

Committee on Banking, Housing, and Urban Affairs
of the United States Senate
Hearing on
FINANCIAL PRIVACY AND CONSUMER PROTECTION
September 19, 2002

Prepared Statement of Professor Fred H. Cate

My name is Fred Cate, and I am a professor of law and Ira C. Batman faculty fellow at the Indiana University School of Law in Bloomington, and a senior policy advisor at the Hunton & Williams Center for Information Policy Leadership. For the past 13 years, I have researched, written, and taught about information laws issues generally, and privacy law issues specifically. I directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, served as a member of the Federal Trade Commission's Advisory Committee on Online Access and Security, and currently am a visiting fellow, addressing privacy issues, at the American Enterprise Institute.

I appreciate the opportunity to testify today, and I am doing so on my own behalf. My views should not be attributed to Indiana University or to any other institution or person.

1. The Importance of Consumer Concern

Polling data, newspaper editorial pages, this summer's referendum in North Dakota, and anecdotal evidence all suggest that consumers are concerned about personal financial information and how it is accessed and used both by the government and private industry. It is important to view this concern in context.

The concern is not surprising, given the amount of press and political attention given privacy issues, the increased focus on privacy issues and the dramatic growth in privacy-related products and services by financial institutions, and the deluge of two billion or more privacy notices that financial institutions are required by federal law to mail to their customers annually.

When viewed in this context, I believe the existence of consumer concern is not only predictable but largely healthy: It tells us that consumers are paying more attention to important privacy issues, and are interested in how their privacy can be better protected. Given that many of the most effective privacy protections—especially to guard against identity theft—are the steps that individuals alone can each take individually, this new interest is critical.

2. The Absence of Consumer Action

It is also important not to lose sight of the context of consumer action—as opposed merely to polls. Under the requirements of Gramm-Leach-Bliley, by July 1,

2001, tens of thousands of financial institutions had mailed approximately two billion notices. If ever consumers would respond, this would appear to be the occasion: The notices came in an avalanche that seems likely to have attracted consumer attention, the press carried a wave of stories about the notices and about state efforts to supplement Gramm-Leach-Bliley's privacy provisions, privacy advocates lauded the opt-out opportunity and offered online services that would write opt-out requests for consumers, and the information at issue—financial information—is among the most sensitive and personal to most individuals.

Yet the response rate was negligible. The available published information indicates that fewer than 5 percent of consumers responded to the deluge of notices by opting out of having their financial information shared with third parties. For many financial institutions, the response rate was lower than 1 percent. And this appears to be consistent with response rates to other privacy-related opt-out opportunities, such as the Fair Credit Reporting Act's opt-out provisions applicable to prescreening and sharing credit reports with affiliates; the Direct Marketing Association's mail, telephone, and e-mail opt-out lists; and other company-specific lists.

Before considering the adoption of new privacy laws, I would urge Congress to first consider why consumers don't take advantage of existing opportunities to restrict the sharing or use of information.

3. The Interference with Competing Desires

Consumers' concern about privacy protection must also be examined in the context of other consumer issues. Consumers want not only more privacy, but also lower rates on mortgages and loans, higher returns on CDs and investments, and faster and more personalized service. Privacy laws can interfere with these other objectives, both by restricting the flow of information on which they depend, and by imposing high transaction costs on consumers and financial institutions alike.

a. Restricting the Benefits of Open Information Flows

Consider just a few of the many examples of the consumer benefits that depend on accessible information and that are threatened by more restrictive privacy laws. Businesses and other organizations use personal information to identify and meet customer needs. According to Federal Reserve Board Governor Edward Gramlich: "Information about individuals' needs and preferences is the cornerstone of any system that allocates goods and services within an economy." The more such information is available, "the more accurately and efficiently will the economy meet those needs and preferences."¹

Information-sharing allows financial institutions to "deliver the right products and services to the right customers, at the right time, more effectively and at lower cost," Fred Smith, founder and President of the Competitive Enterprise Institute, has written.² The use of personal information to recognize and respond to individual customer needs is the

definition of good customer service. Personalized service—epitomized by George Bailey, small-town banker played by Jimmy Stewart in “It’s a Wonderful Life”—is what many consumers want. The *Los Angeles Times* reported in December 1999 about customers who are understandably “irritated if the bank fails to inform them that they could save money by switching to a different type of checking account.” But, of course, as the newspaper noted, “to reach such a conclusion, the bank must analyze the customer’s transactions”³

By having a complete picture of its customers’ financial situations, banks can offer them bundled services at a single lower price than if provided on an a la carte basis. Customers benefit in two ways: First, they are offered a range of diversified services that are most appropriate for their individual financial situations. Second, they get those services at a lower price.

