THE PRIVATIZATION OF BIG BROTHER:

Protecting Sensitive Personal Information From Commercial Interests In The 21st Century

Mike Hatch †
Minnesota Attorney General

INTRODUCTION

Much of the privacy debate during the last century focused on the need for procedural safeguards restricting the government's ability to monitor the personal lives of its citizens. The mistrust of "Big Brother" is grounded in a legitimate concern that government officials may abuse their power by indiscriminately gathering and using information about citizens. In response to these concerns, the Supreme Court recognized a constitutional right to privacy under the First and Fourteenth Amendment, and held certain methods of wiretapping and searches unconstitutional under the Fourth Amendment. Like many states Congress enacted laws that made it illegal for government employees to misuse tax records or acquire bank account information without specific authorization.

However, legal protections concerning privacy invasions by government have typically not been extended to the collection and use of data about individuals by private entities. Financial institutions and other companies routinely buy and sell sensitive, personal information to target specific consumers who are identified as "susceptible" to their solicitations. On average, companies trade and transfer personal information about every U.S. citizen every five seconds.[1] Accordingly, it is not surprising that the number of privacy violations by commercial interests has grown exponentially in the last decade.

Part I of this Article discusses the origins of the right to privacy as a property right and a liberty right. Part II provides background information on the data-collection industry and the public's expectations for privacy. Part III discusses the societal harm that can occur when an individual's privacy is violated. Part IV sets forth the public policy reasons that support adoption

of an "opt-in" system for sensitive personal information. Finally, Part V advocates for the provision of express consent before sensitive personal information is bought, sold or traded by commercial interests.

I. THE ORIGINS OF THE RIGHT TO PRIVACY.

Corporate lobbyists who oppose any recognition of the right to privacy for bank records, telephone records, and other sensitive, personal information mistakenly argue that the right to privacy is simply an overreaction by people not wanting to be bothered by telemarketing calls. However, the privacy issue is not simply about freedom from "annoyance." The right to privacy is deeply imbedded in American law and is reflected in virtually all contributing cultures to the American lifestyle. There are numerous references in the law to the right of privacy. Some of these laws and court decisions reflect a personal right to privacy similar to that of freedom of association, speech, or religion. Other laws and court decisions reflect a property right to privacy. Part B of this section considers the origins of the right to privacy. To put these philosophical underpinnings in perspective, however, Part A sets forth a hypothetical of events which, while seemingly remote, could readily occur in today's "information age."

A. What Privacy Means in Today's World.

Mary is 30 years old and is about to graduate with a master's degree in engineering. As a teenager Mary was treated by a psychologist for anorexia. Mary recently married James, a 35-year-old attorney who is employed by Alpha Biosource's patent department. James partied heavily in college and went through chemical dependency treatment. He has not had a drink in over 13 years.

Mary wants to undergo elective surgery to correct a cosmetic problem, and Mary and James apply for a $10,000 home equity loan from Beta Bank to pay for the surgery. Beta Bank owns Delta Insurance Company, which provides health insurance to Alpha Biosource. As part of the underwriting process to verify the purpose of the loan, Beta Bank obtains a medical waiver from Mary. Beta Bank receives Mary's data file from a medical bureau, which states that Mary has been treated for mental illness. It also receives a data file from Delta Insurance, which insures Mary through James' group coverage at Alpha Biosource. The data file indicates that James has been treated for chemical dependency. Beta Bank, which has an internal policy concerning the relationship of mental illness to credit reliability, denies the loan application, telling Mary that its decision was only based on "underwriting reasons."

Because Alpha Biosource is engaged in the highly competitive medical technology field, it is highly concerned about corporate espionage. It periodically runs security checks on all of its employees, which are carried out through a blanket authorization signed by employees when they accept employment. Alpha Biosource presents a data request to Beta Bank, which transmits a data file indicating that James has been treated for chemical dependency, that his wife has been treated for mental illness, and that their recent application for a loan for the purpose of securing medical treatment was denied. Alpha Biosource then purchases from the telephone company a list of all telephone calls made by James' household over the past six months. Unbeknownst to Alpha Biosource, Mary had been applying for jobs at a variety of different companies, including a company that engaged in the construction of hospitals, named XI Health Systems. When Alpha Biosource reviewed the telephone numbers called by James' telephone, it discovered a telephone call to XI Health System, which acts as a competitor to some products distributed by

Alpha Biosource. Concerned about the blackmail of its employees, Alpha Biosource terminates James due to a "corporate reorganization."

Mary then applies for employment with Gamma Transportation Systems, a company engaged in the manufacturing of high-speed unit trains. Gamma transportation is heavily involved in international trade, supports the World Trade Organization, and demands strong loyalty on behalf of its employees. Gamma Transportation, as part of its hiring policy, contacts Boomerang Data International, a company that specializes in the purchase, merging, storing and distribution of data files. Boomerang Data periodically sweeps the banking industry for data files. Boomerang Data responds to Gamma's request about Mary by supplying a data file which indicates that Mary has been treated for mental illness, that she is married to James, that James has been treated for chemical dependency, that James was recently separated from employment for unknown reasons, that Mary was denied a loan to pay for health treatment, and that a check had been written on their bank account to an organization which participated in demonstrations against the World Trade Organization. Gamma Transportation politely denies Mary's job application.

Card Shark International is a Visa card vendor that finances its accounts through securitized loans in the secondary market. Card Shark obtains customers by telemarketing prospects. The names of the prospects are obtained by purchasing data from organizations such as Boomerang Data, which lists the names of all depositors of particular banks who have a high monthly balance of $4,000 for 10 of the past 12 months and who have not had a negative balance during 10 of the past 12 months. Card Shark telemarketers contact Mary, who is offered a credit card. The telemarketer tells Mary that he will send her a Visa card with no membership fee and two-percent interest rate for the first six months. The telemarketer also solicits Mary to receive a

30-day membership in a health discount program where patients could receive a steep discount on health care services purchased through a preferred provider network. The telemarketer tells Mary that he will mail to her the list of the health discount program, and that she has 30 days in which to decide whether to participate. At no time was Mary advised that if she did not affirmatively decline the program within 30 days, she would be charged $59.95 per month for one year of service.

Mary thereafter receives the Visa card and starts using it to tide the family over during the family's period of unemployment. In a separate package she receives the materials on the health discount program, but when she reviews the list of health providers, she discovers that only five providers reside in her state and that none of the providers offer services that she is interested in. Accordingly, she throws the materials away.

Sixty days later Mary is charged $59.95 for the first monthly payment in the health membership club. She contacts the health membership program to complain and is told that, because she never contacted the company to terminate the program, she was automatically enrolled in it on the 31st day. Mary immediately terminates the Visa card and tells the company that she will not make any further payments on the program. What she did not know, however, was that the telemarketing firm was also able to bill Beta Bank, which holds the mortgage on her home. Mary does not discover the increased charge until she received her annual RESPA notice from the bank.

While the above facts may seem farfetched, they can all occur in this age of technology.

B. The Origins of Privacy.

The belief that privacy is a fundamental right is as old as civilization itself, crossing all time periods and cultures. For instance, the ancient Greeks in the 5th Century B.C. recognized the right to privacy in the Hippocratic Oath for physicians, which provides, "[w]hat I may see or hear in the course of treatment or even outside of the treatment in regard to the life of men…I will keep to myself…."[2] In the United States, legal scholars Samuel Warren and Louis Brandeis brought attention to the legal underpinnings of the right to privacy over 100 years ago in their now famous law review article entitled *The Right to Privacy*.[3] In advocating for "the right to be let alone," they reasoned that both the right to liberty and the definition of property can encompass privacy interests and that failure to recognize privacy would mean that "what is whispered in the closet shall be proclaimed from the house-tops."[4]

1. Privacy as a liberty interest.

The United States Supreme Court has repeatedly held that the United States Constitution provides a basis for certain protections of an individual's privacy from governmental intrusion, finding privacy interests rooted in fundamental liberty rights.[5] This right of decisional privacy has been extended by the courts to decisions involving marriage,[6] procreation,[7] contraception,[8] family relationships,[9] and childrearing and education.[10] For example, in *Griswold v. Connecticut*, the United States Supreme Court ruled that the marital relationship lies within "a zone of privacy created by several fundamental constitutional guarantees."[11] The Court also held in *Roe v. Wade* that the right to privacy, either grounded in the Constitution's concept of personal liberty or in the Ninth Amendment, includes a woman's decision to terminate her pregnancy.[12] Further, a woman who makes a decision to have an abortion has the right not to have her name

publicized and the right to keep the decision private from others, including her partner.[13] Later in *Planned Parenthood v. Casey*, the Court reaffirmed the notion that constitutional liberty and privacy are intertwined, asserting that, "[a]t the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life."[14]

The United States Supreme Court has established that the constitutional right to privacy also protects an individual's freedom of association, stating that privacy includes "an individual's choice to enter into and maintain certain intimate or private relationships."[15] The sanctity of the home is embraced in constitutional privacy as well. In *Frisby v. Schulz*, the Court recognized the worth of residential privacy by stating that, "protecting the well-being, tranquility, and privacy of the home is certainly of the highest order in a free and civilized society."[16] The Fourth Amendment also emphasizes privacy rights by asserting that individuals have a right to be free from unreasonable searches and seizures.[17] When interpreting the Fifth Amendment privilege against self-incrimination in *Miranda v. Arizona*, the Court stated it gives an individual a "right to a private enclave where he may lead a private life. That right is the hallmark of our democracy."[18]

Most states have developed torts for invasion of an individual's right to privacy which reflect the liberty interest in privacy. The Restatement of Torts has long recognized four distinct invasion of privacy torts consistent with the right to privacy.[19] These torts are intrusion upon seclusion, appropriation of one's likeness, publication of private facts and false light.[20] Intrusion upon seclusion occurs when a person intrudes upon the solitude of another's affairs when the intrusion is highly offensive to a reasonable person.[21] Appropriation happens when a person takes the name or likeness of another for his own benefit.[22] Publication of private facts takes places when a person publicizes another's private matter when the publication is highly offensive

and not of genuine public interest.[23] False light applies when a matter is publicized in a way that places another in a false light when the falsity is highly offensive to a reasonable person and the publisher knows of or acts in reckless disregard of the falsity.[24]

