Testimony

of

Professor Joel R. Reidenberg
Fordham University School of Law
140 West 62nd Street
New York, NY 10023
Tel: 212-636-6843

Email: <reidenberg@sprynet.com>
Web: <http://reidenberg.home.sprynet.com>

before the

Committee on Banking, Housing and Urban Affairs
United States Senate

108th Congress, 1st Session

Hearing on "Affiliate Sharing Practices and Their Relationship to the Fair Credit Reporting Act"

June 26, 2003

Mr. Chairman, Ranking Member and Distinguished Members of the Committee,

I commend you for convening this hearing on affiliate sharing practices and their relationship to the Fair Credit Reporting Act and I thank you for the honor and privilege to appear before you. My name is Joel R. Reidenberg. I am a Professor of Law at Fordham University School of Law where I teach courses in information privacy, international trade and comparative law. As a law professor, I have written and lectured extensively on the regulation of fair information practices in the private sector. My bibliography includes scholarly articles and two co-authored books on data privacy.[1] Of relevance to today's hearing, I have studied and written about the Fair Credit Reporting Act ("FCRA") and have advised both federal and state government agencies on FCRA litigation issues. I am a former chair of the Association of American Law School's Section on Defamation and Privacy and have also served as an expert advisor on data privacy issues to state and local governments, to the Office of Technology Assessment in the 103rd and 104th U.S. Congresses and, at the international level, to the European Commission and foreign data protection agencies. I appear today as an academic expert on data privacy law and policy and do not represent any organization or institution with which I am or have been affiliated.

My testimony will focus on three points: (1) the US credit reporting system needs strong privacy protections to preserve a robust national information economy; (2) the affiliate sharing provisions of the 1996 Amendments create significant unrecognized loopholes that eviscerate the protections of the FCRA; and (3) the affiliate sharing loopholes pose security risks and a threat to the soundness of the U.S. credit reporting system.

I recommend that Congress either eliminate the affiliate sharing loopholes or leave the 1996 sunset clauses alone so that states are re-authorized to protect their citizens against abusive practices under the affiliate sharing loopholes. I further recommend that, before taking any other type of legislative action, Congress should investigate thoroughly these broader implications of affiliate sharing. Congress must have a much deeper factual knowledge of the specific types of credit report data that is shared among affiliated companies and a much deeper knowledge of the specific uses, disclosures and onward transfers that are made by the affiliated recipients outside the protections of the FCRA for citizens' privacy.

1. Strong Privacy Protections are Essential for the Credit Reporting System

The FCRA was enacted in 1970 as a response to significant abuses in the nascent credit reporting industry. Decisions affecting citizens' lives were being made in secret with bad data. Congress heard extensive testimony during the late 1960s on the unfair and abusive information practices that voluntary industry guidelines failed to prevent. These included the release of credit information to non-credit grantors, the dissemination of inaccurate credit information, the inability of consumers to gain access to their credit

reports, and the difficulty of consumers to obtain correction of erroneous information.[2] Scandals and distrust were harming the marketplace.

In enacting the original FCRA, Congress wanted to assure the efficiency and integrity of the U.S. banking system. The statute became the cornerstone of US privacy law. Congress recognized that fair information practices were essential for vibrant credit markets and expressly sought "to prevent an undue invasion of the individual's right of privacy in the collection and dissemination of credit information."[3]

A. The FCRA Established the Principles of Opt-in Consent and the Fair Treatment of Personal Information

At the time of enactment, the FCRA was an extraordinary and unique statute precisely because the law set a new standard for strong privacy protection. The FCRA established a then-novel system of opt-in permission for the dissemination of credit report information. The statute defined a specific set of permissible purposes for which the disclosure of credit report information was authorized. These purposes related directly to the reasons for which collected data was gathered and were generally limited to the extension of credit, insurance or employment. Any other disclosure of credit report information required the written consent of the consumer.

Among other important innovations for fairness, the law created transparency in the industry by granting a consumer the right of access to credit report information and by requiring the industry to identify the recipients of credit reports. The law further provided rights for consumers to dispute inaccurate information contained in their credit reports. Lastly, the FCRA included due process safeguards before a consumer reporting agency could disclosure credit report information to government agencies or law enforcement. This overall framework provided a bedrock set of standards for fair information practices.

B. The FCRA Never Created an Overall "Uniform National Standard"

From the start, however, Congress recognized that the credit reporting industry would be likely to evolve significantly and that even greater privacy and fairness could benefit the banking industry. As a result, Congress permitted the states to enact stronger privacy protections for credit reporting since stronger state statutes promoted the main goals of the original FCRA. In fact, at the time of enactment, this Committee specifically endorsed the position of state officials who testified at Senate hearings expressing "a need for Federal legislation to supplement any future State legislation which may be enacted."[4]

The major subsequent fair information practice laws similarly adopted this policy and waived federal pre-emption. For example, the Financial Services Modernization Act, the Health Insurance Portability and Accountability Act, the Cable Communications Policy Act, and the Video Privacy Protection Act, each expressly waived, in whole or in part, federal pre-emption. Despite industry's wishful repetition at a plethora of hearings

this spring,[5] the FCRA never intended nor did it create an overall "uniform national standard." Instead, the statute established a minimum set of federal standards that have always been supplemented by varying state laws.