So, for example, a consumer may choose to link her mortgage loan with a checking or savings account at the lender’s affiliate, and thereby avoid minimum balance requirements for the checking or savings account, and enjoy the convenience of being able to arrange for direct deductions from a bank account to make the monthly mortgage payment. A financial services institution can aggregate all of a customer’s accounts to satisfy minimum balance requirements. It can make an instant decision whether to increase a credit line, based on its total relationship with the customer. Washington attorney Richard Fisher writes: “Information sharing also enables financial institutions to offer consumers popular products such as ‘affinity’ or ‘co-brand’ credit card accounts. Such programs provide frequent flyer miles, grocery or gasoline rebates and other benefits to credit cardholders. Other such programs permit universities and other not-for-profit organizations to benefit from cardholder use of their accounts.”⁴

To provide all of these and other opportunities, access to data is essential. Laws restricting affiliate-sharing or requiring opt-in consent make the provision of these services untenable. How could an affinity program work if the card issuer and unaffiliated partner could not share customer data? How could a lender accurately and rapidly judge the risk of increasing a customer’s credit line if it could not look at all of her accounts with affiliated companies? How would a financial services institution identify appropriate candidates for debt consolidation, if it couldn’t examine both the range of outstanding debts and home ownership or other relevant criteria?

Information-sharing is especially critical for new and smaller businesses. By restricting the availability of information about their customers, privacy laws help to protect established businesses from competition. Laws designed to protect privacy act as barriers to that information-sharing, and therefore, writes Robert E. Litan, Director of the Economic Studies Program and Vice President of the Brookings Institution, “raise barriers to entry by smaller, and often more innovative, firms and organizations.”⁵

b. The Cost of Regulation

There is also a financial cost to privacy regulation. We have already seen that a major component of that cost is caused by the interference of privacy laws with open information flows. Another source of that cost is the burden of complying with privacy laws. Crafting, printing, and mailing the two billion or more disclosure notices required by Gramm-Leach-Bliley, for example, is estimated to have cost \$2-5 billion. Much of that cost will be repeatedly annually.

More burdensome opt-in laws, as discussed below, would prove even more costly. During its opt-in test, U.S. West found that to obtain permission to use information about its customer's calling patterns to market services to them cost between \$21 and \$34 per customer, depending on the method employed.⁶

A 2000 Ernst & Young study of financial institutions representing 30 percent of financial services industry revenues, found that financial services companies would send out three to six times more direct marketing material if they could not use shared personal information to target their mailings, at an additional cost of about \$1 billion per year.⁷

The study concluded that the total annual cost to consumers of opt-in's restriction on existing information flows—precisely because of the difficulty of reaching customers—was \$17 billion for the companies studied, or \$56 billion if extrapolated to include the customers of all financial institutions. And those figures do not include the costs resulting from the reduced availability of personal information to reduce fraud, increase the availability and lower the cost of credit, provide co-branded credit cards and nationwide automated teller machine networks, develop future innovative services and products.

These costs do not include the additional burden to consumers of additional letters, telephone calls, and e-mails seeking consent: U.S. West had to call its customers an average of 4.8 times per household just to find an adult who could consent.

c. The Special Problem of Opt-In

The burden of privacy laws is even greater when they forbid the use of information without affirmative, opt-in consent. While both opt-in and opt-out give consumers the same legal control about how their information is used, the two systems differ in the consequences they impose when consumers fail to act.

The U.S. Post Office reports that 52 percent of unsolicited mail in this country is discarded without ever being read. It will not matter how great the potential benefit resulting from the information use, if the request is not read or heard, it cannot be acted on. Corporate trials of consent-based privacy systems demonstrate that no matter how good the offer or how easy the opt-in or opt-out method, customers rarely respond.

Under opt-out, consumers like those under Gramm-Leach-Bliley who failed to read or respond to a privacy notice, still received services. Under opt-in, consumers who

did not respond could not have their information used. By virtue of not responding—whatever the reason—those subject to opt-in are excluded from receiving information-dependent services. Opt-in is more costly to consumers precisely because it fails to harness the efficiency of having them reveal their own preferences as opposed to having to explicitly ask them.

