Subcommittee on Financial Institutions and Consumer Credit
Committee on Banking and Financial Services
U.S. House of Representatives

FINANCIAL PRIVACY

Professor Fred H. Cate

July 20, 1999

Madam Chairwoman and members of the Subcommittee:

My name is Fred Cate. I am a professor of law, Harry T. Ice Faculty Fellow, and director of the Information Law and Commerce Institute at the Indiana University School of Law—Bloomington, and senior counsel for information law at Ice Miller Donadio & Ryan in Indianapolis. I am testifying today on my own behalf, as someone who has researched, taught, and written about information law issues generally, and information privacy issues specifically, for more than a decade.[1]

"Privacy" is capturing legislative attention in Washington and state capitals as never before. Congress has a number of significant privacy bills—including H.R. 10[2]— under consideration. State legislatures are being no less attentive: in 1998, 2,367 privacy bills were introduced or carried over in U.S. state legislatures; 42 states enacted a total of 786 bills. This year has seen extensive action at the state level; New York alone has already enacted 14 new privacy laws.

These laws respond to dramatic changes in technologies which make it easier and more profitable to collect, process, and use information about individuals. And they respond to reports of mounting consumer fears about privacy. They are often popular laws. Nonetheless, I encourage you to defer additional legislation intended to protect further the privacy of financial information.

Information as Essential Infrastructure

[1]I am the author of *Privacy in the Information Age* (Brookings Institution Press, 1997); *The Public Record: Information Privacy and Access—A New Framework for Finding the Balance* (Coalition for Sensible Public Records Access, 1999) (with Richard J. Varn); "The Changing Face of Privacy Protection in the European Union and the United States," forthcoming in the *Indiana Law Review*; "The European Data Protection Directive and European-U.S. Trade," *Currents*, vol. vii, no. 1, at 61 (1998); "Privacy and Telecommunications," 33 *Wake Forest Law Review* 1 (1998); "The EU Data Protection Directive, Information Privacy, and the Public Interest," 80 *Iowa Law Review* 431 (1995); and "The Right to Privacy and the Public's Right to Know: The 'Central Purpose' of the Freedom of Information Act," 46 *Administrative Law Review* 41 (1994) (with D. Annette Fields and James K. McBain). A biographical statement is attached. In compliance with House Rule XI, clause 2(g)(4), I certify that I have received no federal grant, contract, or subcontract in the preceding two fiscal years.

[2]Financial Services Act of 1999, H.R. 10, 106th Cong., 1st Sess. (1999).

Historically, the United States has placed extraordinary importance on the open flow of information, for good reason. As the Federal Reserve Board reported to you in 1997 in its examination of data protection in financial institutions, "it is the freedom to speak, supported by the availability of information and the free-flow of data, that is the cornerstone of a democratic society and market economy."[3]

My colleague, Richard Varn, Chief Information Officer of the State of Iowa, and I have just completed a report that highlights the critical roles played by just one segment of information—public record information—in our economy and society. In that report, which will be released next week at the annual meeting of the National Conference of State Legislatures, we conclude that such information constitutes part of this nation's "essential infrastructure," the benefits of which are "so numerous and diverse that they impact virtually every facet of American life. . . ." The ready availability of public record data "facilitates a vibrant economy, improves efficiency, reduces costs, creates jobs, and provides valuable products and services that people want."[4]

I attach a draft copy of our report, which offers specific examples of the value of that information, but it is clear that, however essential the infrastructure of public record information in our society, it is only one part of the much larger infrastructure that includes the vast array of information held by financial institutions. To close off part of that infrastructure is likely to be as disruptive of our economy as closing off an interstate on-ramp or off-ramp is to traffic.

The late Anne Branscomb, author of *Who Owns Information?*, wrote: "Information is the lifeblood that sustains political, social, and business decisions."[5] Given the central importance of information in our economy, Congress has long hesitated before interfering with its availability. Protecting privacy inevitably impedes the availability of information and free-flow of data.

The Unanticipated Consequences of Restricting Information Flows

The cost of such restrictions is further magnified by the inevitable unanticipated consequences of regulating information flows in an effort to protect privacy.

