No. 04-16334; 04-16560

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

AMERICAN BANKERS ASSOCIATION,
THE FINANCIAL SERVICES ROUNDTABLE, and
CONSUMER BANKERS ASSOCIATION,

Plaintiff-Appellants,

vs.

BILL LOCKYER, in his official capacity
as Attorney General of California, et al.

Defendant-Appellees.

On Appeal from the United States District Court
for the Eastern District of California

Case No. S-04-0778 MCE KJM

BRIEF OF AMICI CURIAE AARP, ACLU OF NORTHERN CALIFORNIA, CALIFORNIA PUBLIC INTEREST RESEARCH GROUP, CONSUMER FEDERATION OF CALIFORNIA, CONSUMERS UNION, ELECTRONIC PRIVACY INFORMATION CENTER, EVAN HENDRICKS, NATIONAL ASSOCIATION OF CONSUMER ATTORNEYS, PRIVACY RIGHTS CLEARINGHOUSE, AND US PIRG, IN SUPPORT OF DEFENDANT-APPELLEES, SUPPORTING AFFIRMANCE

Chris Jay Hoofnagle
Electronic Privacy Information Center
1718 Connecticut Ave. NW 200
Washington, DC 20009
(202) 483-1140 x108
Attorney for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

AARP is a non-partisan, non-profit membership organization, which is tax-exempt under section 501(c)(4) of the Internal Revenue Code, dedicated to addressing the needs and interests of older Americans. AARP neither has a parent corporation, nor has it issued shares or securities.

The ACLU of Northern California is a 501(c)(4) organization, affiliated with the American Civil Liberties Union, a nationwide nonprofit, nonpartisan membership organization, which does not issue shares.

The California Public Interest Research Group, Inc. ("CALPIRG") is a statewide nonprofit organization that stands up for California's consumers. CALPIRG is organized under section 501(c)(4) of the IRS Code and has no parent corporation, nor has it issued shares or securities.

Consumer Federation of California is a non-profit public benefit corporation organized under section 501(c)(4) of the IRS Code. CFC does not have a parent corporation and has not issued any stock.

Consumers Union of U.S., Inc., is a nonprofit corporation organized under the laws of New York. It has no parent corporation, nor has it issued shares or securities.

The Electronic Privacy Information Center is a not-for-profit research center organized under section 501(c)(3) of the IRS Code. It has no parent corporation, nor has it issued shares or securities.

The National Association of Consumer Attorneys is a non-profit membership organization of law professors, public sector lawyers, private lawyers, legal services lawyers, and other consumer advocates. It is organized under the laws of the State of Massachusetts and is tax-exempt under section 501(c)(3) of the Internal Revenue Code. It has no parent corporation, nor has it issued shares or securities.

The Privacy Rights Clearinghouse is a nonprofit consumer information and advocacy organization. Its parent organization is the 501(c)(3) Utility Consumers' Action Network. Neither it nor the PRC has issued shares or securities.

U.S. PIRG is organized as an IRS 501(c)(4) non-profit corporation that conducts advocacy on behalf of its members; it has no parents or subsidiaries, nor has it ever issued stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Statutes

California Constitutional Provisions

State Statutes

Cases

Other Authorities

STATEMENT OF AMICI CURIAE

AARP is a non-partisan, non-profit organization with more than 35 million members nationwide aged 50 and older, including 2,900,000 members in California.[1] As the largest membership organization serving older Americans, AARP is greatly concerned about ensuring strong consumer protections in the marketplace that enhance economic security. AARP thus seeks to protect the financial and medical privacy rights of consumers, including measures that prevent identity theft. AARP supports state privacy laws that improve upon federal privacy protections. AARP believes that consumers' financial privacy shouldn't be considered incidental to the modernization of the financial services industry; rather, it should be an integral part of it.

The American Civil Liberties Union of Northern California is the regional affiliate of the American Civil Liberties Union (ACLU), a nationwide, nonprofit, nonpartisan membership organization with more than 400,00 members, dedicated to the defense and promotion of the guarantees of individual liberty contained in state and federal Constitutions. The ACLU believes that privacy is a critically important value in a free society. The ACLU strongly supported passage of SB1.

The California Public Interest Research Group, Inc. ("CALPIRG") is a statewide nonprofit organization that stands up for California's consumers.

---

[1] Consistent with FRAP 29(a), this brief has been filed with the consent of all parties. Shelley Curran of Consumers Union and EPIC Internet Public Interest Opportunities Program Clerk Katherine Oyama participated in the drafting of this brief.

CALPIRG has actively supported legislative measures in California, including SB1 and the bill's predecessors, which provide consumers with greater privacy protections. CALPIRG also researched, wrote and released a report called "Privacy Denied," which compared the privacy practices of several banks.

Consumer Federation of California ("CFC") is a federation of some 50 labor, senior and consumer organizations, which in turn represent well over one million Californians. CFC also has several hundred individual members. CFC has supported legislation at the state and federal level to give consumers greater privacy rights. CFC was very active in the legislative campaign to enact SB1.

