United States House of Representatives
Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit

Hearing on "The Importance of the National Credit Reporting System to Consumers and the U.S. Economy"

May 8, 2003

Professor Peter P. Swire
Moritz College of Law of the Ohio State University
Email: peter@peterswire.net
Phone: (240) 994-4142
Web: www.peterswire.net

Introduction

Chairman Bachus, Congressman Sanders, and other distinguished members of the Financial Services Committee, I thank you for your invitation to testify concerning reauthorization of the Fair Credit Reporting Act. The FCRA was the first data privacy statute enacted in the United States, and our history under this statute can teach us important lessons about how best to proceed in considering its reauthorization.

My testimony today will provide a brief historical and analytic background for the FCRA. I will discuss the principles for financial privacy legislation that I support as a law professor and that also reflect my experience as a government official on financial privacy and related issues. I will then apply these principles of good legislation to preemption and other FCRA issues before the Committee.

Background of the Witness

I am currently a Professor of Law at the Moritz College of Law of the Ohio State University. I live in the Washington, D.C. area and am Director of the school's Washington, D.C. summer internship program.[1]

It is a particular pleasure for me to appear before this Committee because my first academic focus when I entered law teaching in 1990 was in the area of financial services law. I have often taught in the area of banking regulation, and have published law review articles on the topic in journals such as the Duke Law Journal and Virginia Law Review. I am a past Chair of the American Association of Law Schools Section on Financial Institutions and Consumer Financial Services.

I have also made a special academic study of the issue of financial privacy, and in fact received an Ameritech Faculty Fellowship in 1997 to study "The Role of Law in Assuring Financial Privacy." I have written four law review articles and a book chapter

specifically on the topic of financial privacy,[2] and have addressed related issues in numerous other writings, most of which are available at www.peterswire.net.

In March, 1999 I was named the Chief Counselor for Privacy in the U.S. Office of Management and Budget. In that position, I was intensively involved in Administration policy during consideration of Title V of the Gramm-Leach-Bliley Act, which was of course enacted in November, 1999. I was also deeply involved in development of the bill that became the Consumer Financial Privacy Act, H.R. 4380, in the spring of 2000. Since returning to law teaching, I have written an article entitled "The Surprising Virtues of the New Financial Privacy Law", which was published last year by the Minnesota Law Review. That article presents my views on affiliate sharing, notice, and other issues in the wake of the Gramm-Leach-Bliley Act.

The History of FCRA as an Effective Legal Regime

In watching the intense controversies that exist for FCRA reauthorization, I am primarily struck by the large degree of consensus on the basic structure of the Act. In most respects, both industry and consumer advocates see the FCRA as a model that is substantially superior to the systems that exist in other countries.

The FCRA without a doubt has helped to build the enormously effective system for granting credit that exists today in the United States. Today a car loan typically takes a few minutes, and a mortgage loan is no longer the lengthy process that it was when my family and I bought our first house 17 years ago. The vast majority of transactions are rapid and accurate for both lenders and consumers. Most consumer finance markets are intensely competitive, with thousands of competing credit cards offering a dazzling array of product features.

From the consumer perspective, the FCRA has provided legal safeguards that assure that the advantages of price, speed, and variety of products actually reach the greatest possible number of consumers. Anyone involved in FCRA reform should go back and read some of the hearings from the 1960s or the Arthur Miller book[3] that described the terrible problems in the credit-granting system in the period leading up to passage of the FCRA in 1970. Quite simply, people's lives were being ruined. There were numerous, documented horror stories of people being turned down for jobs and mortgages due to erroneous credit reports. Because consumers have no direct relationship with credit reporting agencies, there was no effective way for individuals to discover the mistakes and make changes. In most instances, applicants would never learn why they were being rejected for job after job or loan after loan.

The Fair Credit Reporting Act of 1970 addressed these problems, and in so doing formed the foundation for the vastly improved consumer credit markets we enjoy today. A basic opt-in rule applies to credit reports – consumer consent is required before a lender or employer can see the credit report. Consumers gained the right to see their credit histories, and to correct mistakes. Consumers now receive notice of adverse actions based on a credit report. The Federal Trade Commission became a watchdog agency on the credit reporting agencies. Private rights of action back up FTC enforcement.