By 1996, when Congress adopted a number of significant amendments to the FCRA, the credit reporting industry had grown dramatically and, indeed, operated nation-wide in a seamless fashion notwithstanding diversity at the state level. In testimony earlier this month before the House Subcommittee on Financial Institutions and Consumer Credit, Vermont Assistant Attorney General Julie Brill thoroughly documented the significant variations among state laws.[6]

Nevertheless, among the 1996 FCRA amendments, Congress included a temporary and partial pre-emption clause that prevents states for another six months from implementing certain types of stronger credit reporting provisions. Notwithstanding the temporary and narrow pre-emption, the 1996 amendments explicitly exempted the stronger California, Massachusetts and Vermont statutes from specific elements of the narrow pre-emption.[7] Hence, even the 1996 amendments did not create an overall "uniform national standard."

C. State Differences Do Not Appear to Impede Credit Reporting or Financial Decision-Making

The fairness rules and opt-in approach contained in the FCRA enabled the credit reporting industry to progress from its fragmented, chaotic and abusive period in the late 1960s to a successful, respected component of the U.S. information-based economy. The FCRA obligations coupled with the ability of states to enact stronger protections, in effect, created today's thriving national infrastructure of credit reporting.

Industry funded projects, however, assert the imminence of a 'parade of horribles' should Congress not support industry's desire to preclude stronger state privacy laws. Key "findings" from these projects are based on ideological hyperbole rather than comprehensive and accurate analysis. For example, some have argued that strong credit reporting rules overseas substantially hinder the "miracle of instant credit" and result in much higher interest rates or more onerous borrowing conditions.[8] These arguments have no apparent basis in fact or analysis. No other major country to my knowledge has a comparable statute governing only credit report information. Comprehensive data privacy laws applicable to most processing of personal information do exist outside the United States such as those in Canada, in the United Kingdom and throughout Europe under European Directive 95/46/EC. These laws typically apply to credit reporting and are generally more protective of consumers than the FCRA. However, foreign consumer credit markets are structured by banking law, bankruptcy law, real estate law, and consumer protection laws that often deviate significantly from those in the US legal system. The attribution of differences in credit markets to general data privacy laws without examination of the direct regulatory constraints on credit relationships such as interest rate regulation, down payment restrictions, or legal protections for security interests is specious and a misrepresentation of foreign privacy law.

Others have even argued that "increased competition, driven in part by pre-screening, has caused [credit card] interest rates today to be … lower overall"[9] as compared to 1990. Yet, the "analysis" omitted any mention of the dramatic drop in the prime rate that many card issuers use to calculate their credit card interest rates. In fact, between 1990 and 2002, the prime rate declined from 10.01% to 4.67%.[10] Most rational observers would give Chairman Greenspan and the Federal Reserve the acclaim for declines in credit card rates rather than pre-screening.

To my knowledge, there is no study or evidence that examines the actual, existing differences among state protections and that shows these stronger protections demonstrably impede the credit reporting system. Indeed, to my knowledge, no industry group has examined the effects of the three stronger state statutes recognized by Congress under the 1996 Amendments on either the credit markets in those states or on the nation-wide industry. This is not surprising. A rudimentary look at federal statistics suggests that credit decisions in these states benefit both lenders and consumers. Consumer bankruptcy filings per household, a basic sign of bad credit decisions, are markedly better for the three states with statutes recognized by Congress as more protective of consumer information. Vermont ranks 50th with the lowest rate of consumer bankruptcies in the nation, Massachusetts is 49th and California comes in below the median at 27th.[11]

Similarly, federal statistics on interest rates seem to indicate that states with stronger credit reporting laws have lower rates. The most current annual federal mortgage loan data indicates that the effective rate on a conventional mortgage for 2002 was 6.25% in California, 6.43% in Massachusetts and 6.59% in Vermont.[12] All were below the national median and California had the lowest rate in the nation. Vermont Assistant Attorney General Julie Brill has also noted in testimony presented to the House Subcommittee on Financial Institutions and Consumer Credit that Vermont has the second lowest auto loan rates in the country and the other more privacy protective states rank well with low rates.[13]

While these statistics leave out important elements for a thorough assessment of the impact of stronger state laws such as a correlation with state unemployment data for bankruptcy filings and non-interest transaction costs for home mortgage loans, the data does show that the horror stories circulating about the pre-emption provisions make good theater, but reflect poor research.[14]

In fact, other countries with comprehensive data protection statutes such as Canada demonstrate that robust credit information services can co-exist with strong, comprehensive data privacy laws. For example, one major US credit reporting agency operating in Canada offers a typical credit report for Canadians that contains information strikingly similar to the typical report for Americans. In the United Kingdom where a comprehensive data privacy law also applies, major credit card companies offer instant approvals for platinum cards just as they do in the United States.