Consumers Union is a non-profit membership organization chartered in 1936 under the laws of the State of New York to provide consumers with information, education, and counsel about goods, services, health and personal finance; and to initiate and cooperate with individual and group efforts to maintain and enhance the quality of life for consumers. Consumers Union actively supported the passage of the California Financial Information Privacy Act, the statute at issue in this case.

The Electronic Privacy Information Center ("EPIC") is a not-for-profit public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC is a leading national advocate on privacy issues, and its Advisory Board and staff members possess expertise on commercial exploitation of personal information. EPIC maintains a detailed Web site on privacy online at http://epic.org/.

Evan Hendricks is the Publisher of *Privacy Times*, the leading subscription-only newsletter covering privacy and freedom of information law and policy. He frequently testifies as an expert witness on credit reporting laws, and is the author of *Credit Scores and Credit Reports: How The System Really Works, What You Can Do*. *Privacy Times* is online at http://www.privacytimes.com.

The National Association of Consumer Attorneys ("NACA") is a non-profit group of attorneys and advocates committed to promoting consumer justice and curbing abusive business practices that bias the marketplace to the detriment of consumers. Its membership is comprised of over 1,000 law professors, public sector lawyers, private lawyers, legal services lawyers, and other consumer advocates across the country. NACA has established itself as one of the most effective advocates for the interests of consumers in this country. Its advocacy takes many forms, including conducting seminars on application of the Fair Credit Reporting Act and filing amicus briefs in support of American consumers affected by financial institution activities.

The Privacy Rights Clearinghouse ("PRC") is a nonprofit consumer information and advocacy organization. It was established in 1992 and is located in San Diego, California. The definition of privacy that the PRC espouses is the ability of the individual to control what is done with his/her personal information. The PRC believes that the ability of individuals to opt-out of the sharing of personal information among the affiliates of financial companies is a key component of consumer privacy protection. The PRC's web site is http://www.privacyrights.org.

U.S. PIRG serves as the non-profit, non-partisan national advocacy office for the state Public Interest Research Groups, which have half a million members nationwide. The state PIRGs and U.S. PIRG have long supported efforts to ensure the financial privacy of their members and of all Americans.

Amici have been actively involved in promoting the interests of U.S. and California consumers for decades. These organizations, with collective memberships or subscribers of approximately forty-one million consumers, are all national in scope and represent interests of consumers in areas related to the extension of credit and consumer privacy rights.

Many of these organizations were intimately involved in the enactment of the California Financial Information Privacy Act, popularly known as "SB1."[2] Many were also involved in the revisions to the Fair Credit Reporting Act ("FCRA"),[3] the privacy provisions of the Gramm-Leach-Bliley Act ("GLBA"),[4] and the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"),[5] which amended the FCRA.

Amici have strong interests in maintaining for consumers the reasonable privacy protections offered by SB1. SB1 was enacted to provide consumers with a greater ability to restrict how a dizzying array of financial institution affiliates

---

[2] Cal. Fin. Code §§ 4050 *et seq*. (2004).

[3] 15 U.S.C. § 1681-1681x (2004).

[4] 15 U.S.C. §§ 6801-6809 (2004).

[5] Pub. L. No. 108-159, 117 Stat. 1952 (2003).

share sensitive information collected about them. The information shared includes intimate details of a consumer's financial life, including income, marital status, and debt loads. The information may reveal sensitive facts about a consumer, such as religious and political affiliation and purchase patterns on credit or debit cards. *Amici* believe, and the California Legislature determined, that consumers should have a choice in the sharing of this type of information among affiliates. We therefore urge affirmance of the lower court's opinion.

SUMMARY OF ARGUMENT

At issue in this case is whether the strong privacy protections afforded by SB1 are preempted by the FCRA. We urge this Court to affirm the lower court in holding that the FCRA only preempts state law with respect to affiliate sharing of "consumer reports."

SB1 provides Californians with a critical tool to limit the exchange of detailed, personal information among financial institution affiliates. SB1 is a carefully constructed law that allows legitimate information sharing to continue while allowing consumers to place reasonable limits on information flows.

The choice that SB1 offers is more important now than ever, as the sharing of personal information is directly linked to risk of fraud and identity theft. New studies show that many identity theft cases can be traced to insiders—trusted employees with access to personal information. The more information is shared, the more insiders have access to personal information—a consumer's "financial DNA." SB1 gives individuals the choice to limit their risk of fraud and identity

theft by preventing the indiscriminate flow of personal financial information to all companies in an affiliate structure.

Amici urge this Court to consider carefully the breadth of preemption under the FCRA, and to limit it only to "consumer reports." A broader interpretation of preemption under the FCRA would lead to unintended consequences, including the invalidation of other important state regulation wholly unrelated to consumer reporting. Finally, *amici* explain that the appellants' interpretation of preemption is so broad that it would undermine the national credit reporting system and rob individuals of important rights extended under the FCRA.

For the foregoing reasons, *amici* respectfully urge this Court to affirm the ruling of the lower court.

