Comments of the Electronic Privacy Information Center to the
Federal Trade Commission Workshop on Information Flows
FTC File No. P034102
June 18, 2003

Pursuant to the notice published by the Federal Trade Commission regarding the costs and benefits of information flows, the Electronic Privacy Information Center (EPIC) submits the following comments.[1] EPIC is a 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. We commend the Commission for hosting this public workshop on the costs and benefits that result from consumer information flows.

The information brokerage industry has presented policymakers with a Hobson's Choice on consumer information flows—either information can be exploited by businesses for any purpose or privacy laws can be enacted that will proscribe all use of personal information. The Commission should not be distracted by this false dilemma. The real issue here is whether those who enjoy the benefits of personal data should also bear responsibilities for fair use of individuals' information. To focus the debate, our comments below summarize Fair Information Practices (FIPs) and propose that such practices can provide a method for measuring the costs and benefits of information flows. The public benefits from open and transparent flows, consistent with FIPs, where the control of the information resides with the individual.

Information flows alter the power relationship among individuals, businesses, and government entities. The public is sensitive to changes in this relationship, and supports a framework of FIPs in law for handling of personal information. The second section of our comments demonstrates this strong support for FIPs. The third section discusses industry-sponsored studies that have employed dubious research methods in order to steer public debate towards self-regulation. This section also provides a framework for the Commission to evaluate studies on the costs and benefits of information flows.

[1] Federal Trade Commission, Public Workshop: Information Flows: The Costs and Benefits to Consumers and Businesses of the Collection and Use of Consumer Information, 68 Fed. Reg. 20389 (Apr. 25, 2003).

Business information flows lay the groundwork for law enforcement or other government access to personal information. The fourth section of our comments explains how many large information brokers have sold personal information to the government with little apparent oversight or controls. This is a new "cost" of a lack of information privacy rarely considered by policymakers.

The fifth section of our comments summarizes the commercial sale of personal information, which includes databases of financial information, identifiers, and even medical information. These information flows impose real costs on consumers, including a loss of dignity, and wasted time and frustration with unwanted telemarketing, spam, and direct mail.

Information broker lobbyists employ a series of unverifiable or specious claims to support unrestricted secondary use of personal information. The Commission should not accept these claims unless they can be supported with cogent arguments and demonstrable evidence. These claims include promises of lower prices, consumer desire for personalization, fewer solicitations, more consumer choice, and reduced fraud. In fact, personal information can be used to increase prices, to deny consumer choice, and to commit fraud. We explain examples of each of these risks in the last section of this submission.

Fair Information Practices Apportion Rights and Responsibilities in Personal Data

Fair Information Practices, principles that set out the rights and responsibilities of data subjects and data collectors, are central to the understanding of the consumer perspective on privacy. The Organization of Economic Cooperation and Development (OECD) articulation of FIPs takes the form of eight data guidelines, or "principles," for addressing the collection and maintenance of personal information.[2] The OECD specifies that these principles are the minimum standards for the protection of privacy. Policymakers are encouraged to establish protections that go beyond the eight principles to guarantee the privacy and security of personal data.

[2] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Organization of Economic Cooperation and Development (1980), at http://www1.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM; Marc Rotenberg, Privacy Law Sourcebook 326 (2002).

Collection Limitation

First, the collection limitation principle specifies that information should be collected lawfully and fairly, and with the consent of the data subject. Collection limitation also implies that data collectors should "minimize" their data collection. That is, only the minimum amount of data necessary to process a transaction should be collected. This principle often has been overlooked in American e-commerce. In fact, many of the profilers in the "Customer Relations Management" industry urge businesses to collect the maximum amount of information from individuals.[3] There are substantial benefits to following a policy of minimization. In many circumstances, when entities collect less information they assume less risk by reducing the amount of information that could be misused by malicious crackers or by employees. Additionally, privacy policies of entities that minimize information collection tend to be simpler to write, and easier for individuals to digest.

Collection limitation plays an important role in protecting individuals. For instance, a terrorist suspect connected to the Al Qaeda network was recently charged with selling the Social Security Numbers (SSNs) of twenty-one people who were members of the Bally's Health Club in Cambridge, Massachusetts. The SSNs were sold in order to create false passports and credit lines for bank accounts.[4] Some viewed this incident as a breach of internal security. However, the underlying risk was created by Bally's in requiring the SSN for membership, and then making it available to employees. Bally's could have assigned members a different number, or could have collected the information for an initial credit check, and then purged the SSN.

Data Quality

Second, the data quality principle specifies that personal data should be accurate and complete. Accuracy allows for better business decisionmaking.

[3] Harold Zimmerman, Remarks at the Meeting of the Direct Selling Education Foundation on Facets of Customer Relations Management, May 21, 2001. Mr. Zimmerman recommends that incentives be given to sales employees so that they will collect the maximum amount of personal data and input the information into a database.
[4] Robert Ellis Smith, Privacy Protects Against Terror, Privacy Journal, Mar. 2002.

Purpose Specification

Third, the purpose specification principle requires that data collectors give notice of the purposes for which personal information is collected. This notice should be given when the data is collected.

Use Limitations

Fourth, the use limitation principle specifies that data collected for one purpose should not be employed for another purpose absent consent. For example, use limitation is violated by magazine companies that transfer their subscription lists, which are collected for the purpose of mailing a publication, to marketers who use the subscription lists for other direct mailings.