D. Weakening of Privacy Protections Raises Uncertainty and Decreases Confidence

The bottom line is that strong privacy protections are essential for public confidence in the integrity of financial services in the United States. Without adherence to strict fair information practices, financial markets will face uncertainty because the risk of newsworthy privacy scandals increases such as those commited by Citibank,[15] US Bancorp[16], Fleet Bank[17] or Chase Manhattan[18]. The weakening of fair information practice standards at the federal level or the preclusion of stronger state protections puts companies at greater risk for privacy scandal and diminishes public trust in the fairness of industry treatment of personal information.

2. The Affiliate Sharing Loophole Eviscerates FCRA Protections

The FCRA created fundamental fairness in the treatment of personal information through adherence to the basic principle that information collected for one purpose should not be used for different purposes without the individual's written consent. Surveys show that 95% of Americans object to secondary use of personal information.[19] For information used to make financial decisions about consumers, citizens believe that fairness requires opt-in permission. In 2001, citizens in North Dakota had the first and only opportunity in the nation to take a real position at the polls on the dissemination of their personal financial information. The North Dakota state legislature had just watered down financial privacy from an opt-in rule on third-party data sharing to an opt-out rule. The citizens of North Dakota revolted. By an overwhelming 72% majority, the voters of North Dakota approved a referendum restoring the old opt-in rule and rebuking the legislature's weakening of privacy standards.

Previous to these expressions of public opinion, Congress introduced in 1996 a significant deviation from the FCRA's historical commitment to this fundamental permissible purpose principle. Congress amended the definition of a "consumer report" in Section 603(d) to exclude information shared among companies affiliated by common ownership or control. This deviation allows organizations to escape the fair information practice obligations of the FCRA for information that would otherwise be covered when such data is disseminated to affiliates. Those affiliated companies will not be subject to important FCRA requirements including those of use only for a permissible purpose, access, accuracy and civil liability.

Congress permitted this departure from the core principle only if the company provided consumers with notice of affiliate sharing and an opportunity to opt-out. The far-reaching consequences of this deviation as a result of the successful liberalization of the financial services sector have not, however, been recognized or subject to public scrutiny. Large groups of affiliated financial and non-financial organizations can now easily engage in exactly the same behavior that Americans find troubling-- the

dissemination of confidential credit report information for a wide range of activities unrelated to the purpose of collection—and escape the obligations of consumer reporting agencies and the opt-in rule.

A. The Blanket Exemption for Experience and Transaction Data Opens a Pandora's Box

The 1996 amendments first create a blanket exemption from FCRA protection for experience and transaction data. Section 603(d)(2)(A)(ii) excludes from the definition of "consumer report" any communication of experience or transaction data among "persons related by common ownership or affiliated by corporate control." This means that organizations may disseminate experience and transaction data such as credit card performance information, insurance status or brokerage account activity among related companies without key protections under the FCRA such as accuracy. If, however, the organization qualifies as a financial institution under the Gramm-Leach-Bliley Act, then GLBA will require the organization to provide notice of its sharing practices to the consumer. But, under GLBA, consumers will not have any right to dispute erroneous information, access the information or even opt-out of the sharing.

The breadth of this exemption is likely to be very large with organizations such as Citibank that have an extraordinary array of related companies. At the same time, the scope of this exemption is also poorly understood. Industry practices are not transparent and consumers do not have access to specific information on the types of transaction and experience data that is shared nor do they have access to the identities of the actual recipients of such data and nor do they have information about the specific purposes for which the data is actually used by an identified affiliate. If this exemption is retained, I believe that Congress needs to investigate the reach of this exemption.

B. Affiliate Sharing Allows the Circumvention of Basic Protections

The most sweeping damage to the FCRA's fairness principles comes from the next part of the affiliate sharing exemption. Section 603(d)(2)(A)(iii) excludes "communications …. [to] persons related by common ownership or by corporate control" from the definition of "consumer report." To qualify for the exemption, the company must provide a one-time "clear and conspicuous" notice and must provide a single opportunity to opt-out. Experience with GLBA teaches that this limitation, however, is not likely to be particularly informative or useful for consumers.

Some companies justify this affiliate sharing provision by arguing that corporate families should be treated as one unit for consumer privacy purposes because corporate organizational structure does not have an effect on consumers.[20] This claim is simply not credible. The existence of separate entities to avoid consolidated legal liability confuses operational responsibility for privacy, impacts consumers seeking to assure the fair treatment of their personal information, and undermines consumers seeking legal redress for violations. A confusing maize of companies helped Enron obscure its true behavior. The same holds true for affiliates sharing personal information.