Georgia, the first state to recognize the right to privacy in its tort law, concluded that the right derived from natural law and was based on the constitutions of both the United States and Georgia.[25] Other states have determined that the right to privacy evolves from common law.[26] Minnesota recently became one of these states in *Lake v. Wal-Mart Stores, Inc*.[27]

In *Lake*, a woman sued a film processor for unauthorized distribution of a photograph depicting her in the nude.[28] The Minnesota Supreme Court found that she alleged privacy interests worthy of protection and subsequently recognized three of the four traditional privacy torts.[29] In doing so, the court echoed the sentiments of Warren and Brandeis by stating, "[t]he right to privacy is an integral part of our humanity; one has a public persona, exposed and active, and a private persona, guarded and preserved. The heart of our liberty is choosing which parts of our lives shall become public and which parts we shall hold close."[30]

Legislative bodies have likewise enacted numerous statutes that recognize a liberty right to privacy, designating certain government data recorded about citizens as confidential and protected from public inquiry. Information about cancer victims, for instance, may not be publicized.[31] HIV tests are considered private.[32] Tax returns are also deemed confidential.[33] The identities of individuals who participate in or receive information about alcohol or drug abuse programs must be kept confidential.[34] Welfare application data is protected.[35] Data on students attending educational institutions is considered private.[36] A library patron's book selections may not be disclosed to the public.[37] The names of individuals who register complaints against real property owners are regarded as confidential.[38] All information transmitted in confidence

between a victim of sexual assault and a sexual assault counselor is private.[39] Similarly, most data about farmers who receive county assistance is private, including information about financial history, current debts and personal and emotional status.[40]

Other laws recognize a liberty interest in the right of privacy by imposing confidentiality restrictions on personal data. For example, physicians generally may not disclose patient data absent consent.[41] Pharmacists are prohibited from disclosing certain data about their customers.[42] Insurers also must not share personal information without authorization.[43] Congress statutorily recognized a personal right to privacy when, in reaction to the disclosure of Judge Robert Bork's viewing habits by a video storeowner, it enacted legislation to prohibit the unauthorized distribution of a customer's video tape rentals.[44] Another federal law recognizing the importance of privacy requires subscriber cable television records to be kept confidential.[45] The Driver's Privacy Protection Act prohibits government employees from "knowingly disclosing or otherwise making available to any person or entity personal information about any individual obtained…in connection with a motor vehicle record" without that person's "express consent."[46]

The courts have similarly adopted rules that reflect a liberty interest in the right to privacy. Attorneys are prohibited from disclosing clients' secrets and confidences.[47] Domestic abuse records and juvenile records are generally kept confidential.[48] Juvenile hearings are closed to most members of the public as well.[49] Further, judges are permitted to impose protective orders to preserve the private nature of evidence.[50]

The courts and legislative bodies have also developed evidentiary rules to safeguard privacy interests as it relates to the testimony of witnesses. For example, in most legal proceedings spouses cannot testify for or against their partners without consent.[51] Members of

the clergy may also not be examined as to any communication made "by any person seeking religious or spiritual advice, aid, or comfort" without the person's consent.[52] Additionally, information provided to therapists, whether for mental health or chemical dependency, is typically considered privileged and may not be disclosed absent the patient's consent.[53]

2. Privacy as a property interest.

Courts and legislative bodies have also articulated privacy rights rooted in property law. The Minnesota Supreme Court has recognized that a bank is generally under a fiduciary duty not to disclose the content of loan records, particularly as it relates to the business plan of a company.[54] There are also numerous statutes that recognize that the disclosure of a business's information may constitute an unfair trade practice. Minnesota's Uniform Trade Secrets Act, for example, gives businesses remedies for misappropriation of information that is not generally known or readily ascertainable and has an independent economic value from its secrecy.[55] Courts have recognized that customer lists of a company may be considered a trade secret and an asset of the company that may not be disclosed by an employee.[56] Courts have made similar decisions with respect to company business plans, records and processes.[57] Judges may also protect trade secrets by using measures such as in-camera hearings.[58]

Congress has established the right to privacy as a property interest in certain contexts as well, particularly as it relates to Social Security numbers[59] and to credit information held by credit bureaus.[60] Congress has also enacted statutes regulating the collection of information by government employees,[61] restricting when government may access financial information,[62] limiting governmental access to telephone records,[63] and regulating government employees' use of tax records.[64]

3. Privacy interests cross national boundaries.

The right to privacy is not only deeply embedded in the American culture, but internationally as well. The 1948 Universal Declaration of Human Rights asserts that, "[n]o one should be subjected to arbitrary interference with his privacy…"[65] The 1950 Convention for the Protection of Human Rights and Fundamental Freedoms specifies that, "[e]veryone has the right to respect for his private and family life.…"[66] South Africa's constitution also declares that, "[e]veryone has the right to privacy…."[67] Argentina's constitution states that, "[t]he home is inviolable as is personal correspondence and private papers; the law will determine what cases and what justifications may be relevant to their search or confiscation. The private actions of men that in no way offend order nor public morals, nor prejudice a third party…are free from judicial authority."[68]

Many countries have enacted laws that relate to privacy and the disclosure of personal information. The European Union's recent directive requires that individuals be informed before organizations disclose personal data and that the individuals give consent before disclosure.[69] In 1995, Hong Kong created a law "to protect the privacy of individuals in relation to personal data."[70] New Zealand enacted a privacy law in 1993 that requires agencies that collect personal information from individuals to make sure that the individuals are aware that the information is being collected, the purpose for which the information is being collected, and the intended recipients of the information.[71] Russia's privacy act states that, "collection and dissemination of information about private life, and processing of information which concerns personal and family secrecy… is only permissible if a legal provision provides for this, or the person affected has agreed."[72] Sweden's privacy law requires that organizations which maintain personal data to register with the Data Inspection Board and receive permission from the board prior to collecting

most types of personal information.[73] Japan has a data protection law that governs the use of personal information in computerized files held by government agencies.[74] It limits the information that data agencies may collect and imposes duties of security, access and correction.[75] In 1994, South Korea enacted laws regarding the management of computer-based personal information held by government agencies.[76] The actions of these countries show that protection of individual privacy has universal importance.

II. BACKGROUND.

A. The Collection and Dissemination of Personal Information.

1. Monitoring and tracking individual people.

In his novel *Nineteen Eighty-Four* George Orwell warns of an omnipresent "Big Brother" that knows and sees all.[77] The government monitors every individual's conversation and movement.[78] The novel's main characters live in constant fear of saying or doing the wrong thing. It is a world without freedom or personal autonomy. Individuals have no control over what information will become public or remain private.

Today, the greatest threat to privacy may not be Orwell's large government computer, but rather the commercial sector's infinite network of private databases that collect information about everyday business transactions and purchases.[79] This thought is captured by commentator Jane Bryant Quinn, who writes:

> When we worry about who might be spying on our private lives, we usually think about the Feds. But the private sector outdoes the government every time. It's Linda Tripp, not the FBI, who's facing charges under Maryland's laws against secret telephone taping. It's our banks, not the IRS, that passed our private financial data to telemarketing firms.[80]

Indeed, there are currently over 1,000 private companies compiling comprehensive databases about individual consumers, a ten-fold increase in just five years.[81] These companies do not

engage in the "mass marketing" of products or the researching of general demographic groups. Rather, they focus on gathering as much information as possible about *specific* people to engage in what is sometimes called "personalization" or "personal marketing."

The array of available information is only limited by the technology itself. Each electronically recorded transaction provides a glimpse into a person's private life.[82] These pieces of information, when layered on top of one another, create a complete picture of each individual.[83] For example, Acxiom Corporation in Conway, Arkansas maintains a database that operates twenty-four hours a day, amassing and processing information on 95% of all American households.[84] For a price, Acxiom will sort information based on income, lifestyle (outdoor, mechanic, intelligentsia, etc.), or even a psychological profile of "ethnics who may speak their native language but do not think in that manner."[85]

Similarly, the Medical Marketing Service (MMS) offers lists of people with particular medical conditions.[86] Last fall, MMS offered for sale nearly 50 lists of individuals suffering from different medical ailments.[87] MMS sells the names and addresses of 427,000 people who are clinically depressed, 1.4 million women who have yeast infections, and 1 million individuals who have diabetes.[88] MMS also sells lists of people with Alzheimer's Disease, birth defects, Parkinson's Disease, and "physical handicaps."[89]

No information appears to be too personal for companies to collect and sell, and the boundaries of consent are often ill defined or non-existent. A New York company offers the names of high school students according to GPA, religion, ethnicity, and SAT scores.[90] Another company sells the names of obese African-American women. A hospital sells the names of its patients who may be eligible for Social Security insurance to a lawyer.[91] All of this data is merged into a consumer tracking and information infrastructure that becomes larger every day

and sold to whomever may be interested. Every piece of information gathered, stored, and sorted by these large databases represents an incremental erosion of an individual's right to privacy.

Private information is also readily available for little cost from electronic research companies: an unlisted phone number costs $49, a Social Security number costs $49, a bank balance costs $45.[92] A company will obtain another person's driving record for $35, trace a cell phone call for $84, or create a list of stocks, bonds, and securities for $209.[93] A reporter for *Forbes Magazine* recently learned first-hand this reality of the information age:

> In all of six days Dan Cohn and his web detective agency…shattered every notion I had about privacy in this country (or whatever remains of it). Using only a keyboard and the phone he was able to uncover the innermost details of my life- whom I call late at night; how much money I have in the bank; my salary and rent. He even got my unlisted phone numbers, both of them. Okay, so you've heard it before: America, the country that made 'right to privacy' a credo, has lost its privacy to the computer. But it's far worse than you think. Advances in smart data-sifting techniques and the rise of massive databases have conspired to strip you naked.[94]

2. The consumer tracking and information infrastructure.

The sale, collection, and integration of personal information about consumers are new industries in the information age.[95] Technology allows businesses to cheaply gather information about their existing or potential customers and then use that information to sell or market other products to those customers.[96] Using complex mathematical formulas and private financial information, data is sorted and categorized to isolate specific people for marketing purposes. This process is called "data mining."