In short, a rigorous legal regime created accountability in the credit granting system. The people with the most at stake in accuracy – the individuals – became the watchdogs to make sure that their own credit history remained accurate. With this foundation of accurate information, credit grantors enjoy a much lower risk when making loans. Effective checks and balances in the system, backed up by legal enforcement, have created the United States credit system that performs so well in comparison to the systems in other countries.

The credit granting system, at heart, is a vast combination of information flows. The FCRA was created in 1970 in response to the development of huge mainframe computers in the three emerging national credit reporting agencies. The 1996 amendments were passed just as the Internet was first being used for commercial activity. The Committee's challenge today, in my view, is how to continue the success of the FCRA in the networked computer systems of today and the almost unimaginable systems of a decade from now. The checks and balances that have served us well to date will, in my view, inevitably need adjustment as the underlying technologies change. Reauthorization of the FCRA is thus a work in progress, and not a task that can be finished this year for all time.

Principles for Assessing Legislation

In signing the Gramm-Leach-Bliley ("GLB") Act in late 1999, President Clinton tasked OMB (where I worked), Treasury, and the National Economic Council to draft additional legislation to finish the unfinished business of financial privacy from GLB itself. That policy process resulted in the President's announcement the following April of the proposal that became H.R. 4380, the Consumer Financial Privacy Act. Portions of that bill were incorporated into Chairman Leach's bill, H.R. 4585, the Medical Financial Privacy Protection Act, which was favorably reported by this Committee to the House.

Based on my participation in this process and my academic work on financial privacy, I offer the following principles for assessing legislation in this area. I begin with an overall effort to understand the costs and benefits of various flows of information through the financial system.[4] The following principles reflect my experience in assessing legislative proposals:

(1) *Match reasonable customer expectations.* This is the most general principle, but perhaps the most useful. If you create systems where people say "that's just not fair" then you are likely to have an unstable system that will require costly amendment over time. The credit reporting system applies to many millions of individuals, who cannot bargain effectively with credit reporting agencies on how their data will be handled. The simplest test is often to put yourself in the position of an individual with a problem in the system, and ask what would seem reasonable to you as that individual.

(2) *Adjust the level of protection to the sensitivity of the data*. We now have extensive experience on types of data that Americans consider most sensitive. Medical and financial data are at the top of the list, based both on polling and on the experience in the political system. Since 1970 there has been a general opt-in standard for sharing

credit histories. The medical privacy rule under the Health Insurance Portability and Accountability Act, which just last month entered into effect, similarly has an opt-in rule. Other information is less sensitive. In the Consumer Financial Privacy Act, for instance, we proposed opt-in protection for medical data and personal spending habits, but a less strict opt-out rule for target marketing activities.

(3) *Ensure that appropriate security and related safeguards are in place*. Having good privacy policies is not enough. The policies must also be implemented effectively in the real world. In GLB, for instance, there are information security guidelines and other important safeguards such as re-use limits, requirements of confidentiality contracts for principal-agent relationships, and so on.

I believe the Committee should determine the extent to which credit reporting agencies and entities that receive credit reports are already under the security guidelines created by GLB. To the extent they are not, the Committee might wish to consider whether FCRA reauthorization should address the issue. Recognition of the importance of information security standards largely post-dates the 1996 amendments. As part of our overall greater attention to identity theft and the risks that come from inappropriate disclosure of sensitive personal information, there may be sensible safeguards that can be created on the security side for organizations governed by the FCRA.

(4) *Create appropriate exceptions to ensure that privacy laws do not inadvertently burden important economic activity.* All of our privacy laws allow data flows in some instances without the need for customer choice, such as in the case of court orders. My view is that the exceptions under GLB, Section 502(e), generally work quite well. When we drafted the Consumer Financial Privacy Act, we proposed a new exception to assure that data could be used for customer service activities within a holding company. By contrast, my experience with the European Union Data Protection Directive, on which I wrote a book, is that other countries have sometimes failed to create needed exceptions, with harmful effects to the overall system.

(5) *Federalism.* Legislation drafted in Congress should of course consider which tasks should be handled at the state or federal level. This topic is the difficult question of when federal law should preempt state law, to which I return below.