For a practical, specific example of the impact of opt-in on consumers, Michael Staten, an economist, Distinguished Professor, and Director of the Credit Research Center at Georgetown University's McDonough School of Business, and I conducted a case study of MBNA Corporation, a diversified, multinational financial institution. Incorporated in 1981, and publicly traded since 1991, by the end of 2000, the company has experienced 40 consecutive quarters of growth, provided credit cards and other loan products to 51 million consumers, had \$89 billion of loans outstanding and serviced 15 percent of all Visa/MasterCard credit card balances outstanding in the United States.⁸

The case study examined the impact of three forms of opt-in: (1) Opt-in for sharing personal information with third parties; (2) Opt-in for sharing personal information with affiliates; and (3) Opt-in for any use (other than statutorily excluded uses) of personal information.

The study found that any form of opt-in would have significant economic effects on MBNA and its customers, because of the company's extensive use of direct marketing to attract customers and its heavy reliance on personal information to identify out of the 1 billion prospect names the company receives annually from its more than 4,700 affinity groups for which MBNA issues credit cards the 400 million names of people who are likely to be both qualified for and interested in a credit card solicitation.

Given the low response rates to opt-in requests universally reflected by organizations that seek consent other than at time of service or in response to a communication initiated by the customer, the case study concludes that even the least restrictive opt-in regime—for third-party information-sharing—would result in MBNA's marketing materials being 27 percent less well targeted. As a result, 109 million people would receive solicitations who should not have. This translates into an 18 percent lower response rate and a 22 percent increase in direct mail costs per account booked. There would also be an additional 8 percent reduction in net income because of increased defaults and reduced account activity, resulting from less qualified people receiving credit card solicitations.

The broader opt-in regimes would result in more significant losses to MBNA and its customers, largely in three areas. First, MBNA's affiliates would be unable to cross-sell services to existing customers or provide one-stop customer service, because of the restriction of sharing information across affiliates. Second, MBNA's corporate structure, which currently includes affiliates because of tax and regulatory reasons, would be less efficient and more expensive because centralized service units would no longer be able to provide services for all of the affiliates. Third, opt-in would interfere with fraud detection

and prevention efforts which depend on information-sharing across affiliates and among companies.

These costs would be incurred despite the fact that as of the end of 2000, only about 130,000 customers (one-quarter of 1 percent of MBNA's customer base) had exercised their legal right to opt out of having their credit report information transferred across MBNA affiliates, and approximately 1 million customers (less than 2 percent) had taken advantage of MBNA's voluntary opt-out from receiving any type of direct mail marketing offers.

The important point is not simply that complying with privacy laws is expensive, but rather that it imposes costs on consumers. Privacy polls rarely if ever ask consumers whether they are ready to bear that cost. But ultimately, it is consumers and individuals, in the words of Alabama Attorney General Bill Pryor, who "pay the price in terms of either higher prices for what they buy, or in terms of a restricted set of choices offered them in the marketplace."⁹

4. The Bigger Context

It is also important to evaluate consumer concerns about financial privacy in a broader context. Gramm-Leach-Bliley was passed in 1999 and the first notices were required to be mailed by July 1, 2001. Only 14 months has passed since that date, examinations of financial institutions under the new requirements are only now beginning, and enforcement has been limited. It is simply too early to judge meaningfully how well the new system is working.

Despite the short time, however, financial institutions have been busy working with federal regulators, consumer advocates, and others trying to improve their privacy notices and increase the effectiveness of consumer education. There was considerable criticism of the first round of Gramm-Leach-Bliley privacy notices, a key element of the law. While some of that criticism may be justified, the complexity of privacy notices seems in large part to have reflected the complexity of the law and regulations requiring them. Title V uses many terms that consumers would likely find confusing and that must be used precisely to make sense of the law's requirements. For example, the law makes a significant distinction between "consumers" and "customers," and this distinction was necessarily reflected in many notices, even though many people use the terms interchangeably.

It should also be noted that clarity may be in the eye of the beholder. On June 18, 2001, at a hearing on financial privacy of the California General Assembly's Committee on Banking and Finance, the Committee Chairman challenged the financial services industry representatives in the audience to live up to the standard set by American Express' privacy notice. In fact, he distributed to every person attending the hearing a copy of the American Express notice so that they could, in the Chairman's words, use it as a "model." Two weeks later, on July 9, 2001, *USA Today* editorialized in favor of clearer privacy notices, citing American Express' notice—the same notice lauded only two weeks earlier—at its first example of a difficult to comprehend notice.¹⁰

As Federal Trade Commission Chairman Timothy Muris has noted, we are still learning:

The recent experience with Gramm-Leach-Bliley privacy notices should give everyone pause about whether we know enough to implement effectively broad-based legislation based on notices. Acres of trees died to produce a blizzard of barely comprehensible privacy notices. Indeed, this is a statute that only lawyers could love—until they found out it applied to them.¹¹

Today, regulators, industry, and consumers are learning from the emerging experience with Gramm-Leach-Bliley, and are collectively improving the quality and variety of available privacy protections. The Hunton & Williams Center for Information Policy Leadership, for example, hosts a project in which leading financial institutions are trying to develop layered notices—an approach that would make privacy disclosures easier to understand and compare. The Federal Trade Commission has hosted a workshop on effective financial privacy notices, and is working with industry and privacy rights advocates to improve notices. The Commission is also pushing forward related privacy initiatives, including a national do-not-call list and increased privacy enforcement.