This was the painful lesson of the State of Maine when it enacted legislation to protect the privacy of health records, a subject that I know is also before this Congress. The legislation, passed after two years of debate, took effect on January 1, but the legislature had to rescind this well-

---

[3]Board of Governors of the Federal Reserve System, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud* 2 (1997).

[4]Fred H. Cate and Richard J. Varn, *The Public Record: Information Privacy and Access—A New Framework for Finding the Balance* (Coalition for Sensible Public Records Access, 1999).

[5]Anne W. Branscomb, "Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition," 36 *Vanderbilt Law Review* 985, 987 (1983).

intentioned law 14 days later because it had the effect of keeping family members from learning whether their loved ones were in the hospital, blocking deliveries of flowers and balloons to patient rooms, and even interfering with the access of clergy to their hospitalized parishioners.

Other states have experienced similar results: it is extraordinarily difficult to close off information flows, even for the best of reasons, without imposing wide-ranging costs on individuals and institutions alike.

The likely scope and impact of unintended consequences is even greater in the context of financial information. The substantive privacy provisions of H.R. 10, which are far more moderate that some would have liked, create definitions and distinctions that are often difficult to follow, particularly when compared with federal regulation of related areas of commerce such as credit reporting. It is far from clear how the bill would apply in practice. For example, how does "personally identifiable financial information," a term that H.R. 10 uses but does not define, relate to the information regulated by the Fair Credit Reporting Act?

Similarly, H.R. 10 forbids a bank from disclosing financial information to nonaffiliated third parties unless the bank provides customers with an opportunity to "opt out" of such use, and forbids nonaffiliated third parties from redisclosing such information to other nonaffiliated third parties. The bill expressly exempts credit reporting agencies from the first limitation (on receiving information), but it is silent on whether they are subject to the second limitation (on redisclosing that information), despite the fact that only three years ago, in the 1996 amendments to the FCRA, Congress expressly exempted experience and transaction information from the scope of that law. Should H.R. 10 be enacted into law, which of these two statutes would control?

Because the privacy provisions of H.R. 10 were adopted quickly and without public hearings, there is no sense of those provisions' likely impact on the cost of financial services. That cost may be measured in terms of both lost revenue and decreased opportunities for customers. Moreover, H.R. 10 is silent on affiliate information sharing and on whether the bill would pre-empt state laws that regulate affiliate information sharing.

If the bill had gone further, as some proposed, and prohibited the sharing of financial information among affiliates, the potential ramifications would have been far greater, especially as banks increasingly rely on affiliates to provide key services to their customers. I applaud the restraint that this committee has already demonstrated. I urge you to wait before enacting additional restrictions until you and federal regulators have an opportunity to measure the impact—intended and unintended—of H.R. 10, should it be enacted into law.

Market Responses to Protect Privacy

In addition to the vital role played by information, and the virtual impossibility of restricting information flows to protect privacy without imposing other, unanticipated costs, I encourage you to defer further regulation because of the widespread and escalating response of financial institutions and associations to customer privacy concerns, and the increasing availability of technological and other forms of self-help.

In this, I concur fully with the Federal Trade Commission's recommendation last week in the context of online privacy. Despite finding that "the implementation of fair information practices is not [yet] widespread among commercial Web sites," the Commission concluded that "legislation to address online privacy is not appropriate at this time,"[6] recommending instead that "effective self-regulation is the best way to protect consumer privacy."[7] The principle reflected in Chairman Pitofsky's statement— that market responses offer more tailored and effective privacy protection and impose fewer costs than legal restrictions—certainly applies to financial privacy.

In recent years we have witnessed not only an increase in concerns about privacy, but also a parallel increase in the tools available to consumers to protect their privacy and in the self-regulatory actions of industries responding to consumer demands. Moreover, there are exciting developments that are just coming into reality that promise to give consumers greater ability than ever before to express meaningful preferences for how information about them is collected and used. This is especially true in the rapidly expanding arena of online banking.

Many companies are actively competing for customers by promoting their privacy policies and practices, and with good reason: in a trust-based industry such as consumer financial services, companies cannot survive if they lose their customers' confidence. Banks have every reason to provide the privacy protections that their customers desire, because if customers don't trust banks' handling of their data, they aren't likely to trust banks' handling of their money. Moreover, in such a competitive industry, giving customers as much control over their information as they desire is likely to an effective competitive tool. This was the calculation made by Bank of America, when it announced that it would not share customer information with nonaffiliated entities.

