to Financial Privacy Act	Gives individuals civil remedies against financial institutions that improperly grant access to their financial records
Identity Theft and Assumption Deterrence Act	Criminalizes the possession of false identification and the gathering, use and sale of personal information under false pretenses

Telemarketing

The Telephone Consumer Protection Act of 1991	Grants rulemaking authority to the FCC to issue regulations governing telephone solicitations; also allows consumers to opt out of such solicitations
The Telemarketing and Consumer Fraud and Abuse Prevention Act of 1991	Gives consumers a civil cause of action for money damages for abusive telemarketing practices. Also gives states authority to bring enforcement actions

Television and Video Rentals

Video Rental Act of 1988	Prohibits video rental stores from releasing customer rental records
The Cable Communications Policy Act of 1984	Prohibits sharing of customer data without prior consent of consumers, affords consumer inspection and correction of information that is collected

Government Use of Data

Privacy Act of 1974	Prohibits government agencies from sharing personal information with other agencies