The information possessed by these marketing companies goes far beyond mere demographic data. For example, during a privacy lawsuit against Metromail Corp., a marketing company, it was forced to reveal the types of information contained in its database.[97] Metromail's computer files contained more than 900 tidbits of information on individual

consumers dating back more than a decade.[98] One individual's file was 25 single-spaced pages and contained information such as her income, marital status, hobbies, medical ailments, her preferred brand of antacid tablets, whether she had dentures, and how often she had used room deodorizers, sleeping aids, and hemorrhoid remedies.[99] Technology like this allows corporations to probe deep into the personal lives of individual consumers:

> [A] jewelry retailer maintains a profile of a person named John Ring in a customer database, which culls and integrates data from multiple sources both inside and outside the firm. John's profile shows that he is 42 years old, lives in Boston, purchases diamond jewelry every six months, and has a high lifetime value rating. Since John is predisposed to buy diamonds, the next time he visits the [web]site the personalization engine can immediately show him the firm's current sales on diamond products. In addition, statistical analysis of all the customer records shows that John falls in a group that is pre-disposed to purchase high-end leather products and foreign automobiles. The firm decides to run a special promotion in which it e-mails John a Web-redeemable coupon for a high-end leather briefcase if he purchases $300 worth of jewelry by the end of the month. (The e-mail is sent at the time when John typically buys jewelry.)[100]

Some will claim that this example demonstrates how technology may benefit both the consumer and the business--the consumer receives discounts on products he usually purchases, and the jeweler acquires a new loyal customer. However, the technology utilized in this hypothetical may easily be used to target consumers in more harmful ways. Some individuals most susceptible to telemarketing and direct marketing include the unemployed, disabled, and the elderly, in part because they are the most likely to be home during the day and read unsolicited mail.[101] Sophisticated reporting and analysis tools may be used to target such persons for improper purposes, just as easily as they may identify a person who likes jewelry and leather jackets.

B. The Public's Expectations Concerning Privacy.

1. The emergence of privacy as a major issue of public policy.

Privacy is not a new concern. Yet, protecting an individual's right to privacy has recently emerged as one of the most important public policy issues of the information age. Over one-hundred years ago, Warren and Brandeis, in their now famous law review article, warned:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual…the right 'to be let alone'….[N]umerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.[102]

As privacy abuses by financial institutions and other large corporations and the lack of legal safeguards have come into national prominence, novel coalitions have formed among civil liberties activists, social conservatives, and libertarians in favor of more privacy protection.[103] On October 13, 1999, for example, the Coalition For Financial Privacy was formed.[104] Its members included among others Phyllis Schlafly of the Eagle Forum and Ralph Nader of the Consumers Union.[105] On February 10, 2000, various members of Congress formed the bi-partisan Congressional Privacy Caucus.[106] The Caucus supports notice and consent requirements before personally-identifiable information may be disclosed.[107] On March 31, 2000, Attorneys General from thirty-three states joined together in support of stronger financial privacy protections under the Financial Services Modernization Act, sometimes called the Gramm-Leach-Bliley Act, which broke down legal walls put in place during the Depression to keep separate the banking, securities and insurance industries.[108] The concerns expressed by these policymakers are strongly supported by public opinion polls.

2. Overwhelming expectations by the public concerning a right to privacy.

Public opinion polls and strong consumer reaction in the face of privacy violations reflect a strong expectation by consumers concerning their privacy rights.

a. Anecdotal experience.

When personal information about an individual is collected and sold, it generates intense feelings of betrayal and outrage.[109] For instance, after the Minnesota Attorney General's Office announced its litigation against a bank for revealing its customers' personal and financial information, the Office was flooded with thousands of phone calls and letters. Individuals were outraged that financial institutions engage in such practices. One consumer wrote, "The offer of 'free services' from a telemarketer who represents an organization that has my account number does little to enhance my sense of trust." Another wrote, "This is unacceptable, this is wrong, it is infuriating." Yet another wrote, "I am still dumbfounded that a supposedly ethical organization…would violate my trust and confidence in them by selling their customer list." A report in an Oregon newspaper aptly summarized most consumers' reaction to such behavior as "appalling" and "horrifying."[110]

The fair treatment of personal information is an element of basic human dignity and respect.[111] In fact, in one survey, nearly four out of five people regarded privacy as a fundamental right, worthy of addition to the list of "life, liberty, and the pursuit of happiness."[112]

b. Public surveys concerning consumers' expectations of privacy.

i. 2000 USA Weekend Poll.

In the USA Weekend poll, 84% of respondents believed that too many people have access to their credit report, and 79% thought that too many people have access to their financial

records.[113] 75% of the respondents considered phone calls at home from telemarketers an invasion of privacy, and 70% expected privacy invasions to become worse in the next five years.[114] The majority of respondents also believed that current laws are inadequate to protect their privacy and are extremely concerned about their ability to control who has access to their personal information.[115]

ii. 1999 Wall-Street Journal-NBC Survey.

In the Fall of 1999, a *Wall-Street Journal*-NBC survey asked people what they feared most in the coming century.[116] The answer most often given was "the loss of privacy."[117] Indeed, people were more fearful of the invasion of their privacy than of terrorism, global warming, or overpopulation.[118]

iii. 1999 IBM Consumer Privacy Survey.

In December 1999, IBM conducted an international survey about privacy and privacy issues. It found that more people in the United States believe that personal information is vulnerable to misuse than respondents in the United Kingdom or Germany.[119] Specifically, 94% of consumers surveyed in the United States think that personal information is vulnerable to misuse compared to 78% and 72% in the United Kingdom and Germany, respectively.[120]

iv. 1998 AARP Survey.

A survey conducted by the American Association of Retired Persons (AARP) in December 1998 and released in February 1999 shows the concern many elderly people have about the loss of their privacy: 78% of the respondents believed that federal and state laws are not strong enough to protect personal privacy from businesses that collect information about consumers,[121] 87% of respondents are bothered by businesses, government agencies, and web sites that sell their personal information to other businesses,[122] 81% opposed the internal sharing

of customers' personal and financial information by corporate affiliates, and 42% of respondents did not know whom they would turn to for assistance if a company inappropriately shared or sold their personal information.[123]

v. Harris Surveys.

In 1997, a Harris survey found that the majority of consumers engaging in online activities are worried about the confidentiality and security of the internet.[124] Respondents stated that they do not trust internet companies, nor do they trust the voluntary privacy policies of these companies.[125] Some 56% of online users believe that the government should enact laws governing the use of consumer information collected via the internet.[126] In December 1998, another Harris survey found that 88% of consumers are worried about threats to their personal privacy.[127] 78% believed businesses ask for too much information about them.[128]

vi. Boston Consulting Group Survey on Electronic Commerce.

According to a survey conducted by the Boston Consulting Group, 86% of consumers want to be able to control personal data, and 81% believe web sites do not have the right to resell personal information about them to third parties.[129] Indeed, 70% of survey respondents said that concerns about privacy were the primary reason they do not register at web sites and, when they do, 27% of the time the information they provide to register is false.[130]

vii. 1996 DIRECT Poll.

In 1996, DIRECT, a prominent marketing magazine, conducted a national survey.[131] 83% of the public surveyed supported a law requiring companies to obtain consent before including consumers on mailing lists.[132] 78% of respondents supported an opt-in system, even if it meant that they would not receive new mailings,[133] and 58% of the poll's respondents wanted to outlaw the collection and dissemination of Social Security numbers.[134]

viii. 1997 MONEY Magazine Poll and 1991 TIME-CNN Poll.

In 1997, a Money Magazine Poll found that 88% of the public favor a privacy bill of rights.[135] This bill of rights would require companies to tell consumers and employees exactly what kind of personal information they collect and how they use it.[136] Similarly, a 1991 TIME-CNN poll found that 93% of respondents believed that the law should require companies to obtain permission from consumers before selling their personal information.[137]

ix. 2000 Star Tribune Poll.

A survey by Minnesota's largest newspaper revealed that 87% of those surveyed want a ban on the commercial sharing of their phone-calling and Web-browsing habits unless the company obtains a consumer's permission.[138] The survey of Minnesota citizens, conducted by the Star Tribune newspaper, also found that the support for such privacy measures runs "deep and wide" across party lines.[139]

c. Consumers strongly react to breach of privacy by vendors.

When consumers are made aware of how their personal information is being sold or collected without consent, they overwhelmingly condemn the action in what may be called a "privacy revolt." These privacy revolts, some of which are listed below, illustrate the passion people feel about their privacy.

i. Sale of telephone listings.

In 1990, New York Telephone disclosed in its billing statements that it intended to sell its customer white pages listings to third parties.[140] A full 800,000 customers told the company to remove their names from the list.[141] Bell Atlantic's announcement to sell its white pages directory in 1995 created a similar outcry from consumers for more privacy.[142]

ii. Sale of name, address, estimated income, and propensity to buy.

In 1991, Lotus Development and Equifax announced a plan to market a CD-ROM product known as "Lotus Marketplace: Households."[143] The CD-ROM was to contain information on 80 million households, including names, addresses, estimated income, and propensity to buy over 100 types of consumer products.[144] Anyone could purchase this information for $695.[145] After the product was announced, 30,000 consumers demanded removal of their names, and the project was abandoned.[146]

iii. Sale of computer chip that monitors on-line activity.