ARGUMENT

A dizzying array of financial institutions, including banks, brokerage houses, and insurers, is allowed to affiliate under federal law. Once affiliated, these companies share individuals' sensitive personal information, including income, marital status, purchase histories, credit scores, and employment information. SB1 provides individuals with a reasonable opportunity to limit the scope of this sharing.[6]

Signed by the Governor in August 2003 after a multiple session legislative effort, SB1 requires financial institutions to obtain the affirmative consent of consumers before sharing their personal information with non-financial third

[6] Cal. Fin. Code § 4050 *et seq.* (2004).

parties. SB1 also allows consumers to opt-out of sharing information among non-affiliated third parties who have entered financial joint marketing agreements.[7] At issue in this case is an equally important provision that requires financial institutions to allow consumers to opt-out of information sharing among some affiliated companies.[8]

This right to opt-out of affiliate sharing is important for individuals' privacy and for the prevention of fraud, as the breadth of unbridled disclosure among affiliates, and the subsequent consequences to consumers, cannot be overestimated. For example, in hearings before Congress on the FCRA amendments, Senator Boxer noted that CitiGroup has 1,630 affiliates, Bank of America has 1,323 affiliates, JP Morgan has 967 affiliates, and Wachovia Corporation has 886 affiliates.[9] The sheer volume of such disclosures, absent consent, underscores the importance of SB1 in protecting the financial privacy of California consumers. Without SB1, consumers would have no opportunity to limit the use of their personal information among these networks of companies.

In passing SB1, California was exercising its historic power to protect privacy and consumer protection.[10] Privacy is a special concern for Californians. California is one of only ten states with an explicit constitutional right to privacy,

---

[7] Cal. Fin. Code § 4053(a) (2004).

[8] Cal. Fin. Code § 4053(b) (2004).

[9] 149 Cong. Rec. S13874 (Nov. 4, 2003) (statement of Sen. Boxer).

[10] Consumer protection has long been recognized as an area of state police power regulation. *California v. ARC America Corp.*, 490 U.S. 93 (1989).

and the California right not only prohibits the State from committing privacy intrusions, but also applies that provision to the private sector:

> SECTION 1. All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.[11]

I. SB1's Provisions Provide Californians With a Meaningful Tool to Exercise Control Over Their Personal Information

The potential advantages of unlimited affiliate sharing come at a significant social cost: the rejection of the public's desire for more control over the dissemination of personal information. SB1 provides individuals with a level of control over their personal information while allowing the banking industry to perform critical functions, such as information sharing for fraud control.

While the banks have argued that affiliate sharing confers benefits to consumers, the California legislature has determined that consumers should be able to choose whether those alleged benefits outweigh the loss of privacy.

A. SB1's Exemptions Will Allow Critical Banking Activities to Continue While Providing Individuals with Privacy

SB1 was carefully crafted by the California Legislature to allow critical information sharing at a consumer's request and for anti-fraud purposes. In urging preemption of SB1, *amici* supporting Appellants did not fully appreciate how the law accommodates certain information sharing activities. Contrary to the

---

[11] CAL. CONST., ART. I § 1 (2004).

representations of America's Community Bankers ("ACB"),[12] critical bank activities can continue under SB1. SB1 permits consumers to opt-out of some affiliate sharing, but also creates other categories of sharing that remain authorized regardless of consumer choice.

The ACB *amicus* letter leaves the impression that all affiliate sharing under SB1 is banned. That letter includes references to alleged benefits of information sharing including, "Assessing Consumer Needs," "Providing Quick Access to Products/Services," and "On-Line Product Offerings."[13] While it is unclear whether information sharing among affiliates truly provides consumers with demonstrable benefits,[14] nothing in SB1 prevents a financial institution from informing consumers of all the potential benefits in order to persuade consumers not to opt out.

---

[12] *Amicus* Letter of America's Community Bankers in Support of Appellants American Bankers Association, et al. at 4-5 (herein, "ACB *amicus* letter").

[13] *Id.*

[14] If financial institutions are saving money by affiliate sharing, they do not appear to be sharing the benefits with consumers. According to the most recent Federal Reserve report on financial services fees and services, large institutions are generally increasing fees and lowering the number of services offered. The Federal Reserve found: "Of the fourteen fees for which comparisons are available…multistate banks charged significantly higher fees in eight cases and in no case charged a significantly lower fee." FEDERAL RESERVE, ANNUAL REPORT TO THE CONGRESS ON RETAIL FEES AND SERVICES OF DEPOSITORY INSTITUTIONS 8 (June 2003), *available at* http://www.federalreserve.gov/boarddocs/rptcongress/2003fees.pdf Further, the Federal Reserve found that: "Of the twenty-four measures that may be considered indicators of service availability, six changed a statistically significant amount, and five of these were in the direction of less service availability." *Id.* at 1.

ACB also raises "One-Stop Call Centers" and "Consolidated Billing Statements/Operations Centers" as benefits from information sharing among affiliates.[15] To the extent that their letter implies that these alleged benefits will be lost, they significantly overstate the scope of the statute. SB1 includes specific instances when financial institutions may share information in order to perform these banking activities. Section 4056(b)(1) allows information sharing that is "necessary to effect, administer or enforce a transaction requested by a consumer." The definition of "necessary to effect, administer, or enforce" includes activities to "service or maintain the consumer's account." Additionally, Section 4056(b)(2) allows information sharing with the consent or at the direction of the consumer. Under these sections, a consumer may contact a call center and ask the representative to access their information in all lines of business. Or, affiliates may provide information to a single affiliate responsible for account statements and then provide consumers a consolidated account statement. In fact, Section 4053(b)(1) includes a provision that expedites customer service in either instance as it allows for shared databases.