Ultimately, of course, if enough consumers are concerned about better privacy protection and back-up their concerns, if necessary, by withdrawing their patronage, virtually all competitive industry sectors are certain to respond to that market demand. In fact, consumer inquiries about, and response to, corporate privacy policies are an excellent measure of how much we really value privacy.

---

[6]Federal Trade Commission, *Self-Regulation and Privacy Online* 12 (1999).

[7]"Self-Regulation and Privacy Online," FTC Report to Congress, Federal Trade Commission news release, July 13, 1999 (quoting Chairman Robert Pitofsky).

Clearly, these extra-legal measures for protecting privacy do not exist in a legal vacuum. Federal and state law already provides important protections and rights, ranging from those that address privacy issues explicitly, such as the Fair Credit Reporting Act, to broader legal rights that empower courts to enforce contractual promises and the Federal Trade Commission to investigate "unfair or deceptive acts or practices in or affecting commerce."[8]

The privacy provisions in H.R. 10 are, therefore, consistent with past legal measures and commendable in carrying out this important principle of "say what you are going to do, and do what you say you will." This requirement for disclosure and for behavior consistent with that disclosure is a fundamental underpinning of American contract and consumer law. And it is essential if consumers are to be able to make intelligent choices about the level of privacy protection they desire.

At the same time, I believe that H.R. 10 goes too far in not merely requiring financial institutions to provide customers with notice of their privacy policies and to act consistent with that notice, but by imposing certain substantive terms that must be included in those policies themselves, rather than letting consumers choose in this competitive market how much privacy protection they want and how much they are willing to pay for it.

It is not an answer to say that all the bill requires is an opportunity for individuals to opt out of nonaffiliate information sharing. Substantive legal restrictions to protect privacy impose costs on everyone, even those who not desire the heightened level of privacy protection. Moreover, those restrictions are likely to conflict with the interest of the persons whose privacy is being protected. Customer services such as instant credit in a retail store, overdraft protection on checking accounts, debit cards, and online banking all depend on the ready availability of information, often collected and maintained in advance. Substantive legal restrictions (including the opt-out provisions) may make it untenable to provide instant access to credit histories, to market overdraft protection and debit cards to appropriate customers, or to verify the identity and creditworthiness of the online shopper. When that happens, the customer is harmed, even though he or she may be willing at that moment and for that purpose, to consent to the disclosure of his or her credit information. Restrictions on information to protect privacy inevitably restrict the range of opportunities to which consumers will be given the chance to consent in the first place.

Legislation in the Face of Rapid Change

[8] 15 U.S.C. § 45(a)(1) (1997).

However great the impact of H.R. 10—or any other privacy legislation—today, we should be even more concerned about its likely impact on our future. Electronic commerce is finally beginning to take off in the United States. A recent University of Texas study calculates that the Internet generated $301 billion in revenue in the United States last year, including $102 billion in on-line sales.[9] Financial services promise to be the central component of e-commerce, both because of the need to find secure ways to pay for goods and services purchased online, and because of the dramatic cost savings available when banking online. A Booz-Allen Hamilton study found that a single banking transaction costs $1.08 at a bank branch, 60 cents at an ATM machine, 26 cents with PC banking, but only 13 cents on the Internet.[10]

Online financial services require reliable and accurate means for identifying the parties engaging in the transaction, verifying their consent to the deal, and transferring funds from the purchaser to the seller. Financial services and technology companies alike are racing to develop the tools to do this, but it seems unthinkable that e-commerce and online banking will work without ready access to information, just as check clearance and credit authorization services today require such access. Restricting the collection and accessing of information, as H.R. 10 and proposals for other financial privacy legislation do, threatens online banking activities in more ways than we can imagine.