(6) *Create a system that works over time.* We should try to do more than create a good static system, one that works for today. We should also create a good dynamic system, one that is likely to work well over time. I return to this principle below in my discussion of preemption.

Preemption and Creating a System That Works Over Time

I now turn to the linked issues of preemption and how to create an effective system for credit reporting over time.

The essential argument for preemption is systems efficiency. Credit information flows from all fifty states to the credit reporting agencies. The three key credit reporting

agencies are national and international in scope. Data then flows from these agencies to lenders and other users of credit reports in all fifty states. The basic operation of the system is thus national. The more that state and local laws alter the fundamental operations of the systems themselves, the greater the burden on participants in this national system.

There are two traditional arguments for a role for the states in the process. The first is the well-known idea that states can serve as a laboratory for experimentation. A current example of this comes from the anti-spam legislation that Congress is now considering. Although there have been some anti-spam proposals in Congress for several years, the center of legislative experimentation has been in the states, many of which have passed anti-spam laws. Some of these laws have worked better than others, and the most successful ones are now serving as models for possible federal legislation. Another current example is the do-not-call list for telemarketing. Again, the states experimented with legislation establishing do-not-call lists. After some of these state laws had proven successful, the Federal Trade Commission moved forward with the national do-not-call list that was approved recently. In both of these important areas of consumer concern, the experience with state laws was an essential step in considering establishment of national consumer protections.

The role of the states has historically been especially strong for consumer protection issues. Consumer protection legislation has repeatedly been passed to alter the common law of contracts, itself a subject of state jurisdiction. This Committee is well-versed in this special role for the states in consumer protection, as shown for instance in the Riegle-Neal provisions that permit the states to continue their role in consumer protection even in the era of nationwide banking. Congress chose not to preempt stronger state laws for privacy in the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

In addition to these two traditional arguments – laboratories for experimentation and the state role in consumer protection – my experience in government and in the study of privacy laws suggests a third, important reason to consider limiting the scope and duration of preemption in the consumer credit area. Limited preemption, in my view, plays a key role in bringing the players to the table, so that all perspectives are considered in the revision of legislation.

The recent history of privacy legislation shows that privacy protections have been enacted almost exclusively when they were part of a larger legislative package that was strongly desired by key industry groups. The medical privacy rule arises from the passage of HIPAA in 1996. In that bill, industry groups strongly supported the "administrative simplification" provisions that would reduce costs by requiring payments to be in standard electronic formats. Congress decided that security and privacy safeguards should be created at the same time that the medical system was shifting to electronic records. The telecommunications privacy rule arises from the Telecommunications Act of 1996. That bill, which restructured so much of the telecommunications industry, included the so-called CPNI (customer proprietary network information) privacy rule. In 1999, this Committee participated in the creation of the

Gramm-Leach-Bliley Act. The privacy protections of Title V were once again included as part of an overall package that was strongly desired by industry stakeholders.

The same pattern holds true today. We simply would not be having the same discussions on how to update consumer protections in the credit reporting system except for the desire for legislation on the part of the affected industry. The push for reauthorization creates a forum for examining how to create an FCRA that is appropriate for today and the future.

The focus on the future is especially important because the FCRA is a statute that regulates information flows in an era of rapid changes in information flows. Whatever is appropriate in January, 2004 will almost certainly be different for the changed information systems of January, 2012. We have already seen rapid change since 1996 in the area of identity theft. It is difficult or impossible to predict what emerging information challenges will arise in the coming years.

To pull the themes together on preemption, a core goal of reauthorization is to assure the efficient operation of the national credit reporting system. State laws that require costly re-engineering of the national system are the ones that are the best candidates for preemption. On the other hand, the closer one comes to actual customer relations, the more that localized approaches relevant to that individual and community are likely to be appropriate.

In addition to possible limits on the subject matter scope of preemption, I think the case is particularly strong for limiting the duration of federal preemption. The overall policy goal facing this Committee is how to build a credit reporting system that works both today and in the future. The rise of identity theft shows how new problems will arise as information systems change. Limiting the duration of preemption will likely spur a better public policy process when reauthorization is next due.