In 1999, Intel Corporation abandoned its plan to introduce a new Pentium III chip that contained an imbedded serial number to allow the company to trace the equipment and consumer use.[147] Despite possible benefits, consumers threatened to boycott Intel when the chip was announced.[148]

iv. Coupling internet browsing habits with user names and addresses.

In March 2000, DoubleClick abandoned its plan to merge consumers' heretofore anonymous internet browsing habits with their names, addresses, and phone numbers gleaned from more traditional database sources.[149] DoubleClick is the largest and most influential e-commerce advertising network and has a partnership with virtually every advertiser on the internet.[150] DoubleClick collects millions of pieces of information about consumers every day, such as where they shop and spend time on the internet, but much of this information is anonymous.[151] The company planned to start matching this anonymous information with outside sources, thus eliminating an individual's on-line privacy.[152] DoubleClick abandoned these plans in the face of public and governmental pressure, including the threat of litigation.[153]

v. Sale of drivers' license photographs.

Likewise, in February 1999, South Carolina, Florida, and Colorado canceled their attempt to sell drivers' license photographs to retailers and police.[154] When citizens learned of the effort, they flooded state offices with calls and e-mails.[155] Facing such strong citizen opposition, the states terminated their contracts.[156]

3. Strong public expectation of privacy stifled at legislative level by intense lobbying efforts of industry.

Despite staunch public support, recent legislative efforts to safeguard individual privacy have been largely unsuccessful. In the 1999-2000 legislative session, 41 states introduced more than 100 bills designed to enhance individual privacy protection.[157] Virtually every proposal to strengthen privacy protection was defeated. Most people attribute the defeat to a powerful lobbying effort on behalf of financial institutions, insurance companies, telemarketers, and retailers.[158]

According to news reports, a proposal for enhanced financial privacy in the State of Washington was defeated by "an army of lobbyists" from "out-of-state megacorporations."[159] Washington Attorney General Christine Gregoire counted 69 business lobbyists actively working to defeat her privacy proposals.[160] In Minnesota, privacy proposals were formally opposed by 118 lobbyists.[161] At one hearing, 59 lobbyists signed up to testify against a bill to establish a state "Do-Not-Call" list and to require telemarketers to get express consent before they bill a credit card.[162]

Federal privacy proposals also face intense opposition by both companies and traditional trade associations.[163] There have been several proposals to close many of the loopholes in the federal Gramm-Leach-Bliley Financial Services Modernization Act, which allows affiliated

banks, insurance companies, stock brokerages, and telemarketers to share consumer information with one another without consent.[164] However, these proposals have not as of this writing emerged from committee due to intense pressure from lobbyists opposed to stronger privacy laws.[165] The industry wants desperately to retain the privacy provisions originally enacted, which one commentator, William Safire, referred to as a "sellout" engineered by the banking lobby.[166]

Indeed, privacy opponents have created well-financed organizations designed to stop any legislation.[167] The National Business Coalition on E-Commerce and Privacy has over a dozen members, including General Electric Co., Fidelity Investments, Visa USA Inc., State Street Corp., and Deere & Co.[168] Each member of the group must pay at least $40,000 a year to fund the lobbying effort.[169] The Financial Services Coordinating Council represents the American Bankers Association, American Council of Life Insurance, American Insurance Association, Investment Company Institute, and the Securities Industry Association.[170] The Privacy-Plus Coalition is comprised of telemarketers and insurance companies and has been active in virtually every state.[171] Senator Margarita Prentice, a sponsor of the Washington State financial privacy bill, described the Coalition's strategy as utilizing "innuendo, lies, timing, [and] bad faith."[172] The lobbyists' goal is simply to hold the line, under the theory that if privacy legislation is adopted anywhere "it's a hole in the dike and others will begin adopting it."[173]

III. PROPERTY DAMAGE DUE TO PRIVACY VIOLATIONS.

Not all information sharing is alike. There is a significant distinction between information sharing for the purposes of responding to a customer's request versus sharing information without the consumer's knowledge or consent to market goods or services unrelated to that request. The difference is rooted in the expectations of the consumer and whether he or

she has given consent to the particular use of the data. The privacy debate should properly focus on the use of information beyond the legitimate purposes for which it was initially collected or disclosed--the so-called secondary use of information. This section therefore focuses only on the harm caused when commercial entities share information with third party telemarketers or for marketing an affiliate's unrelated goods and services.

Over the past ten years, commercial interests have collected massive amounts of information about individuals which is used readily to encroach on consumer privacy. The wide dissemination of such information and purchasing habits has harmed consumers by creating an environment susceptible to identity theft and unauthorized charges.[174] There is also a growing perception that the financial market is less secure and that partnerships between financial institutions and telemarketers may destabilize the financial industry.

An example of the widespread use of this information is the explosion of pre-approved credit card offers filling mailboxes across the country on a daily basis. Credit card interest rates, however, have remained stable at about 18% for over twenty years despite the decrease in the costs to service and fund these credit cards. *U.S. Credit Card Industry: Competitive Developments Need To Be Closely Monitored*, U.S. GEN. ACCOUNTING OFFICE, CHAPTER REP., Apr. 28, 1994, at 1-2. The interest rates also seem to bear little relation to an individual's actual credit-worthiness, or fluctuations in the economy. *See id.* at 2 (noting the wide difference between the cost of funds and average credit card interest rates). Meanwhile the amount of credit card debt in the United States has increased from $39 billion in 1983 to approximately $156 billion in 1993. *Id.* There is no evidence that credit card debt has decreased from 1993 to present.

A. Increase In Identity Theft.

Between 500,000 and 700,000 people will have their identities stolen this year, and the problem costs consumers nearly $1 billion per year.[175] Identity thieves often operate by opening a credit card account using their victim's name, date of birth, or Social Security number.[176] They then use that credit card to rack-up charges for which they never pay the bill.[177] Identity thieves also open checking accounts and write bad checks, or establish cellular phone service, in the victim's name with no intention of paying the service fees.[178] In all of these cases, the delinquent charges are recorded on the victim's credit report. Individual victims of identity theft spend an average of two or more years attempting to fix their credit report and restore their credit rating.[179] A recent study found an average of $18,000 in unauthorized charges per identity theft victim.[180]

Identity theft is directly related to the erosion of privacy. As personally-identifying information has become freely available, the rate of identity theft has increased. According to Trans Union Corporation, one of the national credit bureaus, two-thirds of all consumer inquiries to the company's Fraud Victim Assistance Department involve identity fraud.[181] The total number of inquiries has also increased from 35,235 in 1992 to 522,922 in 1997,[182] and yet, the free-flow of personal information continues virtually unchecked.[183]

There are currently no laws that provide consumers the right to block access to their credit reports without consent.[184] There are also no laws to prevent someone from buying or selling an individual's Social Security number without their consent, or to prevent a company from refusing to do business with individuals who do not divulge their Social Security number.[185]

Neither consumer education nor criminalizing identity theft has been sufficient to stop the misuse of personal information and subsequent fraud. While an individual's financial privacy has eroded, credit bureaus have generated "tens of millions" of dollars annually from the sale of personally-identifying information.[186]

B. Prevalence Of Unauthorized Charges Via Pre-Acquired Account Telemarketing.

Telemarketing fraud is a $15 to $40 billion dollar enterprise.[187] Many consumer organizations, federal agencies, and state agencies have joined together to fight telemarketing fraud by educating consumers and prosecuting unscrupulous telemarketers.[188] Unfortunately, the free-flow of information has created a new marketing method called pre-acquired account telemarketing.

Pre-acquired account telemarketing typically occurs when financial institutions sell their customer's account history to a telemarketer without the customer's express consent.[189] The telemarketer then uses this information to call individual consumers without disclosing that they already possess the individual's account information or that they have the ability to charge the individual's account. The telemarketer's possession of this information can lead to a significant number of unauthorized charges, in part because consumers believe that a customer must read his or her account number over the phone or submit a signed form in order to consent to the charge.[190] Pre-acquired account telemarketing deceptively takes advantage of this belief because the telemarketer never asks for an account number or other financial data. Rather, the telemarketer engages in a low threshold sales technique where the customer's assent to try a 30-day free offer is, unknown to the consumer, used to charge his or her account 30 days later. Interviews of hundreds of complainants by the Attorney General's Office show that the

consumers had no knowledge that their assent to a 30 day "free trial" meant that the telemarketer could charge their account.

While telemarketing companies investigated by the Attorney General's Office claim that they obtain express oral consent before billing an individual's account, a Federal Trade Commission task force found that the companies' definitions of "consent" frequently fall far short of protecting consumer interests.[191] Consumers often are not meaningfully told that the telemarketing company will automatically bill their credit cards after thirty days, and thus the consumers' belief that the telemarketer cannot charge them since they never actually disclosed their account number remains intact.[192] Rather than obtain a card number from the consumer, the telemarketer obtains agreement from the consumer only to receive a "packet of information," which the telemarketer takes as express consent to debit the consumer's account.[193]

The State of Minnesota's lawsuit against MemberWorks, which uses customer information obtained from financial institutions to market a variety of discount membership programs, is illustrative of how pre-acquired account telemarketing works. MemberWorks used data obtained from financial institutions to telemarket an offer of a 30-day free trial enrollment in its membership programs, telling some consumers that "you don't have to make a decision over the phone."[194] However, consumers actually *were* making an important decision over the phone to allow MemberWorks to charge their credit card or checking account for enrollment in the membership club if the consumer did not call MemberWorks within 30 days to cancel.[195] Numerous consumers believed they were protected because they had not revealed their account number to MemberWorks.[196] Unfortunately, they did not know that MemberWorks could charge their account because of their marketing agreement with the customer's bank.[197] MemberWorks made much fanfare about its claim that it had audiotapes documenting consumers' consent to

such charges; however, many audiotapes produced by MemberWorks during litigation did not document a meaningful consent from consumers prior to charging their accounts.[198]

State and federal prosecutors of those who perpetrate telemarketing fraud typically tell consumers to protect themselves by never giving a credit card number, checking account number, Social Security number, or other sensitive information to an unknown caller. Unfortunately, this advice will no longer stop fraud because telemarketing firms have already purchased that information from financial institutions before the phone call is ever made.