ACB references "Fraud Prevention" as a benefit to information sharing. SB1 specifically allows financial institutions to share information regardless of consumer choice in order to prevent fraud. Section 4056(b)(3)(B) allows the release of information to protect consumers against actual or potential fraud.

---

[15] ACB *amicus* letter at 4-5.

Section 4056(b)(3)(C) allows information sharing required for institutional risk control.

Finally, representations about the importance of the national credit system[16] are not relevant here—SB1 does not interfere with the ability of creditors or other furnishers of information to report to consumer reporting agencies. SB1 simply gives individuals an option that the banks will not—the ability to place some limit on the sharing of their financial DNA among hundreds or even thousands of affiliated companies.

Some bank representatives removed their opposition to SB1 immediately before the legislation was enacted and described it as a workable, fair compromise. Some also expressed a preference for a national standard, but such a standard is not relevant to this case. John Ross, a lobbyist who represented CitiGroup, was quoted in the *American Banker* saying, "We were part of this and are pleased with the work done -- it's a good fair result for everyone."[17] Mike Knudsen, a lobbyist for Wells Fargo, said, "We prefer a national approach, but we remove our opposition."[18]

---

[16] *Amicus* Brief of Citizens for a Sound Economy in Support of Appellants American Bankers Association, et al. at 4-5.

[17] Laura Mandaro, *Growling Over Calif. Privacy Act Won't Fade; B of A skipped talks, still a foe; seeking a national standard*, THE AMERICAN BANKER, Aug. 25, 2003.

[18] *Id*.

In a press release, the California Bankers Association announced, "We believe that, with the latest changes, this proposal qualifies as both reasonable and workable in many, but not all, aspects…We want to be clear that CBA would much prefer a national standard to a patchwork of state or local privacy laws."[19]

Appellants assert that information sharing benefits consumers, but the California State Legislature has decided that Californians have a strong interest in limits to information sharing. Information sharing does in some contexts benefit customers; in others it harms them. The State of California adopted legislation to maximize the benefits of information sharing while safeguarding the privacy interests of consumers. They included in SB1 exemptions that allow specific forms of beneficial information sharing among affiliates while allowing individuals to exercise choice for all other forms of information sharing among affiliates. Appellants now seek to eviscerate these statutory safeguards and to substitute their own judgment about the benefits and risks of information sharing for the judgment of the elected representatives of the people of California.

B. Public Opinion Strongly Supports Curbs on Information Sharing

Amici emphasize the public's strong desire to control the sharing of their information among financial institutions. As early as 1991, a Time/CNN poll found that 93 percent of respondents believed that the law should require

---

[19] CALIFORNIA BANKERS ASSOCIATION, CALIFORNIA BANKERS ASSOCIATION STATEMENT ON FINANCIAL PRIVACY (Aug. 14, 2003).

companies to obtain permission from consumers before selling their personal information.[20] More recently, AARP Research found that:

> Eighty-one percent of respondents opposed the internal sharing of customer personal and financial information by corporate affiliates. Only 10% supported it, and the majority of these said that affiliated companies should be required to notify and obtain written permission from customers before sharing their personal information.[21]

Privacy is a strong concern for Californians. A February 2003 survey conducted by Fingerhut Associates found that 91 percent of California voters favored an initiative measure that "would require a bank, a credit card company, insurance company, or other financial institution to notify a customer and receive a customer's permission before selling any financial information to any separate financial or non-financial company."[22] In enacting SB1, the California Legislature acted upon this important concern, and chose to give consumers the right to protect their privacy.

Public polling further indicates that individuals think that the ability to limit information sharing is important, and they will exercise opt-out rights when they are available. Recent polls indicate that individuals regularly claim that they have

---

[20] TIME-CNN, PRIVACY POLL, 1991.

[21] AARP RESEARCH, AARP MEMBERS' CONCERNS ABOUT INFORMATION PRIVACY (Feb. 1999), *available at* http://research.aarp.org/consume/dd39_privacy.html.

[22] CONSUMER FEDERATION OF CALIFORNIA, FINANCIAL PRIVACY INITIATIVE PRESS STATEMENT, Jan. 2003, *available at* http://www.consumerfedofca.org/bin/view.fpl/551008/article/730.html.

withheld personal information or have requested that they be removed from marketing lists. In a February 2002 Harris Poll, 83 percent of respondents had asked a company to remove their names and addresses from mailing lists.[23] An April 2001 study performed by the American Society of Newspaper Editors found that 70 percent of respondents had refused to give information to a company because it was too personal and 62 percent had asked to have their name removed from marketing lists.[24]

This popular support and willingness to act manifests itself when consumers are actually given the opportunity to vote on matters of privacy. In a ballot referendum, voters in North Dakota favored requiring financial institutions to obtain the affirmative consent (opt-in) of consumers before sharing information with third parties over opt-out, which was favored by the Legislature and banks. Although proponents of stronger privacy protections were outspent by seven to

---

[23] HARRIS INTERACTIVE, PRIVACY ON AND OFF THE INTERNET: WHAT CONSUMERS WANT (Feb. 19, 2002).