Matching Preemption Rules to the National Market

The analysis here supports federal preemption for issues that would impede national efficiencies in systems operations, and greater tolerance for state law experimentation for issues that apply predominantly within each jurisdiction. Reasonable people may differ on which provisions deserve to be more "national" or "local." I offer a few observations here based on my current understanding of how the systems are likely to operate.

One strong candidate for preemption would appear to be a firm offer of credit or insurance. The offer is likely to be made to multiple states, drawing on a national credit reporting agency and often a national financial institution that is making the offer. Suppose, for instance, that one state required a particular double-check before the firm offer could be made. The programmers for the credit reporting agency or financial institution would then need to write costly programming to screen how all of the files would be handled. If these facts are correct (and I base my comments on prior site visits to credit card companies and other financial institutions), then state laws governing pre-screening could easily place a significant burden on a national set of operations. (To the

extent that additional consumer protections are appropriate for the topic of pre-screening – and the current statute really does not provide privacy standards for how the pre-screening is done – then such protections would be a suitable topic for the Committee to address in the federal reauthorization process.)

My current view is different, however, for state laws concerning those who furnish information to the credit reporting agencies and those who use credit reports. The furnishers and users are companies that have chosen to do business in a particular state. They already comply with tax laws, consumer protection laws, and numerous other rules that may be specific to that state. As to furnishers, there may be a useful role for state experimentation when it comes to the issue of ensuring that incorrect information does not get sent repeatedly to the credit reporting agencies. A recurrent problem, both for private furnishers and for public records, is that an individual may correct data at the credit reporting agency. The same mistake, however, is often re-inserted in the individual's record by a private furnisher or a state agency that has not corrected its public record. Similarly, on the user side, it may be an appropriate use of the state police power to experiment with information security standards or other measures that ensure that credit reports do not fall into the wrong hands. For both furnishers and users, the state laws would apply to companies that have availed themselves of that state to do business.

The rapidly changing nature of the problem provides a different reason to believe that Congress should not preempt experimentation in the area of identity theft. It is difficult to have confidence in how to combat this growing problem. With our imperfect understanding of the problem, there is quite possibly a useful role for state experimentation. In addition, the nature of our authentication and other information systems is clearly in rapid transition. Writing a permanent preemption into the FCRA would run the risk of freezing us into a limited and likely sub-optimal set of responses to this problem.

Two Substantive Issues for Further Attention

Based on my ongoing privacy research, I will briefly discuss two additional areas that merit attention as part of the FCRA reauthorization process.

Medical privacy. I think it is quite possible that Congress should consider updating the treatment of medical records under the FCRA. Medical privacy occupied a large fraction of my time as Chief Counselor for Privacy in OMB. The FCRA today has only limited provisions that govern the use of "medical information" in credit reports. The term "medical information" is considerably narrower in scope than the "protected health information" that is covered under the HIPAA medical privacy rule. In the FCRA, the term covers only "information or records obtained, with the consent of the individual to whom it relates, from licensed physicians or medical practitioners, hospitals, clinics, or other medical or medically related facilities." This "medical information" cannot be furnished "for employment purposes, or in connection with a credit or insurance transaction", except with the individual's consent.

The HIPAA definition of "protected health information" is considerably broader than the FCRA definition of "medical information." For instance, HIPAA applies to medical records beyond those gained "with the consent of the individual to whom it relates." The HIPAA rule itself, as amended in 2002, does not require patient consent as part of medical treatment. Many states do not require consent, although some do. A large portion of doctors' records, therefore, would not appear to fall within the plain language of the FCRA definition. In addition, HIPAA is broader because it applies to protected health information that comes from essentially any health care provider (not just the narrower list in the FCRA), as well as from a health plan or health care clearinghouse.

In the limited time available since I was called as a witness, I have not been able to do fact-finding on the way that medical records are used today in the credit reporting system. There is a well-known loophole in Gramm-Leach-Bliley for sharing medical information within a financial holding company. That loophole was the basis of Chairman Leach's effort in 2000 to pass H.R. 4585, the Medical Financial Privacy Protection Act. That bill on this issue was essentially identical to Section 4 of H.R. 4380, the Consumer Financial Privacy Act. Perhaps that proposal, based on inter-agency efforts that included HHS, Treasury, and OMB, would be a fruitful beginning point for bringing the FCRA more in line with the heightened protections for medical records that now exist nationally under the HIPAA medical privacy rule.