Use limitations are often ignored by companies that exploit personal information, and recent changes in the law has accelerated secondary use of data. The Gramm-Leach-Bliley Act (GLBA) now allows a broad spectrum of institutions to affiliate and operate under a single corporate umbrella, called a financial holding company. These institutions engage in a wide range of activities and compile a vast amount of information about their customers. Affiliates may include banks, insurance companies, securities firms, as well as institutions that significantly engage in financial activities, such as retailers that issue credit cards, auto dealerships that lease vehicles, and entities that appraise real estate. The law allows these companies to merge not only themselves into one financial holding company, but also their customers' data into one comprehensive database. This data may include financial, medical and other sensitive information.

Some financial holding companies have thousands of affiliates, making it exceedingly difficult for consumers to even begin to understand how personal information will be employed for secondary purposes. CitiGroup, Inc., for example, has over 2700 corporate affiliates.[5] Similarly,

[5] *Financial Privacy and Consumer Protection Hearing Before the Senate Comm. on Banking, Housing and Urban Affairs*, 107th Cong., Sept. 19, 2002 (statement of William H. Sorrell, Attorney General, State of Vermont).

Bank of America has almost 1500.[6] Given the vast scope of corporate affiliates, individuals can take no comfort in a financial institution's claim that information is shared only for purposes consistent with its original collection.

Security Safeguards

Fifth, the security safeguards principle requires data collectors to protect personal information from loss, unauthorized access, destruction, improper use, modification, or disclosure.

Openness

Sixth, the openness principle requires data collectors to be forthcoming with information about database practices. Policies involving the use and maintenance of the databases should be public, and there should be no secret databases. The financial services industry has failed to incorporate meaningful openness in its practices. Both the GLBA and the Fair Credit Reporting Act (FCRA) require financial institutions to provide clear and conspicuous notice to consumers about their information sharing practices and consumers' rights to opt-out of some of this sharing. Companies have failed to provide individuals with the information they need to better understand how their personal information may be used and how they may exercise their opt-out rights.

Financial services companies have failed on openness because they do not identify with adequate specificity what information they share, or the possible recipients of personal information. Consequently, if information is misused by one of the thousands of an institution's affiliates and marketing partners, individuals will continue to have trouble identifying the offender.

Many consumers overlook the notices, in part because they are not sent in separate mailings and are couched in language that make them appear to be marketing materials. The notices also are difficult to understand, and written in tiny font sizes. A readability expert determined that, of

[6] *Id.*

sixty privacy notices examined, most were written at a third or fourth year college reading level, rather than the eighth grade level standard typically used for notices to the general public.[7]

Evidence regarding opt-out notices provided in other contexts suggests that companies may purposely be drafting unintelligible notices to mislead customers. In *Ting v. AT&T*, a district court found that AT&T conducted research to develop a notice regarding new contract terms that consumers would be likely to consider as a "non-event."[8]

Individual Participation

Seventh, the individual participation principle requires that data subjects have access to and a right to correct their personal information stored in databases. Such rights are important because they contribute to data quality, and place the individual on a level playing field with the business.

Under this principle, individuals should have a right to access all information stored by the data collector. This includes "enhanced" data purchased or obtained from cooperative databases, and attributes assigned to the individual through data mining or other data analysis methods.

Accountability

Last, the accountability practice specifies that data collectors should be responsible for complying with FIPs. This responsibility comes in the form of legal liability. Privacy violations

[7] Mark Hochhauser, Lost in the Fine Print: Readability of Financial Privacy Notices, July 2001, at http://www.privacyrights.org/ar/GLB-Reading.htm.

[8] "Another part of AT&T's research, the Qualitative Study, concluded that after reading the bolded text in the cover letter which states 'please be assured that your AT&T service or billing will not change under the AT&T Consumer Services Agreement; there's nothing you need to do,' 'at this point most would stop reading and discard the letter.' One of the authors of the study did not find this conclusion to be a cause of concern, and no one on the detariffing team ever expressed concern to her about this conclusion. "…AT&T was concerned that if its customers focused on the Legal Remedies Provisions, they might become concerned, less likely to perceive detariffing as a non-event and possibly defect. As a high ranking member on the detariffing team stated: "I don't wantthem to tell customers that now individual contracts need to be established with customers and pay attention to the details [sic]." While presenting the CSA as a non-event may have helped AT&T retain its customers, it also made customers less alert to the fact that they were being asked to give up important legal rights and remedies." *Ting v. AT&T*, 182 F. Supp. 2d 902 (N.D. Cal. 2002).

should give rise to a private right of action where data collectors can be held responsible for liquidated damages and legal fees.

FIPs Constitute A Framework for Evaluating the Costs and Benefits of Information Use

These FIPs provide a method for evaluating the privacy-invasiveness, or the cost of a proposed consumer information flow. Policymakers should consider whether the use of personal information is minimized; whether it incorporates systems to ensure accuracy and completeness; whether the information flow is consistent with the purpose for which the data was collected; whether consent was obtained before employing information for a secondary purpose; whether the system is secure; whether the system is open to public scrutiny; whether there is a right to access and correction; and whether accountability is incorporated in the system. Personal information flows that do not incorporate these responsibilities are privacy invasive and transfer costs onto the individual.