C. Potential To Destabilize Financial Institutions.

The Great Depression of the late 1920s and early 1930s caused tremendous financial instability in the United States.[199] Nine-thousand banks collapsed between 1929 and 1933.[200] At the urging of President Roosevelt, Congress enacted laws to bring order to the system, including creation of the Federal Deposit Insurance Corporation (FDIC) to guarantee stability and be a "symbol of confidence."[201] With the deregulation of the financial industry by the Gramm-Leach-Bliley Act of 1999, many of the statutory safeguards put in place as a result of the Depression have been repealed. Widespread information sharing may threaten confidence individuals have in their financial institutions.[202]

In the mid-1990s, state and federal agencies were alerted to an information-sharing agreement between NationsBank and its in-house stock brokerage subsidiary. NationsBank had revealed the names of its customers whose low-risk CDs were coming due.[203] The stock brokerage then enlisted a telemarketing firm to target those customers. The telemarketers allegedly convinced more than 18,000 bank customers to shift their low-risk investments into high-risk uninsured hedge funds.[204] Yet, NationsBank claimed it did not violate any existing

privacy laws. It would appear that such actions might even be permissible under the lackluster privacy provisions of the Gramm-Leach-Bliley Act.[205]

According to John Hawke Jr., Comptroller of the Currency, banks have "assiduously shied away" from taking a leadership role in developing industry standards for consumer protection.[206] Specifically, Hawke condemned the information sharing practices between some financial institutions and telemarketers as "seamy, if not downright unfair and deceptive."[207]

1. Information sharing is a widespread practice in the financial industry.

With little notice to their customers, many financial institutions and telemarketers have routinely entered into marketing agreements with one another over the past few years. These marketing agreements allow the telemarketer to have access to bank customer information, such as names, phone numbers, Social Security numbers, account balances, and credit limits. The amount of information distributed varies, but the marketing agreements have become a standard industry practice among the country's largest financial institutions.[208]

On June 9, 1999, a lawsuit against US Bancorp by the Minnesota Attorney General's Office revealed the prevalence of financial information sharing between telemarketers and financial institutions.[209] The lawsuit alleged that the bank disclosed the names, phone numbers, social security numbers, account balances, and credit limits of almost one million of its customers after telling them that "all personal information you supply to us will be considered confidential."[210] At the end of June, US Bancorp settled Minnesota's lawsuit for $3 million and stopped participation in marketing programs for nonfinancial products.[211]

In the weeks following the US Bancorp lawsuit, numerous other financial institutions revealed that they had been engaging in similar practices that affected millions of consumers.[212] While it initially did not reveal the details of its marketing practices, Wells Fargo eventually

revealed that it had shared customer information with telemarketers and claimed it would temporarily suspend the practice.[213] Bank of America, Union Bank, and Citigroup also admitted to sharing customer financial data.[214] CHASE Manhattan revealed that it similarly had entered joint marketing agreements, and eventually entered a settlement agreement with the New York Attorney General's office.[215] In total, these financial institutions have at least 70% of the market share in the nation's 40 largest metropolitan areas.[216]

2. Loss of confidence and destabilizing effect of information sharing.

Although financial institutions may profit from cross-marketing opportunities, these developments come at a price.[217] Customer complaints to the Office of the Comptroller of Currency (OCC), the agency that regulates nationally-chartered banks, have more than quadrupled from 1997 to 1999.[218] If financial institutions continue to share information, an increase in such complaints are likely.

In November of 1997 a convict on probation for aiding and abetting a counterfeiting scheme was able to purchase from Charter Pacific Bank of Los Angeles at least three credit card databases. Charter Pacific Bank sold several million credit card numbers to the convicted felon, who then fraudulently billed 900,000 of the accounts for a total of $45.7 million before he was stopped.[219] These Visa and MasterCard holders were billed for unauthorized charges to a network of X-rated websites run by the felon.[220] Charter Bank responded to the fiasco by stating that it had not violated any existing privacy laws.[221]

The sale and abuse of confidential consumer information is contrary to the expectations and trust individuals have historically placed in their financial institutions and may cause fundamental damage to the banking system.[222] The Comptroller of the Currency, John Hawke, has observed:

> I cannot overstate the importance of addressing consumer expectations about the confidential treatment of financial information to maintaining the public's confidence in the banking system. And I urge that, in crafting an appropriate response to consumer privacy concerns, banks and Congress put themselves in the shoes of a customer and ask, "Will my financial institution use my personal information in a manner consistent with my expectations?" and "Will I have any control over the use of my information?" [223]

Under the existing law, the answer to both of Hawke's questions is uncertain.

IV. PROTECTING CONSUMERS WITH AN OPT-IN.

The best response to many of the privacy concerns that have recently arisen is the adoption of an "opt-in" system for highly sensitive personal information. Unfortunately, the debate over whether commercial entities should implement an opt-in or an opt-out system, or no system at all, has been muddled with misinformation and wild claims about the effect either system will have on information collection and an individual's right to privacy.[224] The following section attempts to describe an "opt-in" system, describe the inherent problems with its alternative, an "opt out" system, and outline the reasons that an "opt in" system is good public policy with respect to protection of our most personal information.

A. Defining An Opt-In and Opt-Out System.

"Opt-in" and "opt-out" are terms that create presumptions. Under an opt-in system, information will remain private unless a person consents to its disclosure. "Opt-in" provides an opportunity for consumers to weigh in--to say "yes"--before their information is shared.[225] By contrast, under an opt-out system, information may be shared and made public unless a person instructs the entity to keep it confidential. An opt-out system allows unlimited sharing of private information unless and until a consumer says "stop."[226] Conservative commentator William Safire describes the difference between opt-in and opt-out as "the difference between a door locked with a bolt and a door left ajar."[227]

B. The Inherent Problems With An Opt-Out System.

There are three fundamental problems with an opt-out system that undermine its ability to adequately protect an individual's privacy interests concerning the treatment of sensitive personal information. First, a successful opt-out system is conditioned upon individuals being able to understand how companies are using their personal information. Second, a successful opt-out system is conditioned upon individuals getting meaningful notice that they have a right to opt-out of this information sharing. Third, a successful opt-out system is conditioned upon consumers being able to effectuate their preference without undue convenience. An opt-out system cannot operate effectively because there is no true individual control over the exchange of personal information.

1. Consumers do not understand how personal information is being disclosed.

The secrecy surrounding how personal consumer information is used by commercial entities limits the potential for consumers to act.[228] Companies routinely fail to disclose the manner in which they use sensitive information. Unless an individual notices an unauthorized charge or some other irregularity, the information sharing will continue indefinitely regardless of the individual's desire to keep that information private. Even companies that provide some notice of their information-sharing practices typically fail to disclose who will receive the information, how it will be used, whether the information will be merged with another databased or networked information, and the manner a company may use to solicit a consumer whose information has been shared.

In addition, the opt-out notice is usually surrounded by confusing and misleading information that prevents individuals from understanding how their personal information may be

disclosed. For example, in the spring of 2000, *The New Yorker,* a national magazine, sent a lengthy, 44-question survey to "loyal" or "preferred subscribers." The questionnaire sought information about everything from subscribers' shopping habits to their medical ailments, on grounds that the magazine wanted "to maintain an open dialogue with our subscribers." Among other things, the magazine publisher asked subscribers if they were clinically depressed, menopausal, overweight, used birth control, had menstrual pain, gastritis or nail fungus. In the cover letter asking subscribers to return the survey, *The New Yorker* stated that this personal information would be shared with "select advertisers," but failed to identify those "select advertisers," what criteria is used to select the advertisers, or the scope of its so-called "Preferred Subscriber Network." Faced with a company's incomplete, inadequate or deceptive descriptions of its information-sharing practices, consumers are left with little opportunity to exercise meaningful, informed consent to opt out of such collection or sharing.

2. Consumers are not given meaningful notice that they have the right to opt out.

Many Americans are unaware that they have a right to opt out, and companies make a weak effort to give notice of that right.[229] The failure of an opt-out system is demonstrated by a comparison of the vast number of individuals who want to protect their privacy with the small number of individuals who actually opt out. For example, Bank of America's response rate to its opt-out notice is 0.2%, even though most public opinion polls suggest that upwards of 60-80% of individuals do not want their financial information disclosed.[230] Of the 195 million Americans solicited by Acxiom Corporation, fewer than 300 people had opted-out by the end of 1997.[231] Although banks, telemarketers, and internet companies claim that these opt-out notices provide

consumers with a "choice," such opt-out systems are plainly ineffective and far from actual "consent." [232]

An opt-out system encourages businesses to use misleading or vague privacy policies hidden in the fine print of a policy agreement or contract:

> At present, businesses have little incentive to disclose to consumers how their personal information is used or that they can opt-out of its use. As a result, the current system produces inefficient results. A change in the default rule [to an opt-in] gives businesses an incentive to make disclosures and increases the likelihood that an efficient market will result.[233]

A typical opt-out notice has been described as something that you need "the eyes of an eagle" and "a law degree" to find and understand.[234] Typically, the opt-out is placed in the "fine print with other boilerplate terms."[235] Consumers do not take advantage of opt-out opportunities because they often do not know they can opt out, even if they are generally aware of the information sharing practices of the company.