The exemption for affiliate sharing means that credit report information loses protection when shared with far-flung related companies. Affiliated recipients can use and disseminate credit report information and ignore the fairness principles of use only for permissible purposes, consumer access (when no adverse credit, employment or insurance decision is made), storage limitations for obsolete data or obligations for the correction of erroneous information. A consumer reporting agency might, for example, sell credit score information to one company as a permissible disclosure under the FCRA. If that purchaser were to transfer the score to an insurance affiliate, the transferred score would be excluded from the definition of "consumer report" and most of the consumer protection provisions would not apply.

In effect, the exemption undermines the entire philosophy of the FCRA. Industry statements indicate that this mechanism is already being used to subvert the original protections of FCRA: decisions are made once again from data outside the general reach of consumers and without any consumer recourse. For example, Trans Union promotes the use of affiliate sharing for underwriting decisions.[21] Citibank reported to Congress earlier this month that it "shares information among our affiliates … [including] credit application and credit bureau data, as well as information on our transactions with the customer." [22] MBNA indicates that it shares credit eligibility information including credit reports among affiliates.[23] These are precisely the uses of personal information that the original FCRA sought to cover.

The enormous scope of this exemption can be illustrated by a few examples of possible practices among related companies. U.S. Bancorp included in its cardholder agreement a disclosure that said "We share customer information within our organization … to better meet your needs" and provided instructions to opt-out of affiliate sharing. At the same time the company was settling a claim brought by the Minnesota Attorney General for disclosures of customer information to third parties, the company purchased Gargoyles—a company that designs and markets sunglasses.[24] Would any consumer reasonably understand that Gargoyles might receive copies of the customer's credit application or transaction history? While information is not available to determine if US Bancorp actually transferred client data to Gargoyles, the affiliate sharing provisions would disturbingly allow the transfer of credit report data to Gargoyles for sunglass marketing purposes. Gargoyles would then be free to re-disseminate the information outside the confines of the FCRA.

The potential circumventions are similarly disturbing when the affiliations of consumer reporting agencies are considered. Trans Union, for example, belongs to the Marmon Group.[25] The group affiliates companies in a wide range of businesses including one in the syringe needle business and another in residential water treatment.[26] If Trans Union provided notice of affiliate sharing and an opt-out, the company could transfer credit reports to these affiliates. Experian is in the same situation. Great Universal Stores, a British company owns Experian as well as Metromail and Burberrys.[27] If Experian were to provide notice of affiliate sharing and an opt-out, Experian could share the credit reporting database with Metromail, a marketing company

that paid $15 million to settle a lawsuit because the company was caught disclosing sensitive personal information to jailed convicts for processing.[28] Burberrys could also supply credit report information to Metromail outside the protections of the FCRA.

As it turns out, both Experian provides notice of affiliate sharing and opt-out choices to a growing number of consumers. The company offers consumers online access to their credit reports and monitoring services. Experian appears to use registration for these services as a means in the legal boilerplate to provide notice and opt-out for affiliate sharing.[29] In other words, consumers particularly concerned about the sanctity of their credit reports are likely to enable inadvertently the sharing of their data by the credit reporting agency with affiliates outside the protections of the FCRA. No information, however, is readily available to determine whether Experian actually shares data with these affiliates or others.

If these uses are or become widespread, then the FCRA loses both effectiveness and credibility. Since affiliate sharing generally escapes the transparency and accuracy obligations of the FCRA, there is no way for a consumer to learn the magnitude of this problem. Even for those organizations regulated by GLBA, affiliate sharing notices under GLBA would not provide sufficient detail for a consumer to realize that a company like Experian might share with Metromail or that US Bancorp might share with Gargoyles.

If this loophole is closed, Congress can and should investigate whether companies have begun to circumvent the FCRA in this fashion.

C. Affiliate Sharing Allows the Government to Engage in Surveillance Outside the FCRA Due Process Protections

Sections 604 and 625 of the FCRA provide due process safeguards against government surveillance of credit report information. Briefly, government and law enforcement agencies may obtain credit report information for specified purposes with procedural safeguards or pursuant to a court order or a Federal grand jury subpoena or, in the case of counterintelligence investigations, a statutorily defined FBI certification.[30] However, affiliate sharing means that these due process protections for access by law enforcement can easily be circumvented. If consumer report information is shared with an affiliate, the data loses its status as a "consumer report" and the FCRA protections would not apply to subsequent disclosures by the affiliate. This loophole would be one way for the "Total Information Awareness" program, an effort already the subject of Congressional concern,[31] to obtain detailed sensitive personal information on US citizens and escape the need for compliance with privacy obligations.

A simple example of the possible sharing between two affiliated companies illustrates the magnitude of this potential problem. Equifax, the credit reporting agency, operates through a number of changing groups including the currently named U.S. Consumer Services Group.[32] This apparent group of affiliates provides information services to government clients. Equifax includes a statement in its *Online Privacy*

Policy & Fair Information Principles informing consumers who request copies of their credit reports that "we may disclose any of the information, as described above [including Equifax credit file information], to affiliates which are companies that are related to us by common ownership or affiliated with us by common control" and describing for consumers several opt-out choices.[33] Although the specific language of the current opt-out choices might be insufficient to qualify for the affiliate sharing exemption, a simple clarification would clearly enable Equifax to transfer the credit report information to members of the US Consumer Services Group who, in turn, could sell the data to government agencies without an otherwise permissible purpose or court order.