Independent Polls Demonstrate that Americans Want More Control Over Personal Information Flows

Last year, the citizens of North Dakota were the first in the nation to have the opportunity to vote directly on whether an opt-in or opt-out standard should govern the exploitation of personal financial information. On June 11, 2002, 72% of North Dakota residents chose opt-in over opt-out. This occurred despite misleading radio and television advertisements broadcast by the financial services industry depicting the end of modern commerce in the State if opt-in was chosen.[9] Despite being outspent by the banks, a small citizens' group called Protect Our Privacy rallied North Dakotans, and they overwhelmingly chose opt-in over opt-out.[10]

But this result should not be a surprise. Over a decade of public opinion polling has demonstrated that individuals care about the privacy of their personal information, and that they want protections in law following Fair Information Practices.[11] In 1990, a Harris Poll showed

[9] Two television commercials from the debate, paid for by "Citizens for North Dakota's Future," are available online at http://www.privacy.org/ndoptin.mpg.
[10] http://www.protectourprivacy.net/.
[11] *See generally, Public Opinion on Privacy*, EPIC (2003), at http://www.epic.org/privacy/survey/.

that 65% of Americans favored the creation of a privacy protection commission.[12] A year later, a Time-CNN poll showed that 93% of respondents believed that the law should require companies to obtain permission from consumers before selling their personal information.[13] More recent studies illustrate continued support for opt-in. A March 2000 BusinessWeek/Harris Poll shows that 86% of users want a web site to obtain opt-in consent before even collecting users' names, address, phone number, or financial information. The same poll shows that 88% of users support opt-in as the standard before a web site shares personal information with others.[14] An August 2000 Pew Internet & American Life Project Poll showed that 86% of respondents supported opt-in privacy policies.[15]

Public polling indicates that individuals not only care about their privacy, but they take affirmative steps to protect their personal information from commercial exploitation. Since individuals realize that existing laws do not adequately protect their personal data, they often engage in privacy "self-defense." When polled on the issue, individuals regularly claim that they have withheld personal information, have given false information, or have requested that they be removed from marketing lists. In a February 2002 Harris Poll, 83% of respondents had asked a company to remove their name and address from mailing lists.[16] An April 2001 study performed by the American Society of Newspaper Editors found that 70% of respondents had refused to give information to a company because it was too personal and 62% had asked to have their name removed from marketing lists.[17]

---

[12] Harris Poll No. 892049, Jan. 1990.
[13] TIME-CNN Privacy Poll, 1991.
[14] *BusinessWeek/Harris Poll: A Growing Threat*, BusinessWeek Magazine, Mar. 2000, at http://www.businessweek.com/2000/00_12/b3673010.htm.
[15] *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, Pew Internet & American Life Project, Aug. 20, 2000, at http://www.pewinternet.org/reports/toc.asp?Report=19.
[16] *Privacy On and Off the Internet: What Consumers Want*, Harris Interactive, Feb. 19, 2002, at http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=429.
[17] *Freedom of Information in the Digital Age*, American Society of Newspaper Editors Freedom of Information Committee and the First Amendment Center, Apr. 3, 2001, at http://www.freedomforum.org/templates/document.asp?documentID=13597.

The Commission Should View Industry-Sponsored Studies With Skepticism

Much public opinion research on privacy has been sponsored by companies with interests in slowing or stopping federal privacy legislation. Often, this research supports conclusions that serve the interests of the entity sponsoring the study. Other studies tend to divide the public into factions, and fail to inform public debate.[18] Sometimes these divisions are engineered through designing answers that are not mutually exclusive. The resulting ambiguities can then be used to benefit the sponsor of the study. For instance, a 1990 Alan Westin study funded by Equifax concluded that:

> A majority of the public (55%) favors protecting consumer privacy by using the present system (31%) or setting up a nonregulatory privacy board (24%). A strong minority (41%) believe a regulatory privacy commission is needed. Among executives in all the privacy-intensive industries, majorities or pluralities opt for staying with the present system in preference to either alternative.[19]

In this question used to influence policymaking, Westin concludes that a majority of the public favors using "the present system" to address privacy. However, one could make an opposite conclusion that perhaps is less favorable to Equifax's interests: the majority of the public favors the creation of some type of government entity for privacy protection, while only 31% favor self-regulation.

Others in the privacy debate also use questionable methods that benefit study sponsors. As Elizabeth Warren, a chaired professor of law at Harvard, explained recently in the Wisconsin

---

[18] *See* rebuttal comments of the Electronic Frontier Foundation by Deborah Pierce, FTC Online Profiling Workshop, Docket No. 990811219-9219-01, Nov. 30, 1999, at http://www.ftc.gov/bcp/profiling/comments/eff.htm; Oscar H. Gandy, Jr. *The role of theory in the policy process. A response to Professor Westin.* pp. 99-106 in C. Firestone and J. Schement (Eds.) Toward an Information Bill of Rights and Responsibilities. Washington DC: The Aspen Institute Communications and Society Program, 1995; Glenn Simpson, *Consumer-Privacy Debate Raises Questions About a Well-Known Expert's Connections*, Wall Street Journal, Jun. 25, 2001, at http://interactive.wsj.com/articles/SB993415584898492858.htm.

[19] Equifax Executive Summary 1990, at http://www.privacyexchange.org/iss/surveys/eqfx.execsum.1990.html. The three options given were "Stay with the present system of specific laws, congressional oversight, and individual lawsuits," "Create a nonregulatory Privacy Protection Board to research and publicize new controversies over privacy for public policy consideration," "Create a regulatory Privacy Protection Commission with powers to issue enforceable rules for businesses handling consumer information," and "Not sure."