3. Opt-out systems currently utilized impose cumbersome procedures upon the consumer.

The amount of time, inconvenience, and cost of exercising an opt-out right is substantial.[236] For example, the Federal Communications Commission (FCC) has found that subscription rates for different telephone maintenance plans are highly correlated to whether or not the seller used an opt-out system. When telephone companies obtained affirmative consent for optional maintenance telephone plans, about 45% of consumers selected the product, but when the telephone company used an opt-out the number of consumers who "selected" the product nearly doubled. Cable companies in the United States and Canada have also had similar experiences with the opt-out system when selling premium cable channels, with the number of people being billed for additional services 30% higher than if the company was required to obtain affirmative consent.[237]

In short, "[p]eople are too pressed in their daily routines to initiate, lead, or otherwise control most consumer contracting."[238] An opt-out system places a cumbersome burden on consumers to inform a company that they do not want personal information shared, which they reasonably expect should remain confidential, when the burden should rest with the company to obtain consumers' consent before disclosing highly personal information.

C. An Opt-In System Follows a Basic Premise of Contract Law Concerning "Acceptance" of an "Offer."

The right to privacy has alternatively been described as the "right to be let alone," "the right to individual autonomy," and "the right to a private life."[239] Underlying each of these definitions is the desire of the consumer to control access to and use of personal information.[240] The most effective method of protecting an individual's right to privacy is a system that recognizes an individual's ability to contract with companies as to how sensitive personal information, such as financial records, telephone records, and the like, will be maintained.

An opt-out system is a negative-option approach to contract law which undermines a fundamental concept of contract formation under the common law--that silence does not equal consent.[241] A contract requires both an offer and acceptance.[242] Assuming that consumers consent by their silence violates the consumer's autonomy and freedom to contract.[243] An opt-out system transforms silence into acceptance of a company's information sharing practices, contrary to the accepted norms of contract law.[244]

1. An opt-in system offers the consumer a meaningful opportunity of "selection."

An opt-in system offers consumers the legitimate opportunity to affirmative consent.[245] It requires that the company give meaningful notice, and perhaps even pay consideration, for the use of the customer's name and data. By "opting in," the consumer has meaningfully contracted

with the company concerning the private data. With affirmative consent, individuals are afforded a procedural safeguard which gives the consumer control over their data.[246]

2. An opt-in system is consistent with consumers' reasonable expectations of privacy.

The surveys cited earlier make it clear that consumers do not reasonably expect that the information they provide to facilitate a loan or credit card transaction will be collected and later shared with other commercial entities. This is a secondary use of information beyond the reasonable expectations of consumers who provide the information for a different primary purpose. An opt-in system is consistent with these expectations, as it requires commercial entities to obtain consent *before* information is shared for secondary uses.

A banking opt-in law does not interfere with transactions initiated by the customer, such as writing a check, applying for a loan, or using money from an ATM machine.[247] Indeed, depository and ATM account agreements already require the customer to "opt in" because the customer agrees that such information may be shared.[248] However, if a company wants to use information, beyond servicing a customer's request, for whatever reason, then it should explain such information-sharing practices in the depository account agreement. If businesses have worthwhile reasons for disclosing a customer's personal records for secondary uses, then consent should not be difficult to obtain.[249] Indeed, there is nothing to prevent a bank from refusing to service the customer if he does not agree to opt in to the arrangement. An opt-in provision gives notice to the customer that information collected about them for one use will be disclosed for a different, secondary use.

3. An opt-in system better balances bargaining power between businesses and consumers.

Information sharing is often justified as necessary to provide an individual with valuable information about quality products and services. Yet, under an opt-out system, individual consumers are not allowed to determine for themselves whether the information is actually valuable or whether the products and services are of high quality. An opt-in system gives the individual power to control distribution of their personal information, which in turn increases the individual's bargaining power by allowing him or her to effectively set the market price for personal financial or credit information. In order for the consumer to provide consent, the potential products and services must be of sufficient value to offset the corresponding invasion of the consumer's privacy. Opt-in empowers the consumer to decide whether waiver of privacy rights is justified by corresponding benefits of information flow.

4. An opt-in allows businesses to find consumers favorably disposed to marketing.

Information allows businesses to focus their resources to avoid wasteful marketing of products and services to uninterested consumers. An opt-in system identifies a pool of consumers favorably disposed to such marketing, because individuals demonstrate their desire to receive marketing materials about specific products by exercising their right to opt in. An opt-in system thus improves the quality of information that does exist,[250] making marketing of products ultimately more efficient.

Although an opt-out system may increase the quantity of information in the short-term, over time both the quantity and quality of the information may diminish.[251] Individuals will not make a purchase or apply for a job, credit, or insurance because they do not want their privacy

invaded.[252] Individuals may also provide false information requested on such applications in order to protect their privacy.[253]

For example, e-mail marketers used to send unsolicited marketing material, dubbed "Spam," to internet users without their consent.[254] That method of marketing has resulted in a backlash from consumers, and possible litigation.[255] Internet companies have now concluded that the best way to market their materials is through an opt-in system.[256] An industry leader in on-line marketing, NetCreations, Inc., discovered that "empowering" consumers with an opt-in, and then giving them an opportunity to opt-out every time they are sent a marketing message, is the best method to maintain customer goodwill and sell products on behalf of companies like Dell Computer, Compaq, and J. Crew. [257][258] The opt-in system is considered by some internet marketers to be the "best business practice." [259]

V. CONCLUSION.

There is an immediate need to enact privacy laws governing the use of personal information such as bank and telephone records. This need is more acute as deregulation and technology have allowed institutions to merge, affiliate, and associate such that massive amounts of highly confidential information may be readily shared among them. Neither existing laws nor self-regulatory efforts are adequate to protect consumer privacy in the information age. The lack of protection undermines an individual's right to privacy and choice.

Failing to protect an individual's right to privacy has caused real economic harm. An opt-in approach for handling such information protects against these harms, while recognizing both the liberty and property interests in personal information. An opt-in approach is also consistent with consumers' reasonable expectations and is overwhelmingly favored by the

public. Finally, an opt-in system enhances a consumer's bargaining power and better hones a business's target marketing consistent with consumers' legal privacy rights.

Consumer outrage over the unregulated, non-consensual trading of highly sensitive information will continue to mount unless and until policymakers enact strong privacy legislation. Simply, an opt-in system for the sharing of sensitive personal information must be central to those legislative efforts in order to both protect an individual's privacy and prevent information sharing for secondary uses without consent.

---

† Special thanks to the following staff of the Minnesota Attorney General's Office for their assistance on this article: Deputy Attorney General Lori R. Swanson, Assistant Attorneys General Mark Ireland, Erik Lindseth, and David Ramp, and law clerk Jane Prine.

[1] Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 2 (2000).

[2] *See* Hippocratic Oath, Fifth Century B.C.

[3] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[4] *Id.* at 193-95.

[5] *See* Carey v. Population Servs. Int'l, 431 U.S. 678, 684 (1977) (noting that one aspect of liberty is a right of personal privacy, holding that this right includes "making certain kinds of important decisions").

[6] Loving v. Virginia, 388 U.S. 1 (1967).

[7] Skinner v. Oklahoma, 316 U.S. 535 (1942).

[8] Eisenstadt v. Baird, 405 U.S. 438 (1972).

[9] Prince v. Massachusetts, 321 U.S. 158 (1944).

[10] Pierce v. Society of Sisters, 268 U.S. 510 (1925).

[11] Griswold v. Connecticut, 381 U.S. 479, 485 (1965) (holding Connecticut's law that places restrictions on providing information about contraception unconstitutional as it intrudes upon the right to marital privacy). *See also* Eisenstadt, 405 U.S. at 453 (evaluating the constitutionality of a law restricting the distribution of contraceptives to unmarried persons; broadening the *Griswold* privacy definition so that it includes single individuals as well as married couples).

[12] Roe v. Wade, 410 U.S. 113 (1973).

[13] *See* Planned Parenthood v. Casey, 505 U.S. 833, 887 (1992).

[14] *Id.* at 851.

[15] Board of Directors of Rotary Int'l v. Rotary Club of Duarte, 481 U.S. 537, 545 (1987).

[16] Frisby v. Schulz, 487 U.S. 474, 484 (1988) (citing Carey v. Brown, 447 U.S. 455, 471 (1980)).

[17] U.S. CONSTIT. amend. IV. *See also* Katz v. United States, 389 U.S. 347, 353 (1967) (noting that the Fourth Amendment protects not only areas against unreasonable searches and seizures, but also people).

[18] Miranda v. Arizona, 384 U.S. 436, 459 (1966) (citations omitted).

[19] *See* RESTATEMENT (SECOND) OF TORTS §§ 652A-652E (1977). William L. Prosser gave the right to privacy definition by separating the various court rulings that supported Warren and Brandeis's theories into four distinct causes of action. W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS, §117, at 850-51 (5th ed. 1984).

[20] *See* RESTATEMENT (SECOND) OF TORTS §§ 652A-652E (1977) (adopting Prosser's privacy tort theory).