FCRA and the "Patriot II" Act. I would like to call the Committee's attention to a seriously misleading statement in the so-called Patriot II proposal. That proposal, according to press accounts, was circulated to senior Administration officials before being leaked to the press earlier this year. Section 126 of that draft legislation is entitled "Equal Access to Consumer Credit Reports." The proposal would allow law enforcement officials to get any credit report with a simple certification that they will use the information "only in connection with their duties to enforce federal law." There are no limits on re-disclosure to other agencies. There are no mechanisms at all to ensure that the credit reports will be used for the stated purpose once they are given to the government.

The seriously misleading statement is to call this "equal access" to credit reports when it is instead unprecedented access. Under current law, credit reports are *pulled at the choice of the individual*, such as for a loan or other transaction initiated by the individual.[5] The individual decides whether a credit report should be generated. The statute is full of detailed notice requirements, re-disclosure rules, and adverse event reporting. By sharp contrast, the proposed Section 126 would give the government the power to get a credit report secretly, without the consent of the individual, with no indication of adverse actions, and with a prohibition on telling the individual even after the fact that the credit report has been accessed. This is an Orwellian use of the words "equal access." In light of the disingenuous proposal to amend the FCRA, this Committee should give a detailed and public vetting to any proposal to amend the FCRA to give unprecedented access by government agencies to the sensitive data in Americans' credit histories.

Conclusion

In conclusion, I thank the Committee for holding this hearing on the role of national credit reporting system. The furious debate about the scope of preemption should not cloud the very large areas of agreement about the Fair Credit Reporting Act. Effective legal protections for consumers, including full access for individuals to their own credit histories, have helped create a far more accurate and efficient credit granting system than would otherwise have existed. A major challenge is how to ensure that effective privacy and other consumer protections accompany the rapid changes in future years in our information economy. A certain degree of experimentation by the states, and a periodic re-examination of these issues by the Congress, will likely create a better system over time than a permanent preemption of all consumer protections at the state level.

---

[1] I note that I also serve as a consultant to the Washington, D.C. office of the law firm of Morrison & Foerster, LLP, on health privacy and other matters. I am presenting this testimony entirely in my individual capacity as a Professor of Law. I am not an employee of Morrison & Foerster, and am not appearing on behalf of the Firm. I have not performed work for any client on the issue of FCRA reauthorization.

[2] The articles are: "Efficient Confidentiality for Privacy, Security, and Confidential Business Information," Brookings-Wharton Papers on Financial Services (forthcoming, 2003; available at www.peterswire.net); "The Surprising Virtues of the New Financial Privacy Law," 86 Minn. L. Rev. 1263 (2002); "Financial Privacy and the Theory of High-Tech Government Surveillance," 77 Washington U. L.Q. 461 (1999) & Brookings-Wharton Papers on Financial Services; and "The Uses and Limits of Financial Cryptography: A Law Professor's Perspective," chapter in the proceedings of Financial Cryptography '97 (Springer-Verlag, 1997). The chapter on financial privacy is in Peter P. Swire & Robert E. Litan, None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive (Brookings, 1998).

[3] Arthur R. Miller, The Assault on Privacy: Computers, Data Banks, and Dossiers (1971).

[4] For my views on assessing costs and benefits of information flows in financial services, see Peter P. Swire, "Efficient Confidentiality for Privacy, Security, and Confidential Business Information." It is available at www.peterswire.net.

[5] Credit reports can also be shared for purposes of a firm offer of credit or insurance, subject to consumer opt-out, limited disclosure of information to the offeror, and the other detailed safeguards in 15 U.S.C. § 1681b. In addition, the FCRA currently permits disclosure to the FBI for counter-intelligence purposes , subject to numerous safeguards, 15 U.S.C. § 1681u, and disclosure subject to fewer safeguards for counter-terrorism purposes, 15 U.S.C. § 1681v. The proposal in the Patriot II Act entirely lacks the sorts of safeguards that currently exist, for instance, under Section 1681u.