Law Review, the Credit Research Center's academic integrity is questionable based on the research methods that the group employs:

> The Credit Research Center Study of 1982 concluded that the credit industry lost $ 1.1 billion in bankruptcy filings by debtors who could have repaid those debts. The study heaped assumption on top of assumption, with every tilt in favor of the credit industry position. My long-time co-authors…and I wrote our first article together dissecting the 1982 study. For me, the exercise was a private tutorial by a first rate demographer cataloguing the things that a researcher could do in the design, implementation, and data analysis in a study to distort the outcome of the research…[20]

Warren concludes:

> I make only a simple empirical observation: As far as I can tell, the Credit Research Center, funded by the credit industry, has never produced a single piece of work at odds with a credit industry position on any subject, while it has produced multiple papers that support the industry's call for more pro-creditor, anti-debtor legislation - always in the name of independent, academic research.[21]

Other portions of Warren's article provide a roadmap for evaluating research that is heavily funded by interested industry groups: is the research subject to independent peer-review or published in the academic community, or it is simply disseminated to Congress? Is there any disclaimer or explanation of funding sources? Is there an attempt to portray the study as a product of an academic institution? And, perhaps most importantly, can the public inspect the methods and data used to administer the study?[22]

Accordingly, we ask the Commission to carefully consider whether studies submitted to the agency reflect the bias of sponsors' funding. As a method for evaluating public opinion polls and studies, we further suggest that the Commission consult "20 Questions Journalists Should Ask About Poll Results," a guide developed by Public Agenda.[23] One additional question that should

---

[20] Elizabeth Warren, *The Market for Data: The Changing Role of Social Sciences in Shaping the Law*, 2002 Wis. L. Rev. 1, 11 (2002).
[21] *Id.* at 24.
[22] Footnotes 72 and 84 of Warren's article show that the CRC would not release the data used to support its conclusions to the General Accounting Office. *Id.* at 19, 23.
[23] http://www.publicagenda.org/aboutpubopinion/aboutpubop1.htm

be posed is whether the sponsor had "veto power" over publishing the survey. If the researcher could only publish results if the sponsor approves of the outcome, the value of the survey should be questioned.[24]

Finally, we note that privacy expert Robert Gellman authored a study analyzing industry-funded privacy studies in March 2002.[25] We submit that study as an appendix to our comments.

Business Information Flows Have Altered the Balance of Power Between the Individual and the State

An April 13, 2001 article in the Wall Street Journal reported that information broker company ChoicePoint provided personal information to at least thirty-five government agencies.[26] Following publication of that article, EPIC filed a series of Freedom of Information Act (FOIA) requests to determine the nature and amount of information sold to government. To date, EPIC has determined that ChoicePoint has several multi-million dollar contracts with law enforcement agencies to sell personal data. In addition, Experian, a credit-reporting agency, sells personal information to government agencies for law enforcement purposes. Both of these companies have sponsored reports and other public relations material in order to prevent regulations that would empower individuals to limit sharing of personal information.

Other documents obtained by EPIC show that ChoicePoint and Experian sold the IRS credit header data, property records, state motor vehicle records, marriage and divorce data, and international asset location data. IRS employees have access to this personal data from their desktop computers. To facilitate the IRS account and access for other law enforcement agencies, ChoicePoint has created a federal government web portal at http://www.cpgov.com/.

---

[24] We think that, if the Commission had followed this formula, it would not have relied so heavily in its testimony before a Congressional Committee on a recent American Enterprise Institute-Brookings report on preemption in the FCRA. That report made recommendations that closely follows the desires of the financial services industry. Privacy expert Robert Gellman labeled the study "shockingly incompetent."

[25] Robert Gellman, *Privacy, Consumers, and Costs, How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete*, Mar. 2002, available at http://www.epic.org/reports/dmfprivacy.html.

[26] Glenn Simpson, *FBI's Reliance on the Private Sector Has Raised Some Privacy Concerns*, Wall Street Journal, Apr. 13, 2001.

One presentation obtained under the FOIA, titled "The FBI's Public-Source Information Program Fact Versus Fiction" highlights the FBI's access to property records, professional licenses, news articles, driver and DMV records, census records, and credit headers. It lists ChoicePoint, Westlaw, Lexis Nexis, Dun and Bradstreet, and credit reporting agencies as sources for this information. Reliance on these databases has increased by 9600 percent since 1992, according to the presentation.

Privacy advocates have warned for years that business information flows present risks to civil liberties because the government can purchase or subpoena business records. The sale of personal information has direct costs on the individual, as it has altered the balance of power between the individual and the state. At one time, if a law enforcement agency wished to investigate an individual, the agency had to devote human resources to the investigation. Now, the law enforcement agency can simply visit a web site to obtain detailed dossiers on individuals. Despite the power of these new tools, the FOIA documents obtained from the government show no evidence that there are auditing tools or accountability measures to prevent misuse of this information.