[21] *Id.* § 652B.
[22] *Id.* § 652C.
[23] *Id.* § 652D.
[24] *Id.* § 652E.
[25] Pavesich v. New England Life Ins. Co., 50 S.E. 68, 71 (Ga. 1905).
[26] *See, e.g.*, Truxes v. Kenco Enters., Inc., 119 N.W.2d 914 (S.D. 1963); McCormack v. Oklahoma Publ'g Co., 613 P.2d 737 (Okla. 1980); Hinish v. Meier & Frank Co., 113 P.2d 438 (Or. 1941). Other states, finding no constitutional or common law basis for the invasion of privacy tort, have enacted rights to privacy by statute. *See, e.g.,* MASS. GEN. LAWS ANN. ch. 214, § 1B (West 1989); NEB. REV. STAT. ANN. § 20-201 (West 1995); N.Y. CIV. RIGHTS LAW § 50 (1992).
[27] Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231 (Minn. 1998).
[28] *Id.* at 233.
[29] *Id.* at 235. The Minnesota Supreme Court recognized the torts of intrusion upon seclusion, public disclosure of private facts and appropriation of one's likeness. *Id.* at 236.
[30] *Id.* at 235. For an extended discussion of *Lake v. Wal-Mart Stores, Inc.*, see Jane E. Prine, *No Longer Living in a Glass House: Every Minnesotan Is Entitled to a Right to Privacy*, 25 WM. MITCHELL L. REV. 999 (1999).
[31] MINN. STAT. § 144.69 (1998).
[32] MINN. STAT. § 144.768 (1998).
[33] MINN. STAT. § 290.611 (1998).
[34] MINN. STAT. § 254A.09 (1998).
[35] MINN. STAT. § 13.46 (1998).
[36] MINN. STAT. § 13.32 (1998).
[37] MINN. STAT. § 13.40 (1998).
[38] MINN. STAT. § 13.44 (1998).
[39] MINN. STAT. § 13.56 (1998).
[40] MINN. STAT. § 13.531 (1998).
[41] MINN. STAT. § 144.335, subd. 3a (1998). *See also* MINN. STAT. § 144.651, subd. 16 (1998) ("Patients and residents shall be assured confidential treatment of their personal and medical records, and may approve or refuse their release to any individual outside the facility.")
[42] MINN. STAT. §§ 151.213; 151.23 (1998).
[43] MINN. STAT. § 72A.502, subd. 1 (1998).
[44] Video Privacy Protection Act, 18 U.S.C. § 2710 (1999).
[45] Cable Television Record Privacy Act, 47 U.S.C. § 551 (1999).
[46] Driver's Privacy Protection Act, 18 U.S.C. § 2721, *amended by* Shelby Amendment, Pub. L. No. 106-96 (2000). *See also* MINN. STAT. §§ 168.346; 171.12 (1998).
[47] MINN. R. PROF. CONDUCT 1.6.
[48] MINN. R. PUB. ACCESS TO RECORDS OF JUDICIAL BRANCH 4, subd. 1(a); MINN. R. JUV. PROC. 30.02, subd. 3.
[49] MINN. R. JUV. PROC. 2.01.
[50] MINN. R. CIV. PROC. 26.03.
[51] MINN. STAT. § 595.02, subd. 1 (a) (1998). *See also* Lundman v. McKown, 530 N.W.2d 807, 829 (Minn. Ct. App. 1995) (acknowledging that a spouse may assert the marital privilege to bar a witness spouse from testifying).
[52] MINN. STAT. § 595.02, subd. 1 (c) (1998). *See also* State v. Orfi, 511 N.W.2d 464, 469 (Minn. Ct. App. 1994) (finding that portions of the defendant's communication with ministers subject to clergy privilege).
[53] MINN. STAT. § 595.02, subds. 1 (g); 1 (i) (1998).
[54] Richfield Bank & Trust Co. v. Sjogren, 244 N.W.2d 648, 651 (1976) (finding that a bank is generally under a duty not to disclose the financial condition of its depositors). *See also* Cunningham v. Merchants' Nat'l Bank, 4 F.2d 25 (1st Cir. 1925), *cert. denied* 268 U.S. 691 (1925); Milohnich v. First Nat'l Bank, 224 So.2d 759 (Fla. Ct. App. 1969); Peterson v. Idaho First Nat'l Bank, 367 P.2d 284 (Idaho 1961).
[55] MINN. STAT. §§ 325C.01-03 (1998).
[56] *See, e.g.,* Tenant Co. v. Advance Mach. Co., Inc., 355 N.W.2d 720, 726 (Minn. Ct. App. 1984); Creative Communication Consultants, Inc. v. Gaylord, 403 N.W.2d 654, 657 (Minn. Ct. App. 1987).
[57] *See, e.g.,* Burlington N. R.R. Co. v. Omaha Pub. Power Dist., 888 F.2d 1228 (8th Cir. 1989); Minnesota Mining & Manuf. Co. v. Kirkevold, 648 F. Supp. 661 (D. Minn. 1980).

[58] MINN. STAT. § 325C.05 (1998).
[59] 42 U.S.C.A. § 405 (1999) ("Social security account numbers and related records that are obtained or maintained by authorized persons pursuant to any provision of law… shall be confidential, and no authorized person shall disclose any such social account number or related record.")
[60] Fair Credit Reporting Act, 15 U.S.C. 1681 (1999).
[61] Privacy Act, 5 U.S.C. § 552a (1999).
[62] Bank Secrecy Act, 12 U.S.C. §§ 1951-1959 (1999).
[63] Access to Telephone Records Act, 18 U.S.C. § 2709 (1999).
[64] Taxpayer Browsing Protection Act, 26 U.S.C. § 7213(a) (1999).
[65] Universal Declaration of Human Rights, art. 12, 1948.
[66] Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, 1950.
[67] S. AFR. CONSTIT., §14, 1996.
[68] ARG. CONSTIT., arts. 18, 19.
[69] Parliament and Council Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data, 1995 O.J. (L281) 1.
[70] Ordinance No. 81 of 1995 (H. K.).
[71] Privacy Act of 1993 (N. Z.).
[72] Law of the Russian Federation on Information, Informatisation and Information Protection, January 25, 1995.
[73] Data Protection Act of 1973 (Sweden).
[74] Protection of Computer Processed Personal Data Held by Administrative Organs Act of 1988 (Japan).
[75] *See id.*
[76] The Act on the Protection of Personal Information Managed by Public Agencies of 1994 (S. Korea).
[77] GEORGE ORWELL, NINETEEN EIGHTY-FOUR 4 (1949).
[78] *See id.*
[79] CHARLES SYKES, THE END OF PRIVACY 4 (St. Martin's Press 1999). *See also* John Caher, *Privacy Initiative Aims for Consumer Protection*, N.Y. L.J., Jan. 24, 2000, at 1 ("It is not big brother that we now have to be afraid of, but big browser.") (quoting New York Attorney General Eliot Spitzer).
[80] Jane Bryant Quinn, *The Spies in Your Pocket*, NEWSWEEK, Aug. 16, 1999, at 43.
[81] Robert O'Harrow, Jr., *Data Firms Getting Too Personal?*, WASH. POST, Mar. 8, 1998, at AO1.
[82] William J. Fenrich, *Common Law Protection of Individuals' Rights in Personal Information*, 65 FORDHAM L. REV. 951, 952 (1996).
[83] *Id.*
[84] Acxiom Corp., *Marketing Materials*, *in* JOEL R. REIDENBERG, NAT'L ASS'N ATT'YS GEN., EXAMPLES OF THE SALE OF PERSONAL INFORMATION (Privacy Working Group, Sept. 23-24, 1999) [hereinafter EXAMPLES].
[85] *Id.*
[86] Medical Marketing Service, Inc., *Marketing Materials*, *in* EXAMPLES, *supra* note 84. *See also Medical Marketing Service, Inc.* (visited July 6, 2000) <http://www.mmslists.com/>.
[87] Medical Marketing Service, Inc., *Marketing Materials*, *in* EXAMPLES, *supra* note 84.
[88] *Id.*
[89] *Id.* Other examples of the misuse of medical information include the partnership between CVS pharmacy and pharmaceutical companies, and the partnership between a law firm and a hospital.

In 1998, pharmaceutical companies solicited customers of CVS Pharmacies who were identified by the pharmacy as suffering from specific medical conditions. Weld v. CVS Pharmacy, Inc., No. CIV. A. 98-0897F, 1999 WL 494114, at *1-2 (Mass. Super. Ct. June 29, 1999). On behalf of several pharmaceutical companies, CVS allegedly searched their customer database to find customers who suffered from high blood pressure or diabetes. *Id.* Then, CVS allegedly downloaded names and addresses of those customers onto a separate diskette, and gave the disk to a direct marketing firm. *Id.* On behalf of various pharmaceutical companies, those individuals were mailed advertisements about particular drugs and were encouraged to speak with their physician. *Id.* Litigation against CVS Pharmacies is currently pending. *Id.*

In 1993, Warren General Hospital in Ohio entered into a partnership with a local law firm to electronically search its medical records for patients who might be eligible for Supplemental Security Income reimbursement of medical expenses. Biddle v. Warren Gen. Hosp., No. 96-T-5582, 1998 WL 156997, at *1-2 (Ohio Ct. App. Mar. 27, 1998).

The hospital's database included the patient's address, birth date, employment information and their admitting diagnosis. *Id.* The law firm would contact patients about having their medical treatment paid for by the Social Security Administration. *Id.* The law firm would then receive a percentage of whatever money they generated for the hospital. *Id.*

[90] Student Marketing Group, Inc., *Marketing Materials*, *in* EXAMPLES, *supra* note 84. *See also Student Marketing Group, Inc.* (visited July 6, 2000) <http://www.studentmarketing.net>. Student Marketing Group also sells the names and addresses of preschool children ages 2-5. *Id.*

[91] Venture Direct, *Marketing Materials*, *in* EXAMPLES, *supra* note 84. *See also Venture Direct* (visited July 6, 2000) <http://www.venturedirect.com>.

[92] Adam L. Penenberg, *The End of Privacy*, FORBES MAG., Nov. 29, 1999, at 183.

[93] *Id.*

[94] *Id.*

[95] *See* Steven Vonder Haar, *Data Chase*, BRANDWEEK, Sept. 6, 1999, at IQ17 ("Call it the Golden Age of Online Data. More than ever before publishers, marketers and advertising service companies all are racing to compile mounds of information…")

[96] Wayne W. Eckerson & Lynne Harvey, *Customer Intelligence Drives Next-Generation Web Personalization* (Feb. 25, 2000) <http://www.customers.com>; Kayte VanScoy, *Get Inside Your Customers' Heads (and Their Wallets Too)*, SMART BUS. FROM ZDWIRE, June 1, 2000, *available in* 2000 WL 2000378 (describing data mining and rules for customer interaction).

[97] Nina Bernstein, *Lives on File: Personal Files via Computer Offer Money and Pose Threat*, N.Y. TIMES, June 12, 1997, at A1.

[98] *Id.*

[99] *Id.*

[100] Eckerson & Harvey, *supra* note 96, at 2-3.