At present, I have no information to suggest that Equifax engages in this practice or that government agencies or law enforcement officials are currently exploiting this loophole. I do, however, believe that this possible practice needs to be investigated if Congress does not eliminate this loophole.

D. States May Not Protect their Citizens Prior to January 1, 2004

According to Section 624 of the FCRA, stronger state laws applicable to experience and transaction data and to affiliate sharing are temporarily pre-empted, with the exception of Vermont's affiliate sharing rule. If Congress allows these pre-emptions to sunset, the states will be re-authorized to protect their citizens against the circumvention of FCRA protections. The states can play a useful role experimenting and fine tuning workable solutions to the affiliate sharing loopholes.

3. Security Risks and Threats to the Soundness of the Credit Reporting System

The leakage of credit report information to affiliates for secondary purposes outside the protections of the FCRA increases security risks and threatens the integrity of the credit reporting system.

A. *Affiliate Sharing Enhances Identity Theft Risk*

The circulation of credit report information to affiliates outside the core permissible purposes and outside the overall protection of the FCRA increases the risk of identity theft. Reports indicate that identity theft often occurs as an 'inside job.' In testimony to this Committee last week, US Secret Service Special Agent Timothy Caddigan stated: "The method that may be most difficult to prevent is theft by a collusive employee. The Secret Service has discovered that individuals or groups who wish to obtain personal or financial identifiers for a large-scale fraud ring will often pay or extort an employee who has access to this information through their employment at workplaces such as a financial institution, medical office, or government agency."[34] Wide ranging affiliate sharing increases the exposure of credit report information to the risk that a malevolent insider will steal data for identity theft.

Not surprisingly, some lobbyists deny that the wider circulation of personal information through secondary use of credit report data facilitates identity theft.[35] Yet, in the context of pre-screening, the overwhelming consensus among those involved in identity theft prevention is that pre-approved credit card offers are one of the most common resources for identity thieves. The U.S. Postal Inspection Service, the U.S. Department of Justice, the U.S. Secret Service and each of the major credit reporting agencies warn consumers that discarded, pre-approved credit card offers are one of the most common sources of personal information for identity thieves.[36] A lobbying paper sponsored by an industry group, the Privacy Leadership Initiative, admits that the average response rate to credit card offers in 2000 was only 0.6 percent.[37] In other words, American consumers are not interested in 99.4 % of these purportedly targeted offers and throw them away. There is no credible, public evidence to suggest that product or service offers generated through affiliate sharing will be of any greater interest to consumers. Yet, this type of secondary use of credit information creates an important leakage of data from confidential and secure credit reporting.

The exemption for affiliate sharing also appears unnecessary for the purpose of fraud detection and prevention. Fraud detection and prevention would in most cases qualify as a "legitimate business need" under Section 604(a); the disclosure of credit report information for that purpose should be a permissible purpose. If legitimate reasons justify affiliate sharing outside the protections of the FCRA to detect or prevent fraud, a more narrowly drawn exemption for that specific purpose would reduce the risk of identity theft from wide circulation.

B. Affiliate Sharing Introduces Homeland Security Risks

The global reach of US corporate groups means that affiliate sharing may send credit report information on US consumers to countries with high risk of political instability or terrorist action. As a consequence, US consumer data may be subject to compromising risks. For example, banks may share credit report information with affiliates in India or the Philippines where no privacy rights apply and where local concerns for the safety of US data are substantial.[38] Indeed, unconfirmed reports suggest that many US financial institutions transfer client data to India, but take careful steps not to reveal the existence of these off-shore arrangements.

One specific example illustrates this potential risk. Fair Isaacs offers a "decisioning process" that handles "30% of US credit card applicants as well as auto loans, mortgages, loans and lines of credit around the world" and offers a fraud detection system that monitors "more than 400 million payment card accounts worldwide."[39] Fair Isaacs appears to have an affiliated distributor in Malaysia,[40] a country for which the US Department of State has issued a warning about the possibility of terrorist attacks against American citizens and American interests.[41] While the exact ownership relationship between Fair Isaacs and the Malaysian partner is unclear, the point remains that if these companies are under common control, then the US data may be sent there. In this particular case, there is also no readily available information that would suggest whether Fair Isaacs does indeed transfer US credit report information to Malaysia.

Without specific information on where affiliates are located and what information they receive, the magnitude of this risk cannot be evaluated. If Congress does not eliminate the affiliate sharing loopholes, I believe that this risk needs further investigation.

Recommendations for Future Action

When Senator Proxmire introduced the original FCRA, he sought to preclude "the furnishing of information to Government agencies or to market research firms or to other business firms who are simply on fishing expeditions."[42] The implications of the affiliate sharing loopholes seem to return consumers to the unfair and unsafe data handling practices of the pre-FCRA era.