Crafting clear, effective legislation in the face of such rapid change in an area as central to our economy as financial services is a daunting task. It is made even more so by the complexity of and controversy surrounding privacy issues. I know you have just lived through this with H.R. 10, which, as I have already indicated, is subject to a variety of interpretations and serious concerns about its scope and effectiveness from both sides of the free flow debate. The inclusion of medical privacy provisions in a financial services bill only magnifies those concerns. While you are often forced to take on daunting tasks, I query whether you should choose to in the face of such rapid change, so little consensus on how to proceed, and the serious and likely, even if unintended, ramifications of regulating in this area. In short, why impose a legislative solution if there is still a reasonable likelihood (and I believe there is far more than that) that industry action, self-interest, and self-regulation, existing laws, and new technologies may eliminate the need for further regulation? This is especially true given the difficulty of using legislation to keep pace with rapid technological and market changes.

The importance of our information infrastructure, the virtual impossibility of restricting information flows to protect privacy without imposing unanticipated costs, the expanding range of more sensitive and effective mechanisms for protecting privacy that are emerging in competitive markets, and the rapid change in the contexts in which financial services and products are delivered all justify a high degree of caution before creating new restrictions on information flows to protect privacy. There is certainly need for continued enforcement of existing laws to protect against inaccurate or misleading disclosures to customers, information practices that are inconsistent with an institution's agreements with its customers, or other activities that violate existing laws. Moreover,

---

[9]See http://www.InternetIndicators.com.

[10]Sharon Reier, "Battlelines Are Forming For Next 'War of Wires'," *International Herald Tribune*, Sept. 30, 1996.

this is certainly an area, like so many others, that requires close and continuing scrutiny to determine whether new laws are necessary.

I am not suggesting that there may never be a need for additional privacy legislation, but rather that there should be no new legislation until that need is clearly demonstrated. That would require showing that both existing laws and regulations and emerging market mechanisms are insufficient to protect consumers from clearly identified harms resulting from financial institutions' use of information about those consumers. I do not yet see evidence of such a need. Given the significant consequences of regulating information, further legislation should be deferred until that need is clearly demonstrated.

Thank you.

Attachments

Biographical Statement

Fred H. Cate is a professor of law, Harry T. Ice Faculty Fellow, and director of the Information Law and Commerce Institute at the Indiana University School of Law—Bloomington, and senior counsel for information law in the Indianapolis law firm of Ice Miller Donadio & Ryan.

He specializes in information law and is the author of many articles and books in this area, including *Privacy in the Information Age*, which received Honorable Mention as the Association of American Publishers Professional/Scholarly Publishing Division Best New Book in Law 1997, and *The Internet and the First Amendment: Schools, and Sexually Explicit Expression*, both of which were selected for the 35th annual *Choice* Outstanding Academic Books list by the Association of College and Research Libraries. He is the editor of *Visions of the First Amendment for a New Millennium*.

A frequent speaker before professional and industry groups on matters relating to privacy and the ownership and control of information, Professor Cate is vice chair of the American Bar Association Section on Health Law's Electronic Communications and Privacy Interest Group and a member of the Privacy Exchange Advisory Board. He has testified before Congress on privacy in electronic communications, directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, chaired the Department of Health and Human Services' Working Group on Intellectual Property in Networked Health Information, chaired the American Association of University Professors' Intellectual Property Committee, and served as a member of Indiana Governor Frank O'Bannon's Public Access Task Force and of the U.S. Congress Office of Technology Assessment's panel of experts on Global Communications Issues and Technology and panel of reviewers on International Money Laundering. He served as a senior fellow and director of research and projects of The Annenberg Washington Program in Communications Policy Studies; he directed the Program's project on Privacy and the Public Interest, among other initiatives.

Professor Cate writes widely for the popular press and has appeared on CNN, PBS, and many local television and radio programs. In 1998 he hosted WTIU's congressional candidate debates. He received his J.D. and his A.B. with Honors and Distinction from Stanford University. Prior to joining the faculty at Indiana University, he practiced in the Washington, D.C. office of Debevoise & Plimpton. A member of the board of trustees of Phi Beta Kappa Associates, Professor Cate is listed in *Who's Who in American Law*.

Professor Cate can be reached at the Indiana University School of Law— Bloomington, 211 South Indiana Avenue, Bloomington, IN 47405, telephone (812) 855-1161, facsimile (812) 855-0555, e-mail fcate@indiana.edu.