[24] AMERICAN SOCIETY OF NEWSPAPER EDITORS FREEDOM OF INFORMATION COMMITTEE AND THE FIRST AMENDMENT CENTER, FREEDOM OF INFORMATION IN THE DIGITAL AGE (Apr. 3, 2001).

one,[25] the North Dakota financial privacy initiative passed with the support of seventy-three percent of the voters.[26]

When California voters had the opportunity to vote on matters of privacy in 1972, sixty-two percent supported the amendment that added a right to privacy as an inalienable right in the State Constitution.[27]

II. Affiliate Sharing Can Expose Consumers to Risk; SB1 Allows Individuals to Have a Choice in the Matter

Absent SB1's "opt-out" provision, consumers in California are stripped of all meaningful control over the dissemination of their personal information among hundreds or thousands of affiliates. Because of the sheer number of affiliates of some financial institutions, it is essentially impossible for consumers to understand how personal information provided to a single entity will be disclosed across the entity's affiliate structure, let alone to take steps to safeguard privacy.

Consumers are wary that every time personal information is transferred to another affiliate, the risk of fraud and identity theft increases, as the data is available to more and more insiders and any additional people to whom the insiders permit access. As discussed below, affiliate-shared information has been

---

[25] *See* NORTH DAKOTA SECRETARY OF STATE, CITIZENS FOR NORTH DAKOTA'S FUTURE YEAR END MEASURE REPORT (2002)($193,000 raised); *cf.* NORTH DAKOTA SECRETARY OF STATE, PROTECT OUR PRIVACY'S YEAR END MEASURE REPORT (2002)($27,000 raised).

[26] NORTH DAKOTA SECRETARY OF STATE, OFFICIAL ELECTION RESULTS (Jun. 11, 2002).

[27] UNIVERSITY OF CALIFORNIA-HASTINGS, CALIFORNIA BALLOT PROPOSITIONS DATABASE, CAL. PROP. 11 (1972).

used to defraud customers, and its disclosure has placed older persons and those experiencing financial difficultly at greatest risk.

A. Insider Access to Personal Information That Appellants Seek Contributes to Identity Theft

Information sharing can exacerbate identity theft, a crime where an impostor uses personal data to commit fraud in another's name. A 2003 report released by the Federal Trade Commission shows that identity theft is a much bigger problem than public policy makers had previously realized. In that study, 12 percent of respondents reported that their personal information had been used to commit fraud in the last five years.[28] In cases where the victim knew how their personal information was stolen, 23 percent reported that their personal information was stolen by someone at a company or financial institution with access to their data.[29]

A news report covering a forthcoming study from the Michigan State University indicated that a researcher found in a review of 1,000 identity theft cases that between 50-70 percent were insider jobs:

> [The] director of an identity theft program at Michigan State, randomly selected 1,037 cases from around the country, then painstakingly traced each incident to its origins. In 50 percent of the cases, the victim's identity was originally pilfered by a company employee. In

---

[28] FEDERAL TRADE COMMISSION, IDENTITY THEFT SURVEY REPORT (Sept. 2003), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf.

[29] *Id.* at 29.

> another 20 percent of cases, evidence strongly suggested dirty play by an insider.[30]

Insider risks are so severe that the Office of the Comptroller of the Currency has warned banks that organized crime rings were placing low-level employees in financial institutions to commit fraud. In an April 2002 security alert, the agency warned:

> …[I]ndividuals are being encouraged by gang members to apply for teller positions at financial institutions for the sole purpose of providing access to the institution's operating systems and customer access information.[31]

Every time information is shared with a network of affiliates, identity theft is easier and more likely to occur. It is possible that a single entity collecting personal data may have a relatively secure technology platform to protect against computer hackers and other types of security breaches. Upon investigation, a consumer may even feel comfortable providing such an entity with sensitive information in exchange for potential customer service benefits. However, it is a practical certainty that at least one of the hundred and potentially thousands of affiliates with whom the collecting entity may share personal information—as well as contractors who have access to information—will not employ equivalent

---

[30] Bob Sullivan, *Study: ID theft usually an inside job; Up to 70 percent of cases start with employee heist*, MSNBC, May 21, 2004, *available at* http://www.msnbc.msn.com/id/5015565/.

[31] OFFICE OF THE COMPTROLLER OF THE CURRENCY, IDENTITY THEFT: ORGANIZED GANG AND TELLER COLLUSION SCHEMES (Apr. 25, 2002), *available at* http://www.occ.treas.gov/ftp/alert/2002-4.txt.

technical and physical security standards. Variations in technology, personnel, and resources dictate that the protection of sensitive consumer information is inconsistent across affiliates. Aside from abandoning modern financial services all together, perhaps by keeping one's money in a mattress, laws such as SB1 provide the only option to limit transfer of personal information among affiliates and the corresponding risks of disclosure.