Information Brokers Sell Personal Details That Are Private, and Highly Sensitive

A number of companies sell marketing data based on our purchases and behaviors. Consumers would probably object to much of this profiling. For instance, information broker Experian makes a commercial product of our Social Security Numbers, ethic and racialdata, and even medical data. The company's databases include a marketing list of people who suffer from bladder problems.[27]

The medical marketing service offers dozens of direct marketing lists on persons who suffer from a variety of conditions, from breast cancer to obesity.[28] Trans Union, the credit bureau, has

[27] Experian List Services Catalog, at http://www.epic.org/privacy/profiling/experianlistservices.pdf.
[28] Medical Marketing Service, Consumers by Ailment List, at http://www.mmslists.com/consumers_by_ailment_counts.htm.

engaged in a long battle to use credit reports and credit headers for marketing.[29] Claritas divides individuals into categories such as "Urban Achievers," "Pools and Patios," and even "Shotguns and Pickups."[30] Finally, companies are now selling personally identifiable records from pharmacy purchases.[31]

The sale of this information is objectionable, and it comes at a cost to individuals' dignity. It subjects individuals to unwanted marketing communication, including telemarketing, spam, and direct mail.

Specious Claims of the Information Brokerage Lobby Deserve Critical Analysis

Businesses that exploit personal information have employed a series of specious arguments in order to support wholly unregulated consumer information flows. The Commission should not accept these claims unless they can be supported with cogent arguments and demonstrable evidence. Furthermore, as explained in more detail below, benefits from information flows in one context do not justify other uses of information unrelated to the benefit. For instance, fraud prevention from the use of personal information may justify information flows in certain contexts, but it does not justify all information flows that a business seeks.

> *Specious Claim #1: Consumer data profiling gives consumers products at a lower cost.*
> *Fact: Consumer data profiling has been used to increase prices.*

Theoretically, consumer data can be used to lower costs and pass savings onto the consumer. However, the data profilers, and especially those in the financial services markets, have not proved their case that savings have been passed onto consumers.

In the supermarket shopping card context, the evidence suggests that consumer information collection from "loyalty card" programs do not create savings for individuals. A 2003 Wall

[29] *Trans Union v. FTC*, No. 00-1141 (D.C. Cir. 2001), *cert. denied*, 536 U. S. ____ (2002).
[30] *Id.*
[31] National Retail Transactional Database, Response Media Products, at http://www.epic.org/privacy/profiling/pharmacyprices.pdf.

Street Journal study found that "most likely, you are saving no money at all [from supermarket shopping cards]. In fact, if you are shopping at a store using a card, you may be spending more money than you would down the street at a grocery store that doesn't have a discount card."[32]

The Wall Street Journal study surveyed card and non-card grocery stores in five different American cities and concluded that "In all five of our comparisons, we wound up spending less money in a supermarket that doesn't offer a card, in one case 29% less."[33] The author further wrote that "…according to industry experts, our shopping experience was typical, because cards are designed to make customers feel like they got a bargain, without actually lowering prices overall. 'For many customers, the amount of money saved has not risen,' says Margo Georgiadis, a specialist in loyalty programs at McKinsey & Co. The difference is that stores now make you carry a card to get the discounts, whereas before they just offered plain old sale prices.[34]

Some costs from consumer information flows are nascent or unforeseeable. One growing problem is "first-degree price discrimination," a practice where businesses attempt to "perfectly exploit the differences in price sensitive between consumers."[35] 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

---

[32] Katy McLaughlin, *The Discount Grocery Cards That Don't Save You Money*, Wall Street Journal, Jan. 21, 2003, at http://online.wsj.com/article/0,,SB1043006872628231744,00.html; *see also* John Vanderlippe, *Everyday high prices: A comparison of standard supermarket prices*, CASPIAN, Jul. 23, 2002, at http://www.nocards.org/savings/regular_price_study.shtml; Tracy Davidson, *Discount Grocery Cards -- Do They Really Save Money?*, NBC, Feb. 19, 2003, at http://www.nbc10.com/money/1992223/detail.html.

[33] *Id.*

[34] *Id.*

[35] 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); *see also* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev. 1607 (Nov. 1999); Oscar H. Gandy, Jr., *Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace*, 1996 U. Chi. Legal F. 77 (1996)..

> exchange of their data, many characterize the commercial exploitation of consumer transaction data as a classic example of a market failure.[36]

First-degree price discrimination is a goal of some in the information business. CIO Insight Magazine recently published an article discussing pricing ceilings where price discrimination is described as a goal for the industry: "The ideal strategy? To capture the value of the product or service for a particular customer or customer segment."[37]

The entities with the most ability to affiliate share and pass on savings to consumers have not done so. In fact, the largest banks, the entities with the most consumer data and the largest networks of affiliates, have continued to raise fees and penalties associated with their products. This has occurred despite assurances during the Gramm-Leach-Bliley debate that affiliate sharing would results in better products at lower prices.

While most banks charge for non-customer use of ATMs, larger banks are more likely to do so. CardWeb.com, a company that tracks many different types of payment cards, reports that "Nearly 98% of large institutions levy surcharges, while 92% of medium-sized institutions, and 84.5% of small banks currently impose ATM surcharges on non-customers. According to data released this week by the Federal Reserve, the number of major banks surcharging non-customers for ATM use grew 30% last year with an average surcharge fee of $1.44 per transaction. The average surcharge among medium-sized banks was $1.34, and $1.28 among small institutions. The proportion of banks and savings associations charging their depositors for withdrawals using other institutions' ATMs was nearly 80% in 2001, up a significant 6% from 2000."[38] Laura Bruce of Bankrate.com lamented in 2002: "Get used to it. Consumers are losing the battle against ATM surcharges."[39]

---

[36] Janet Dean Gertz, The Purloined Personality: Consumer Profiling in Financial Services, 39 San Diego L. Rev. 943, 964-5 (Summer 2002).
[37] Amy Cortese, *Price Flexing: How the Web Adds New Twists*, CIO Insight, at http://www.cioinsight.com/article2/0,3959,43528,00.asp.
[38] *ATM Fees*, CardWeb.com (Jun. 20, 2002), at http://www.cardweb.com/cardtrak/news/2002/june/20a.html.
[39] Laura Bruce, *Consumers Losing the Fight Against ATM Surcharges*, Bankrate.com, Mar. 28, 2002.