In sum, I believe that Congress needs to restore the FCRA to the higher level of its original protections for consumer privacy.

To do so, I recommend the following:

1. Eliminate the exemption for affiliate sharing from the definition of "consumer report" in the FCRA or allow the partial pre-emption clause in Section 624 to sunset on January 1, 2004.

2. Investigate the actual sharing practices of credit report information among affiliated companies and the uses of such data by the affiliated recipients that escape the protections of the FCRA. To this end, Congress should instruct each of the functional bank regulatory agencies and the Federal Trade Commission to investigate, audit and report to Congress on the actual sharing of consumer report information among affiliated companies and on the actual, unprotected uses of such data by the affiliated recipients.

Biographical Information

Joel R. Reidenberg is Professor of Law and a past Director of the Graduate Program in Law at Fordham University School of Law. He teaches courses in Information Privacy Law, Information Technology Law, International Trade, Comparative Law and Contracts. Professor Reidenberg writes extensively on fair information practice issues in the private sector and is the co-author with Paul Schwartz of two leading books on information privacy law: ON-LINE SERVICES AND DATA PROTECTION LAW: REGULATORY RESPONSES (EUR-OP: 1998) and DATA PRIVACY LAW (Michie : 1996). He has chaired the Section on Defamation and Privacy of the Association of American Law Schools (the academic society for American law professors) and is a former chair of the association's Section on Law and Computers. Professor Reidenberg served as a consultant to the Federal Trade Commission on Fair Credit Reporting Act issues and as an expert advisor on data privacy issues for state and local governments, the U.S. Congress Office of Technology Assessment, the European Commission and several foreign data protection agencies. Recently, he has provided assistance to the Attorney General of the State of Washington and to the County Counsel of San Mateo County, California in connection with privacy litigation. Prior to joining the faculty at Fordham, Professor Reidenberg practiced law in Washington, DC with the international telecommunications group of the national law firm Debevoise & Plimpton.

Professor Reidenberg received an A.B. degree from Dartmouth College, a J.D. from Columbia University, and both a D.E.A. and a Ph.D from the Université de Paris 1 (Panthéon-Sorbonne). He is admitted to the Bars of New York and the District of Columbia.

[1] Paul M. Schwartz & Joel R. Reidenberg, DATA PRIVACY LAW (Michie: 1996); Joel R. Reidenberg and Paul M. Schwartz, ONLINE SERVICES AND DATA PROTECTION LAW: REGULATORY RESPONSES (Eur-OP: 1998); Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies,* 54 HASTINGS L. J. -- (forthcoming); Lorrie Cranor & Joel R. Reidenberg*, Can user agents accurately represent privacy notices?*, TPRC 30th Research Conference Paper # 65 (2002) available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=328860>; Joel R. Reidenberg, *E-commerce and Trans-Atlantic Privacy* , 38 HOUSTON L. REV. 717 (2001); Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace* , 52 STANFORD L. REV. 1315 (2000); Joel R. Reidenberg *, Restoring Americans' Privacy in Electronic Commerce* , 14 BERKELEY TECH. L. J. 771 (1999): Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497 (1995); Joel R. Reidenberg & Francoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in Networks*, 30 WAKE FOREST L. REV. 105 (1995); Joel R. Reidenberg, *Rules of the Road on Global Electronic Highways: Merging the Trade and Technical Paradigms*, 6 HARVARD J. LAW & TECH. 287 (1993); Joel R. Reidenberg, *The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services*, 60 FORDHAM L. REV. S137 (1992); Joel R. Reidenberg, *Privacy in the Information Economy-- A Fortress or Frontier for Individual Rights?,* 44 FED. COMM. L. J. 195 (1992). Copies of most of my articles may currently be found on my web site at: <http://reidenberg.home.sprynet.com>

[2] See e.g. S. Rep. 91-517, 91st Cong., 1st Sess. (1969); Hearings on Commercial Credit Bureaus before the House Special Subcommittee on Invasion of Privacy of the Committee on Government Operations, 90th Cong., 2nd Sess., March 12-14, 1968; Hearings on Fair Credit Reporting S. 823 before the Senate Subcommittee on Financial Institutions of the Committee on Banking and Currency, 91st Cong., 1st Sess. (May 19-23, 1969)

[3] S. Rep. 91-517, 91st Cong., 1st Sess. 1 (1969)

[4] S. Rep. 91-517, 91st Cong., 1st Sess. 3, 8 (1969)

[5] See e.g. Hearing on "The Growing Problem of Identity Theft and Its Relationship to the Fair Credit Reporting Act" before the Senate Banking Committee, 108th Cong., 1st Sess. (June 19, 2003); Hearing on "Fair Credit Reporting Act: How It Functions for Consumers and the Economy" before the Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, 108th Cong., 1st Sess. (June 4, 2003); Hearing on "the Importance of the National Credit Reporting System to Consumers in the U.S. Economy" before the Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, 108th Cong., 1st Sess. (May 8, 2003).