Only recently has the frequency of security breaches into databases containing sensitive personal information come to light. After the passage of Cal. Civ. Code §1798.82, which requires institutions to disclose breaches in the security of personally identifiable data, numerous educational institutions, including San Diego State University and the University of California at San Diego, warned students that they were at risk for identity theft after hackers accessed university servers containing names, driver's license and social security numbers.[32]

In the financial services industry, security breaches into customer databases pose an even greater threat due to the sensitive nature of the stored information and the potential for economic harm caused by identity theft. In November 2003, a thief obtained the names, addresses and social security numbers of thousands of Wells Fargo customers after breaking into the office of a business consultant and stealing computers.[33] This incident illustrates the validity of consumer concerns

---

[32] *UC-San Diego Database Hacked,* ASSOCIATED PRESS, May 7, 2004.

[33] David Lazarus, *A Simple Theft Nets Wells a World of Woe: Break-in Behind Bar Puts Clients' Data at Risk,* SAN FRAN. CHRON., Nov. 21, 2003.

regarding the insecure nature of data sharing. The stolen computers belonged to an outside marketing consultant who reportedly failed to observe Wells Fargo's security protocols.[34]

In March 2004, a Bank of America employee in Santa Ana, California was sentenced to state prison for stealing identity and account information for over 740 Bank of America customers.[35]

Obviously, financial institutions cannot ensure that information is perfectly secure; therefore, it is imperative to at least give consumers the ability to do everything they can to protect themselves from the spread of their personal information to affiliates. SB1 does this in part by conferring an opt-out right on consumers for the sharing of information by financial institutions with certain types of affiliates.

The frequency of security breaches at leading financial institutions and elsewhere suggests that information sharing among affiliates can increase the likelihood of consumer harm. These security breaches can readily result in fraud on the consumer. Consumers, therefore, are legitimately concerned that the greater number of affiliates accessing their information, the greater the possibility of identity theft. SB1 allows information sharing for anti-fraud purposes to continue while allowing individuals to reduce their risk of identity theft by opting out of indiscriminate affiliate sharing.

---

[34] *Id*.

[35] *Identity Theft*, CITY NEWS SERVICE, Mar. 5, 2004.

B. Older Persons and Individuals Experiencing Financial Difficulty Are Most At Risk

Disclosure of personal information can expose older persons and other at-risk consumers to an increased likelihood of deception. For example, the Securities and Exchange Commission ("SEC") accused NationsBank[36] of sharing with its affiliated securities company data on bank customers with low-risk, maturing federally insured CDs.[37] The SEC alleged that the affiliate, NationsSecurities, then aggressively marketed high-risk investments to these conservative investors, misleading many customers to believe that the investments were as safe and reliable as federally insured CDs. Many customers, including retired persons, lost significant portions of their life savings.

After an investigation, the SEC alleged that the companies intentionally blurred the distinction between the bank and the brokerage, and between the insured CDs and riskier investment products. Affiliate sharing of customers' information facilitated this deception. According to the SEC, NationsBank provided the investment representatives with maturing CD customer lists, as well as customers' bank or financial statements and even account balances. As a result, when these investment representatives called NationsBanks' customers and indicated that they were with the "investment division" of the bank, many customers reasonably believed that they were bank employees, not brokers.

---

[36] NationsBank has merged with Bank of America.

[37] *In the matter of NationsSecurities and NationsBank, N.A.*, SEC Order Instituting Cease and Desist Proceedings, No. 3-9596, May 4, 1998, *available at* http://www.sec.gov/litigation/admin/337532.txt.

NationsBank is not the only bank to have engaged in such a practice. First Union settled a private lawsuit alleging similar practices.[38]

A 2004 Federal Trade Commission study found that nearly 25 million adults in the United States, or 11 percent of the adult population, were victims of fraud during a one-year period.[39] AARP notes that, "Older persons can be an appealing target for such thefts because they typically have significant available credit to draw on..."[40]

The Federal Trade Commission study also shows that consumers with high levels of debt were more likely to be victims of fraud. Three of the top four categories of fraud related to credit, including credit-repair scams that are often targeted at individuals who already carry high debt loads or have bad credit. The practice among financial institutions to share lists of individuals with bad credit is a primary factor in perpetuating deceptive schemes. Given the inability of financial institutions to keep track of their affiliates' later use of shared customer

---

[38] *Risky Business in the Operating Subsidiary: How the OCC Dropped the Ball, Hearing Before the Subcommittee on Oversight and Investigations of the House Committee on Commerce.*, 106th Cong. (June 25, 1999) (statement of Jonathan Alpert, Sr. Partner, Baker and Rodems).

[39] FEDERAL TRADE COMMISSION, FTC RELEASES CONSUMER FRAUD SURVEY: MORE THAN ONE-IN-10 AMERICANS FELL VICTIM TO FRAUD (Aug. 5, 2004).

[40] Neal Walters, *The Fair Credit Reporting Act: Issues and Policy Options*, AARP PUB. POL. INST. at 4 (Jan. 2003), *available at* http://research.aarp.org/consume/ib58_credit.html.

information, "opt-out" provisions serve a critical role in enabling consumers to reduce the risk that they will be targeted for deceptive credit schemes.