CardWeb.com has described the current situation in the financial services industry as a "Fee Frenzy."[40] "On average, late payment fees, among larger issuers, have increased 145.9% since 1994, from $11.71 to $28.79, according to CardWeb.com's marketing intelligence services CardData..."[41] This same article describes the creation of a new fee: Chase instituted a $12 charge for making a payment over the phone.

Just this month, the Federal Reserve issued a report on financial services fees and services showing that fees at larger institutions are generally increasing and services are decreasing.[42] The report 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."[43] 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."[44]

Research performed by U.S. PIRG and Consumer Federation of America affiliates have come to the same conclusion: larger banks are charging higher fees, despite being more profitable than ever. "[O]ur findings show that the cost spread, or 'big bank fee gap,' between big banks and small banks continues to widen."[45]

Some of the most vociferous financial services industry advocates of the "free flow of information" have actually been reporting incomplete data to credit reporting agencies in order to "game" the credit system. For instance, in 1999, several banks admitted to withholding positive information about individuals so that their customers would not be lured away by competitors offering better credit terms. A 1999 Office of the Comptroller of the Current press release on the

[40] *Fee Frenzy*, Cardweb.com (Mar. 21, 2002), at http://www.cardweb.com/cardtrak/news/2002/march/21a.html.
[41] *Id.*
[42] Annual Report to the Congress on Retail Fees and Services of Depository Institutions, Federal Reserve (June 2003), at http://www.federalreserve.gov/boarddocs/rptcongress/2003fees.pdf.
[43] *Id.* at 8.
[44] *Id.* at 1.
[45] *Bigger Banks, Bigger Fees*, A National Survey of Bank Fees, PIRG (Nov. 1, 2001).

subject states: "Some lenders appear to have stopped reporting information about subprime borrowers to protect against their best customers being picked off by competitors."[46]

Specious Claim #2: Consumers want personalization.

Fact: Studies show that consumers prefer customization to personalization.

As a primary matter, it is important to distinguish between "personalization" and "customization." Personalization refers to a system where the site operator or business chooses tailored content or advertising for a passive customer. Personalization requires monitoring of clickstream and usually involves the collection of personal information. Conversely, customization is a system where the user actively chooses how services are tailored. With customization, a user can typically alter the content or presentation of a site without being monitored or providing personally identifiable information. Customization places the consumer in control of transparent information flows, and is thus less privacy-invasive.

In the physical world, personalization may be welcome, in part because it shows that an employee invested the time and attention to remember a customer's desires. In the online world, personalization is often viewed as a gimmick. The recommendations chosen for the customer no longer depend of the attention of a human, but rather are the calculation of a computer program. Often, the program makes recommendations that have nothing to do with personal inclinations, but rather with promoting products that the business wants to move.

There is some evidence that individuals prefer customization to personalization. In a study of 300 online consumers, Accenture researchers discovered that "most consumers would prefer to just customize Web site interactions for themselves."[47] The study's authors found that:

> "The great assumption about personalization has been that it would be a godsend to a time-pressed and information-glutted public. So imagine our surprise when 42% of the Web users we polled—with help from a team of students from Vanderbilt University's Owen Graduate School of Management—said they saw

[46] Comptroller Urges Industry to End Abusive Practices And Elevate Customer Service Standards, OCC Press Release, June 7, 1999, at http://www.occ.treas.gov/ftp/release/99-51.txt.
[47] Paul Nunes & Ajit Kambil, *Personalization? No Thanks*, Harvard Business Review, Apr. 2001.

> no benefits from personalization. Even more amazing were the results of the choices we set up. We described two on-line grocers—one allowing customization, the other making personalized recommendations—and only about 6% of respondents said they would prefer to use the personalized site. Most valued some filtering of the product selection based on their profile, but overwhelmingly, they wanted to be in control of the filter. Choices between customized-versus-personalized news sites, investment sites, and sports sites yielded similar results.[48]

Although mixing use of personalization and customization, Wharton Business School Professor Peter Fader has remarked that personalization has not yet been successful:

> "You would think that making something more personalized to customers' needs would make the product or service better, but it doesn't…It's almost impossible to find out what people's true needs are. Their past behavior provides some decent information but not a perfect reflection of what they want today or tomorrow. So trying to customize a website to take advantage of what a customer did the last time he shopped online doesn't always work. And, in many cases, people don't want to be treated as being special in that regard. They're satisfied if the site isn't customized. [49]

Personalization may be used to limit the intellectual stimulation to which a person is exposed. As Cass Sunstein explained in *Republic.com*, content profiling can result in a narrowing of the ideas that one is exposed to. For instance, Amazon.com could require you to sign on upon visiting the site, and then only give recommendations based on your profile. However, often the best discoveries in a bookstore or a library are accidental—a title or a cover catches your eye, and you explore ideas that perhaps could not have been predicted by your profile. Mark Twain himself noted in *What is Man?* that many new ideas are a result of serendipitous exposure to media: "the chance reading of a book or of a paragraph in a newspaper, can start a man on a new track and make him renounce his old associations and seek new ones that are in sympathy with his new ideal; and the result for that man, can be an entire change of his way of life."