[6] Hearing on "Fair Credit Reporting Act: How It Functions for Consumers and the Economy" before the Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, 108th Cong., 1st Sess. (June 4, 2003)(Statement of Julie Brill, Assistant Attorney General for Vermont)

[7] 15 U.S.C. 1681t(b)(1)(F)

[8] Hearing on "the Importance of the National Credit Reporting System to Consumers in the U.S. Economy" before the Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, 108th Cong., 1st Sess. (May 8, 2003) (Statement of Michael E. Staten, Director, Credit Research Center, McDonough School of Business, Georgetown University), at p. 6

[9] See Michael Turner, The Fair Credit Reporting Act: Access, Efficiency & Opportunity The Economic Importance of Fair Credit Reauthorization, at 65 (Information Policy Institute: June 2003)

[10] See Federal Reserve System, Rate of interest in money and capital markets: Prime Rate (not seasonally adjusted, twelve months ending in December) available at http://www.federalreserve.gov/releases/h15/data/a/prime.txt

[11] American Bankruptcy Institute, US Bankruptcy Filing Statistics: Households per filing, Rank (2003) (using "statistics based on data from the Administrative Office of the U.S. Courts (2002 bankruptcies) and the U.S. Bureau of the Census.") available at http://www.abiworld.org/stats/householdrank.pdf

[12] Federal Housing Finance Board, Periodic Summary Tables: Table IX—Terms on Conventional Home Mortgages 2002 available at http://www.fhfb.gov/MIRS/mirstbl9.htm

[13] Hearing on "Fair Credit Reporting Act: How It Functions for Consumers and the Economy" before the Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, 108th Cong., 1st Sess. (June 4, 2003)(Statement of Julie Brill, Assistant Attorney General for Vermont)
[14] See also, Robert Gellman, No Fair Fight over FCRA Provisions, DM News, May 5, 2003, pp. 12-13.
[15] See National Assoc. of Attorneys General, Press Release: Multistate Actions: 27 States and Puerto Rico Settle With Citibank (Mar. 1, 2002) available at http://www.naag.org/issues/20020301-multi-citibank.php
[16] See Minn. Attorney General Press Release, Minnesota Attorney General and US Bancorp Settle Customer Privacy Suit (July 1, 1999) available at http://www.ag.state.mn.us/consumer/privacy/pr/pr_usbank_07011999.html
[17] See N.Y. Attorney General Press Release, Fleet Bank Agrees to New Privacy Protections (Jan. 16, 2001) available at http://www.oag.state.ny.us/press/2001/jan/jan16b_01.html
[18] See N.Y. State Dept. of Law, Annual Report 2000, at 24 (2000) available at http://www.oag.state.ny.us/2000AnnualReport.pdf
[19] Harris Interactive/Privacy & American Business Poll, *Privacy On and Off the Internet: What Consumers want* (Feb. 7, 2002) available at http://www.aicpa.org/download/webtrust/priv_rpt_21mar02.pdf (53% of those polled reported a "major concern" while only 5% were 'not concerned' if "the company will use my information outside of the specific transaction for which it was intended (for example, to offer me other products and services)".)
[20] Hearing on "The Role of FCRA in the Credit Granting Process" before the House Committee on Financial Services Subcommittee on Financial Institutions and Consumer Credit, 108th Cong., 1st Sess. (June 12, 2003) (Statement of Martin Wong, General Counsel, Citigroup Global Consumer Group)(testifying that "Corporate structure is usually driven by concerns that do not affect the customer, such as the company's history of acquisitions or by corporate tax, legal, and accounting concerns.")
[21] Hearing on "The Role of FCRA in the Credit Granting Process" before the House Committee on Financial Services Subcommittee on Financial Institutions and Consumer Credit, 108th Cong., 1st Sess. (June 12, 2003) (Statement of Harry Gambil, CEO, Trans Union), at 8.
[22] Hearing on "The Role of FCRA in the Credit Granting Process" before the House Committee on Financial Services Subcommittee on Financial Institutions and Consumer Credit, 108th Cong., 1st Sess. (June 12, 2003) (Statement of Martin Wong, General Counsel, Citigroup Global Consumer Group), at 4.
[23] See MBNA Privacy Notice, http://www.mbna.com/privacy.html (visited June 23, 2003)
[24] See Minnesota v. US Bank (Settlement dated June 6, 1999) available at http://www.ag.state.mn.us/consumer/privacy/PR/pr_usbank_06091999.html (visited June 23, 2003); U.S. Bank, SEC Form Schedule 13D for Gargoyles (filed with the SEC, June 11, 1999) available at http://www.sec.gov/Archives/edgar/data/1016278/0001047469-99-023944-index.html
[25] See The Marmon Group: Companies, http://www.marmon.com/Companies.html (visited June 19, 2003)
[26] See The Marmon Group: Companies, http://www.marmon.com/Companies.html (visited June 19, 2003)
[27] See Great Universal Stores Interim Report 2002, at 2 (Nov. 21, 2002); GUS plc News: Great Universal Stores completes acquisition of Metromail Corporation, Apr. 4, 1998 available at http://www.gusplc.co.uk/gus/news/gusarchive/gus19998/1998-04-28
[28] See Dennis v. Metromail, No. 96-04451 (Travis Cty D. Tex., June 7, 1999). Settlement agreement available at http://www.entwistle-law.com/news/cases/settled/pdf/newmetronot.pdf
[29] See Experian's Scorecard Privacy Policy, http://scorecard.experian.com/creditexpert/common/privacy_policy.asp (visited June 24, 2003) ("We may disclose any of the information that we collect to our affiliated companies …. If you prefer that we do not share information with affiliated companies, you may opt-out of these disclosures.")
[30] 15 U.S.C. §§ 1681b(a)(3)(D), 1681b(a)(4), 1681f, 1681u.
[31] See e.g. Department of Defense, DARPA Report to Congress Regarding the Terrorist Information Awareness Program (May 20, 2003) http://www.darpa.mil/body/tia/TIA%20ES.pdf
[32] See Equifax, Annual Shareholders Report Form 10-K for the Fiscal Year Ended Dec. 31, 2002 (filed with the SEC on Mar. 23, 2003).
[33] Equifax Online Privacy Policy & Fair Information Principles (US Only) available at https://www.econsumer.equifax.com/consumer/forward.ehtml?forward=privacypolicy (visited June 24, 2003)