III. Appellants' Interpretation of FCRA Preemption Is Overbroad

A. If Adopted, Appellants' Interpretation of Preemption Would Undermine A Broad Range of State Law

The lower court properly interpreted the preemption provisions of the FCRA, limiting their application to consumer reports, rather than to all affiliate sharing. Such an interpretation of the statute is necessary; otherwise a host of laws in areas in which Congress has explicitly allowed states to regulate privacy would be invalidated. As Vermont Assistant Attorney General Julie Brill cautioned the U.S. Senate:

> If context plays no role, then the FCRA could be held to prohibit a state law limiting or regulating the exchange of *any* kind of information under *any* circumstances, not just the type of information and activity regulated by the FCRA; under such a strained reading, state statutes prohibiting conspiracy, dissemination of stolen trade secrets, defamation, and a host of other types of "information" that could be "exchanged" would be preempted.[41]

---

[41] *Hearing on Affiliate Sharing Practices and Their Relationship to the Fair Credit Reporting Act, Before the Senate Committee on Banking, Housing and Urban Affairs*, 108 Cong. 1st Sess. (Jun. 26, 2003) (statement of Julie Brill, Assistant Attorney General, Vermont). We note here that although in a previous case, a court construed FCRA preemption as applying only to "confidential consumer information," the FCRA does not specify that it only applies to "confidential" or "consumer" information. *Bank of Am., N.A. v. City of Daly City*, 279 F. Supp. 2d 1118 (D. Cal. 2003), *vacated as moot by, Bank of Am., NA v. Alameda County*, 2004 U.S. App. LEXIS 14582 (9th Cir. May 14, 2004).

An interpretation that limits preemption of affiliate sharing to consumer reports, on the other hand, soundly fits into the purposes and structure of the FCRA. The FCRA is supposed to, among other things, enhance public confidence in the banking system.[42] It would be fundamentally inconsistent with the purpose of the FCRA to allow for broad, unaccountable and secret use of personal information among hundreds or even thousands of affiliates, as sought by appellant.

A broad interpretation of preemption in the FCRA would cause businesses to race to the bottom—or rather to the top—by affiliating with national financial institutions in order to escape all state privacy regulation. For instance, in order to gain access to an unlimited amount of personal information about individual customers, a neighborhood grocery store need only enter into an affiliate relationship with a financial institution, such as a subsidiary of a holding company of a national bank. Rather than sharing aggregate data about the purchasing trends of their customer portfolios, the local store and national bank could exchange information linked directly to an individual's personal account. Through affiliate sharing, a local store could potentially gain access to—and use—an individual's

---

Therefore, a broad interpretation of the FCRA could endanger unrelated criminal laws. Furthermore, even if FCRA preemption were limited to "confidential consumer information," a broad interpretation could endanger unrelated state information privacy and consumer protection laws.

[42] 15 U.S.C. § 1681(a)(1) (2004).

mortgage, shopping, banking, and investment account histories without his or her knowledge or consent.

B. If Adopted, Appellants' Interpretation of Preemption Would Undermine the Credit Reporting System and the FCRA's Guarantees of Transparency and Correction

Broad exemptions from state regulation of affiliate sharing will undermine the credit reporting system, as it will allow institutions to amass significant databases containing consumer report type information outside of the time-tested procedural and substantive rights conferred by the FCRA. When financial institutions use credit reports to determine consumers' eligibility and terms of credit agreements, consumers enjoy certain protections under the FCRA. For example, if a consumer is denied a financial product or service the consumer may obtain a free copy of the credit report. Furthermore, consumers may see, report, and dispute errors in their reports. These provisions promote accuracy and accountability in the use of personal information by financial institutions. Such protections do not exist if credit decisions are made based upon information that is shared secretly among affiliates of financial institutions.

The FCRA was enacted in 1970 after abuses of the consumer reporting agencies came to the attention of Congress. Consumer reporting agencies were requiring investigators to fill quotas of derogatory information on individuals; investigators were fabricating data; investigators were collecting lifestyle information, including sexual orientation, cleanliness, and drinking habits; and

agencies were maintaining outdated information.[43] The FCRA remedied the practices by flatly prohibiting some, while subjecting others to a system of "fair information practices." These include rights to receive a free report when a consumer has been denied credit,[44] standards of accuracy,[45] and a requirement that obsolete data be expunged from a report.[46]

None of these protections exist when companies can amass information outside the definition of "consumer reports." If the lower court is reversed and an overly broad reading of the FCRA preemption is adopted, financial institutions will create massive, in-house credit reporting operations based on personal information. For example, Citicorp has already stated in testimony to Congress that it shares affiliate information to verify consumer creditworthiness.[47]

Over time, this development of a parallel, unregulated set of private databases will undermine the national credit reporting system, as institutions will rely on internal data not subject to the accountability measures imposed on normal

---

[43] Robert Ellis Smith, BEN FRANKLIN'S WEB SITE, PRIVACY AND SECURITY FROM PLYMOUTH ROCK TO THE INTERNET 316-18 (Privacy Journal 2000).