---

[48] *Id.*

[49] *The Failure of Customization: Or Why People Don't Buy Jeans Online,* Wharton Strategic Management, Mar. 27, 2002, at http://knowledge.wharton.upenn.edu/articles.cfm?catid=7&articleid=535&homepage=yes.

Specious Claim #3: Profiling will result in fewer solicitations because businesses can tailor advertisements to certain customers.
Fact: Despite the availability of more consumer information in the marketplace, consumers have not experienced a reduction in unwanted marketing material.

We are aware of no study that supports this improbable result from information flows. Consumer experience has been the opposite. The more information a business possesses about a consumer, the more solicitations the consumer receives. Recent years have seen dramatic increases in spam and telemarketing; greater availability of consumer information has not reduced these forms of unwanted marketing.

Specious Claim #4: Information allows companies to give consumers more choices.
Fact: Information flows can be used to restrict choice, and mislead consumers.

Financial institutions conduct computerized analysis of the information they collect about their consumers, and use that information to target select consumers for the purchase of products and services. Often, companies enhance their own collected information by combining it with information from other databases. These may include demographic data, such as age, gender, and family dwelling size, as well as lifestyle data, including predicted attributes based on buying habits and organization affiliations. These information flows can be and have been used to deny consumers choice or to steer them towards choices not in their best interest. For instance, in the financial services arena, personal information has been used to "pack" products to certain consumers. The depositions conducted by the Commission in the CitiFinancial investigation demonstrated that information flows allowed employees to access personal financial information without authorization, and pack unneeded products to minorities, the poor, and non-English speakers.

According to a sworn declaration of a former CitiFinancial employee, branch managers targeted deceptive loan solicitations to borrowers in certain zip codes, eliminating zip codes in more affluent areas.[50] The employee also stated that she and other staff would attempt to sell extra

[50] *FTC v. Citigroup, Inc.* No. 1:01-CV-00606, Decl. of Gail Kubiniec, ¶ 10 (May 2001).

insurance by identifying vulnerable borrowers based on their occupation, race, age and education level. One stated, "If someone appeared uneducated, inarticulate, or was a minority, or was particularly old or young, I would try to include all the coverages CitiFinancial offered. The more gullible the consumer appeared, the more coverages I would try to include in the loan."[51]

In a separate case, a Minnesota Attorney General investigation found that the elderly and consumers who speak English as a second language were particularly vulnerable to preacquired account telemarketing fraud. The Office's review of randomly selected sales of one preacquired account telemarketer, for instance, revealed that 58% of customers whose accounts were charged were over 60 years old.[52]

Information flows can also be used to engage in attempts to eliminate certain customers. There is a movement in the "Customer Relationship Management" or profiling field that would systematically exclude customers if they are not profitable to the business. Jim Dion, president of retail consulting firm Dionco Inc., recently urged storeowners to create disincentives for certain customers.[53] Dion characterized 20% of the population as "bottom feeders," who frequently complain and have low-levels of customer loyalty. Businesses, he argues, should try to eliminate these customers: "It'd be cheaper to stop them at the door and give them $10 not to come in."[54] An article in DMNews quotes Dion as suggesting that retailers "should consider a preferred-customer database—prefer that they don't shop here."[55]

As Professors Danna and Gandy explain, information flows may be used more frequently in the future to create such a database of undesired customers:

> "If those customers who have a predicted high lifetime value are the ones a firm needs to keep, then those with a predicted low lifetime value are the ones a firm needs to get rid of or otherwise convert to a more profitable status. Many firms come to the conclusion that low margin customers are not worth the effort

[51] *Id.* at ¶ 14.
[52] *Financial Privacy and Consumer Protection Hearing Before the Senate Comm. on Banking, Housing and Urban Affairs*, 107th Cong., Sept. 19, 2002 (statement of Mike Hatch, Attorney General, State of Minnesota).
[53] Mickey Alam Khan, *Technology Creates Tough Environment for Retailers*, DMNews, Jan. 13, 2003, at http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=22682.
[54] *Id.*
[55] *Id.*

> 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.'[56]

The Commission should consider how customer exclusion based on loyalty attributes could affect competition. It is possible that businesses are trying to locate and retain loyal customers so that they can avoid the traditional means of successful sales—offering the best product or service at the lowest price. The Commission should also consider whether such profiling programs have a disparate impact on protected groups.

Specious Claim #5: Information flows reduce fraud.

Fact: Information flows can prevent fraud, or be used to defraud consumers.

While information sharing can be employed to detect fraud, it can also be used to commit fraud. For instance, major financial institutions have used their customer lists to target consumers for fraudulent telemarketing schemes. Capital One,[57] Chase Manhattan,[58] Citibank,[59] First U.S.A.,[60] Fleet Mortgage,[61] GE Capital,[62] MBNA America,[63] and U.S. Bancorp[64] all have provided their customers' personal and confidential information to fraudulent telemarketers.