Many financial services companies have also responded with privacy-related products and services, or options for individuals to control the use of their information beyond what is required by law. Many financial services companies report today that they do not share personal nonpublic financial information about their customers with third parties. Some provide opportunities for customers to opt-out of information-sharing that is expressly permitted by Gramm-Leach-Bliley. Citicorp, Capital One, Visa, and American Express all advertise credit cards offering privacy- and security-related enhancements. Bank of America and other banks are openly competing for consumer business based on how privacy protective they are. Companies are developing best practices for a variety of privacy protections; for example, Citicorp has released telemarketing best practices developed with state attorneys general.

None of these developments is likely to prove a panacea for privacy protection, but their variety and the speed with which they are being developed suggest that they will afford consumers a greater choice of privacy alternatives than any law is likely to. Most importantly, there is virtually no evidence of tangible harms to consumers that are not already covered by Gramm-Leach-Bliley, the Fair Credit Reporting Act, or some other financial privacy law.

Consumers have understandable concerns about their privacy, and some adjustments to federal financial privacy law may eventually prove necessary. But in the absence of evidence consumers being physically or financially harmed by unregulated uses of their personal financial information, Congress has the time to wait to see how existing laws are working and to allow market responses to more fully mature.

Fred H. Cate is a professor of law, Ira C. Batman Faculty Fellow, and director of the Information Law and Commerce Institute at the Indiana University School of Law—Bloomington. He specializes in privacy and other information law issues, and appears regularly before Congress, state legislatures, and professional and industry groups on these matters.

He directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, served as a member of the Federal Trade Commission's Advisory Committee on Online Access and Security, and currently is a visiting scholar at the American Enterprise Institute and a senior policy advisor at the Hunton & Williams Center for Information Policy Leadership.

Professor Cate is the author of many articles and books concerning privacy and information law, including *Privacy in Perspective* (AEI Press), *Privacy in the Information Age* (Brookings Institution Press), and *The Internet and the First Amendment* (Phi Delta Kappa). He is the co-author of the sixth edition of *Mass Media Law* (Foundation Press) (with Marc Franklin and David Anderson).

A graduate of Stanford University and Stanford Law School, Professor Cate is a member of the Phi Beta Kappa Senate and of the board of directors of the Phi Beta Kappa Fellows, and is listed in *Who's Who in America* and *Who's Who in American Law*.

¹Financial Privacy, Hearings before the Subcomm. on Financial Institutions and Consumer Credit of the House Comm. on Banking and Financial Services, July 21, 1999 (statement of Edward M. Gramlich).

²Fred L. Smith, Jr., Better to Share Information, *Desert News* (Salt Lake City, UT), Oct. 14, 1999, at A22.

³Edmund Sanders, Your Bank Wants to Know You, *Los Angeles Times*, Dec. 23, 1999, at A1.

⁴Financial Privacy Hearings, *supra* (statement of L. Richard Fischer).

⁵Robert E. Litan, *Balancing Costs and Benefits of New Privacy Mandates*, Working Paper 99-3, AEI-Brookings Joint Center for Regulatory Studies (1999).

⁶Brief for Petitioner and Interveners at 15-16, *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1239 (10th Cir. 1999) (No. 98-9518), cert. denied 528 U.S. 1188 (2000).

⁷Ernst & Young LLP, *Customer Benefits from Current Information Sharing by Financial Services Companies* 16 (Dec. 2000).

⁸Michael E. Staten & Fred H. Cate, "The Impact of Opt-In Privacy Rules on Retail Credit Markets: A Case Study of MBNA," *___ Duke Law Journal ___* (forthcoming 2002).

⁹Bill Pryor, *Protecting Privacy: Some First Principles*, Remarks at the American Council of Life Insurers Privacy Symposium, July 11, 2000, Washington, DC, at 4.

¹⁰"Confusing Privacy Notices Leave Consumers Exposed," *USA Today*, July 9, 2001, at 13A.

¹¹Timothy J. Muris, *Protecting Consumers' Privacy: 2002 and Beyond*, Privacy 2001 Conference, Cleveland, OH, Oct. 4, 2001.