[44] 15 U.S.C. § 1681m (2004) .

[45] 15 U.S.C. § 1681b, i (2004).

[46] 15 U.S.C. § 1681c (2004).

[47] *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. (Jun. 12, 2003) (statement of Martin Wong, General Counsel, Citigroup Global Consumer Group).

consumer reporting agencies. This could result in a return to pre-FCRA era practices or to new types of abuses.

C. If Adopted, Appellant's Interpretation of Preemption Would Accelerate First Degree Price Discrimination and Customer Exclusion

Allowing unaccountable and secret use of any collection of personal information among affiliates could lead to unfair and discriminatory practices. The potential uses of the data are not limited to marketing. The information collected and data mined may be employed for nascent or unforeseeable business practices. For instance, one growing problem is "first-degree price discrimination," a practice where businesses attempt to "perfectly exploit the differences in price sensitivity between consumers."[48] As Janet Gertz explained recently in the San Diego Law Journal:

> By profiling consumers, financial institutions can predict an individual's demand and price point sensitivity and thus can alter the balance of power in their price and value negotiations with that individual. Statistics indicate that the power shift facilitated by predictive profiling has proven highly profitable for the financial services industry. However, there is little evidence that indicates that any of these profits or cost savings are being passed on to consumers. For this reason, and because most consumers have no practical ability to negotiate price terms for the exchange of their data, many

---

[48] Anthony Danna & Oscar H. Gandy, Jr., *All That Glitters is Not Gold: Digging Beneath the Surface of Data Mining*, 40 JOURNAL OF BUSINESS ETHICS 373, 381 (2002) (herein, "Danna & Gandy"); *see also* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607 (Nov. 1999).

> characterize the commercial exploitation of consumer transaction data as a classic example of a market failure.[49]

Through price discrimination and the use of information within unaccountable affiliate structures, the costs of financial services could increase for many consumers, and companies could engage in monopolistic practices.

Another emerging problem is "customer exclusion." Information flows among affiliates can be used to eliminate certain customers from commercial opportunities. There is a movement in the profiling field that would systematically exclude customers if they are not profitable to the business. As Professors Danna and Gandy explain:

> Many firms come to the conclusion that low margin customers are not worth the effort necessary to turn them into high margin customers. The easiest thing to do is to entice those customers to leave…Peppers and Rogers…have recommended placing customers into a three-tier hierarchy, based on a calculation of potential value: 'Most Valuable Customers, Most Growable Customers, and Below-Zeros.' According to Peppers and Rogers, Below-Zeros represent 'the flip side of the Pareto Principle—the bottom 20 percent who yield 80 percent of losses, headaches, collection calls, etc.'[50]

Leaders in the information profiling field have started recommending to businesses that they use their access to personal information to create disincentives

---

[49] Janet Dean Gertz, *The Purloined Personality: Consumer Profiling in Financial Services*, 39 SAN DIEGO L. REV. 943, 964-65 (Summer 2002).

[50] Danna & Gandy at 381 *citing* F. Newell, LOYALTY.COM: CUSTOMER RELATIONSHIP MANAGEMENT IN THE NEW ERA OF INTERNET MARKETING (McGraw-Hill, New York 2000).

for certain customers.[51] One was quoted suggesting that retailers "should consider a preferred-customer database—prefer that they don't shop here."[52]

SB1 gives consumers a simple tool to resist these trends in financial services—the right to say no to information sharing among financial services affiliates.

CONCLUSION

For the foregoing reasons, *amici* urge this Court to affirm the decision of the U.S. District Court for the Eastern District of California.

Dated: September 8, 2004

Respectfully submitted,

By:_____

Chris Jay Hoofnagle
Attorney for Amici Curiae
Electronic Privacy Information Center
1718 Connecticut Ave. NW 200
Washington, DC 20009
(202) 483-1140 x108

---

[51] Mickey Alam Khan, *Technology Creates Tough Environment for Retailers*, DMNEWS, Jan. 13, 2003, *available at* http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=22682.

[52] *Id.*

CERTIFICATE OF COMPLIANCE

I certify that pursuant to Fed. R. App. P. 29(d) and 9th Cir. R. 32-1, the attached amicus brief is proportionally spaced, has a typeface of 14 points or more and contains 7000 words or less.

_____

Chris Jay Hoofnagle

CERTIFICATE OF SERVICE

I hereby certify that on this 8th day of September, 2004, two copies of the foregoing amicus curiae brief were served on the following by First Class U.S. mail and by electronic mail:

Counsel for Appellants:

E. Edward Bruce
Stuart C. Stock
Keith A. Noreika
Covington & Burling
1201 Penn. Ave. NW
Washington, DC 20004
<ebruce@cov.com>

Counsel for Appellees:

Susan Henrichsen
Catherine Ysreal
Department of Justice
110 West A St.
San Diego, CA 92101
<Susan.Henrichsen@doj.ca.gov>

Kimberly Gauthier
Judith A. Carlson
Department of Corporations
1515 K St., Suite 200
Sacramento, CA 95814
<KGAUTHIE@corp.ca.gov>

_____

Chris Jay Hoofnagle