---

[56] 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) *citing* Newell, F., *loyalty.com: Customer Relationship Management in the New Era of Internet Marketing* (McGraw-Hill, New York 2000); Peppers, D & M. Rogers: *1997, The 1:1 Future: Building Relationships One Customer at a Time* (Currency, New York 1997).

[57] Office of the Washington State Attorney General, "Settlement with Discount Buying Club Highlights Privacy Concerns," Aug. 4, 2000, available at http://www.wa.gov/ago/releases/rel_branddirect_080400.html.

[58] *Id.*

[59] National Association of Attorneys Generals, "Multistate Actions: 27 States and Puerto Rico Settle with Citibank," Feb. 27, 2002, available at http://www.naag.org/issues/20020301-multi-citibank.php; Settlement document available at http://www.oag.state.ny.us/press/2002/feb/feb27b_02_attach.pdf .

[60] Office of the New York Attorney General, "First USA to Halt Vendor's Deceptive Solicitations," Dec. 31, 2002, available at http://www.oag.state.ny.us/press/2002/dec/dec31a_02.html.

[61] *Minnesota v. Fleet Mortgage Corp.*, 158 F. Supp. 2d 962 (D. Minn. 2001), available at http://www.ag.state.mn.us/consumer/PR/Fleet_Opinion_61901.html.

[62] Office of the Washington State Attorney General, "Settlement with Discount Buying Club Highlights Privacy Concerns," Aug. 4, 2000, available at http://www.wa.gov/ago/releases/rel_branddirect_080400.html.

[63] *Id.*

[64] Office of the Minnesota Attorney General, "Minnesota AG and U.S. Bancorp Settle Customer Privacy Suit," July 11, 1999, available at http://www.ag.state.mn.us/consumer/Privacy/PR/pr_usbank_07011999.html.

The financial institutions provided the telemarketers with the names, telephone numbers and other information about their customers. They also gave them the ability to charge customers' accounts without having to ask consumers to provide an account number. This practice, called preacquired account telemarketing, has subjected thousands of individuals to unauthorized charges for products and services they never wanted or ordered. In one case, during a thirteen-month period a national bank processed 95,573 cancellations of membership clubs and other products that were billed by preacquired account telemarketers without customers' authorization.[65]

In some cases, financial information flows have allowed businesses to defraud non-customers. This can occur where a bank sells personal information to another business. Charter Pacific Bank sold its database containing 3.6 million valid credit card account numbers to a convicted felon who then fraudulently billed the accounts for access to Internet pornography sites that victims had never visited.[66] In fact, approximately 45% of the victims did not even own a computer. Charter Pacific did not develop the database from its own customers' information. Instead, it compiled the information from credit card holders who had purchased goods and services from merchants that had accounts at Charter Pacific. The information included the date of sale, account number, and dollar amount of every credit card transaction processed by the bank's merchant customers. The unrestricted sharing of this information resulted in over $44 million of unauthorized charges.

Information flows can expose the elderly and other at risk consumers to increased likelihood of fraud. NationsBank, for example, shared with its affiliated securities company data on bank customers with low-risk, maturing federally insured CDs.[67] The affiliate, NationsSecurity, 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.

---

[65] Supplemental Comments of the Minnesota Attorney General Office, FTC Telemarketing Sales Rule, FTC File No. R411001, http://www.ftc.gov/os/comments/dncpapercomments/supplement/minnag.pdf.
[66] Federal Trade Commission, "FTC Wins $37.5 Million Judgment from X-Rate Website Operator; Bank Sold Defendants Access to Active MasterCard, Visa Card Numbers," Sept. 7, 2000, available at http://www.ftc.gov/opa/2000/09/netfill.htm.
[67] *Nationssecurities and Nationsbank, N.A.*, SEC Release No. 33-7532, May 4, 1998, available at http://www.sec.gov/litigation/admin/337532.txt.

Many customers, including retired elderly, lost significant portions of their life savings. After an investigation, the Securities and Exchange Commission found 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 made this possible. NationsBank provided the investment representatives with maturing CD customer lists, as well as customers' financial statements and 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. NationsBank is not the only bank to have engaged in such a practice. First Union settled a private lawsuit alleging a similar scheme.[68]

The unrestricted sharing of consumers' information facilitates criminal activity, such as theft of financial identity. Identity theft is one of the nation's fastest growing white-collar crimes. Many of these identity theft cases are "insider jobs," committed by employees who obtain access and misuse individuals' personal information stored in their employers' databanks. Researchers at Michigan State University recently studied over 1000 identity theft cases and found that victims in 50% of the cases specifically reported that the theft was committed by an employee of a company compiling personal information on individuals.[69] Additional cases implied employee theft. Other reports note that many identity fraud cases stem from the perpetrator's purchase of consumers' personal information from commercial data brokers. Financial institutions information sharing practices contribute to the risk of identity theft by greatly expanding the opportunity for thieves to obtain access to sensitive personal information.

[68] *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).

[69] Study forthcoming; results provided in email from Judith M. Collins, Ph.D., Associate Professor, Leadership and Management Program in Security School of Criminal Justice, Michigan State University to EPIC (Apr. 22, 2003, 18:13:35 EST) (on file with EPIC).

Respectfully Submitted,

Chris Jay Hoofnagle
Deputy Counsel

Kerry Smith
IPIOP Fellow
Electronic Privacy Information Center