[34] Hearing on "The Growing Problem of Identity Theft and Its Relationship to the Fair Credit Reporting Act" before the Senate Banking Committee, 108th Cong., 1st Sess. (June 19, 2003)(Statement of Timothy Caddigan, Special Agent In Charge Criminal Investigation Division, U.S. Secret Service)

[35] See e.g. Hearing on "The Growing Problem of Identity Theft and Its Relationship to the Fair Credit Reporting Act" before the Senate Banking Committee, 108th Cong., 1st Sess. (June 19, 2003) (Statement of Michael D. Cunningham, Sr. Vice President, Credit and Fraud Operations, Chase Cardmember Services), at p. 3-4

[36] See See *Criminal Gangs Hitting Mailboxes for Credit Offers, Personal Data,* Privacy Times, June 16, 2003, at 2; U.S. Dept. of Justice, Identity Theft and Fraud, available at http://www.usdoj.gov/criminal/fraud/idtheft.html (visited May 28, 2003) ("What are the most common ways to commit identity theft or fraud? …. If you receive applications for 'pre-approved' credit cards in the mail, but discard them without tearing up the enclosed materials, criminals may retrieve them"); Hearing on "The Growing Problem of Identity Theft and Its Relationship to the Fair Credit Reporting Act" before the Senate Banking Committee, 108th Cong., 1st Sess. (June 19, 2003)(Statement of Timothy Caddigan, Special Agent In Charge Criminal Investigation Division, U.S. Secret Service)(the Secret Service advises Americans to "shred or burn pre-approved credit card applications"), at p. 8; Experian, All about Credit: Fraud Prevention Tips, available at http://www.experian.com/consumer/help/fraud/prevention.html (visited May 28, 2003); Trans Union, Avoiding Fraud available at http://www.transunion.com/content/page.jsp?id=/personalsolutions/general/data/AvoidingFraud.xml (visited May 28, 2003); Equifax, How Identity Theft Strikes, available at https://www.econsumer.equifax.com/consumer/forward.ehtml?forward=identitytheft_fraud (visited June 24, 2003)

[37] Michael E. Staten & Fred H. Cate, Paper prepared for the Privacy Leadership Initiative "The Adverse Impact of Opt-In Privacy Rules on Consumers: A Case Study of Retail Credit," at 25 (April 2002).

[38] See e.g. U.S. Dept. of State, Public Announcement: Philipines (March 7, 2003)(" The terrorist threat to Americans in the Philippines remains high") available at http://travel.state.gov/philippines_announce.html; U.S. Dept. of State, Public Announcement: India (Mar. 27, 2003) available at http://travel.state.gov/india.html

[39] See Fair Isaac, New Product Releases: Capstone Decision Manager, Falcon Fraud Manager for Issuers available at http://www.predictive.com.au/whatsnew.html (visited June 11, 2003).

[40] See http://www.predictive.com.au/contacts.html (visited June 11, 2003)

[41] US Dept. of State, Public Announcement: Malaysia (May 14, 2003) available at http://travel.state.gov/malaysia_announce.html

[42] Cong. Rec. Senate, Jan. 31, 1969 (statement of Sen. Proxmire) reprinted in Hearings on Fair Credit Reporting S. 823 before the Senate Subcommittee on Financial Institutions of the Committee on Banking and Currency, 91st Cong., 1st Sess., at 436 (May 19-23, 1969)