[101] Mark Allan Baginskis, *Telemarketing Fraud upon the Elderly Shows No Signs of Slowing*, 11 LOY. CONSUMER L. REP. 4 (1999); Patrick E. Michela, *"You May Have Already Won…": Telemarketing Fraud and the Need for a Federal Legislative Solution*, 21 PEPP. L. REV. 553, 574 (1994).

[102] Privacy first emerged as an issue of public policy and concern with the publication of Warren and Brandeis' article, *The Right to Privacy*, written over one-hundred years ago. 4 Harv. L. Rev. 193 (1890). The authors advocated for the creation of a new tort that protected the private lives of ordinary people from intrusion or appropriation. *Id.* at 195. The computer has made their words even more applicable and insightful today.

The majority of states have now adopted the common-law right to privacy, but the law does not adequately protect individuals in the information age. Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 235 (Minn. 1998) (becoming one of the last states to adopt the common-law right to privacy).

[103] Robert O'Harrow, Jr., *A Postscript on Privacy,* WASH. POST, Nov. 5, 1999, at EO1.

[104] Senator Richard Shelby, *Coalition for Financial Privacy* (Oct. 13, 1999) <http://www.senate.gov/~shelby/press/prsrs307.htm>.

[105] *Id.*

[106] Clyde Mitchell, *Privacy and Gramm-Leach-Bliley's Financial Services Modernization*, N.Y. L.J., Apr. 19, 2000, at 3 (outlining current disputes as a result of Gramm-Leach-Bliley and formation of Congressional Privacy Caucus).

[107] Senator Richard Shelby, *Congressional Privacy Caucus* (Feb. 10, 2000) <http://www.senate.gov/~shelby/press/prsrs315.htm>.

[108] *Comments from the National Association of Attorneys General on Gramm-Leach-Bliley Act* (Mar. 31, 2000). Comments were signed by Attorney General Bruce M. Botelho (Alaska), Janet Napolitano (Arizona), Bill Lockyer (California), Kan Salazar (Colorado), Richard Blumenthal (Connecticut), Robert A. Butterworth (Florida), Stephen H. Levins (Hawaii Office of Consumer Protection), Alan G. Lance (Idaho), Jim Ryan (Illinois), Tom Miller (Iowa), Carla J. Stovall (Kansas), Andrew Ketterer (Maine), J. Joseph Curran, Jr. (Maryland), Tom Reilly (Massachusetts), Jennifer Granholm (Michigan), Mike Hatch (Minnesota), Mike Moore (Mississippi), Jeremiah W. Nixon (Missouri), Joseph P. Mazurek (Montana), Frankie Sue Del Papa (Nevada), John J. Farmer (New Jersey), Patricia Madrid (New Mexico), Eliot Spitzer (New York), Heidi Heitkamp (North Dakota), W.A. Drew Edmondson (Oklahoma), D. Michael Fisher (Pennsylvania), Sheldon Whitehouse (Rhode Island), Paul Summers (Tennessee), Jan Graham (Utah), William H. Sorrell (Vermont), Iver A. Stridiron (Virgin Islands), Christine O. Gregoire (Washington), Darrell V. McGraw Jr. (West Virginia).

[109] Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1057 (1999) (citing 1996 survey commissioned by Equifax).
[110] Julie Tripp, *Information-Selling Crushes Depositors' Faith*, PORTLAND OREGONIAN, June 20, 1999, at B05 ("'Appalling' and 'horrifying' were some of the other adjectives that got a workout last week when readers learned the details of what the Minnesota attorney general alleges U.S. Bancorp has been doing with their account, credit card, and Social Security numbers.")
[111] *Wal-Mart*, 582 N.W.2d at 235 ("The right to privacy is an integral part of our humanity: one has a public persona, exposed and active, and a private persona, guarded and preserved. The heart of our liberty is choosing which parts of our lives shall become public and which parts we shall hold close.") *See also* Griswold v. Connecticut, 381 U.S. 479 (1965) (recognizing the right to privacy as a fundamental right).
[112] Sovern, *supra* note 109, at 1057.
[113] Jedediah Purdy, *An Intimate Invasion*, USA WEEKEND, June 30-July 2, 2000, at 7 (stating that 62% of the respondents believed that too many people have access to their driving record, and 61% say that too many people have access to their medical records).
[114] *Id.* (noting that 65% of respondents believed that internet companies who track computer use and transactions have invaded their privacy, and 60% of respondents consider junk mail an invasion of their privacy).
[115] *Id.*
[116] N.Y. SENATE, THE SENATE MAJORITY TASK FORCE ON THE INVASION OF PRIVACY 12 (2000) [hereinafter SENATE]. *See also* Albert R. Hunt, *Bright Past Kindles America's Hope*, WALL ST. J., Sept. 16, 1999, at A9 (describing poll results).
[117] SENATE, *supra* note 116.
[118] *Id.*
[119] *Id.* (citing Grant Lukenbill, *Consumers Most Worried About Privacy*, DM NEWS, Dec. 29, 1999)
[120] *Id.*
[121] *Id.* (citing Mary Alice O'Brien, State Legislative Chair, American Association of Retired Persons, Testimony before the New York State Senate Majority Task Force on the Invasion of Privacy (Apr. 15, 1999)). *See also* AM. ASS'N RETIRED PERSONS, 39 DATA DIGEST, February 1999 (reporting December 1998 survey results with a +/- 4 % margin of error).
[122] *Id.*
[123] *Id.*
[124] Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate*, 49 S.C. L. REV. 847, 849 (1998) (citing Dr. Alan F. Westin, Testimony before the Financial Institutions and Consumer Credit Subcommittee of the House Banking and Financial Services Committee, *Electronic Payment Systems, Electronic Commerce, and Consumer Privacy*, FED. NEWS SERVICE, Sept. 18, 1997).
[125] *Id.*
[126] *Id.*
[127] Carol Krol, *Consumers Reach the Point over Privacy Issues: A Hot Marketing Concept is Running Smack into Big Concerns About the Extent of Company Usage of Personal Information*, ADVERTISING AGE, March 1999.
[128] *Id.*
[129] *Id.* at 850 (citing Drew Clark, *Worries About Privacy Rain on Net Commerce Parade*, AMER. BANKER, July 3, 1997, at 14). A 1999 AT&T study that found that Internet users are more likely to provide information when they are not identified. Melinda Reid Hatton & Mark Paulding, *Online Privacy - Some Milestones for the Millennium*, 587 PLI/PAT 823, 825-26 (2000). The AT&T study also found that 79% felt that it was important to their decision to use the internet if the company shares information with other companies or organizations.
[130] *Id.*
[131] SENATE, *supra* note 116, at 12.
[132] *Id.*
[133] *Id.*
[134] *Id.*
[135] Sovern, *supra* note 109, at 1062.
[136] *Id.*
[137] *Id.*

[138] Conrad deFiebre, *Minnesotans Make Public Their Desire for More Privacy Proposals to Restrict Telemarketers, Others Find Broad* Support, STAR TRIB., Apr. 6, 2000, at B1. *See also Jim Ramstad's 2000 Questionnaire Results,* RAMSTAD REP., Summer 2000, at 3 (finding that 84% of Congressional District 3 respondents favored "new regulations to prevent businesses from sharing your personal information with other businesses").
[139] *See* deFiebre, *supra* note 138, at B1.
[140] Budnitz, *supra* note 124, at 849.
[141] *Id.*
[142] *Id.*
[143] Joshua D. Blackman, *A Proposal for Federal Legislation Protecting Informational Privacy Across the Private Sector*, 9 SANTA CLARA COMPUTER & HIGH TECH. L.J. 431, 447 (1993).
[144] *Id.*
[145] *Id.*
[146] *Id.*
[147] Hatton & Paulding, *supra* note 129, at 840.
[148] *Id.*
[149] *Privacy Din Sparks DoubleClick Deal*, ADVERTISING AGE, March 6, 2000.
[150] *Id.*
[151] *Id.*
[152] *Id.*
[153] *Id.*
[154] CHARLES SYKES, THE END OF PRIVACY 4 (St. Martin's Press 1999).
[155] *Id.*
[156] *Id.*
[157] Rachel Zimmerman & Glenn R. Simpson, *Lobbyists Swarm to Stop Tough Privacy Bills in States*, WALL ST. J., Apr. 21, 2000, at A16.
[158] *Id.*
[159] *Id.* (quoting Washington Attorney General Christine Gregoire).
[160] *Id.*
[161] *Id.*
[162] *Id.;* Conrad deFiebre, *House Commerce Panel Puts Telemarketing Measure on Hold*, STAR TRIB., Apr. 19, 2000, at B5.
[163] Zimmerman & Simpson, *supra* note 157, at A16 (quoting Washington Attorney General Christine Gregoire).
[164] Glenn R. Simpson, *Financial-Privacy Legislation Expected Today*, WALL ST. J., May 4, 2000, at A2 (outlining President Clinton's proposal to label financial-privacy violations as unfair trade practices).
[165] *Id.*
[166] William Safire, *Stop Cookie-Pushers*, N.Y. TIMES, June 15, 2000.
[167] Michael Schroeder, *Groups Seek to Pre-Empt Wave of Rules to Protect Consumer-Finance Data*, WALL ST. J., Feb. 10, 2000, at A2.
[168] *Id.*
[169] *Id.*
[170] *See* JOHN DUGAN, FIN. SERVS. COORDINATING COUNCIL, THE NEW FEDERAL FINANCIAL PRIVACY LAW: A COMPREHENSIVE APROACH THAT SHOULD BE GIVEN TIME TO WORK (2000) (listing member organizations "representing America's Diversified Financial Services Community" on booklet header).
[171] *Gregoire Waters Down Her Consumer Privacy Proposal*, SEATTLE POST-INTELLIGENCER, Mar. 2, 2000.
[172] *Id.* Opponents of privacy legislation have advanced three principal arguments against the various privacy proposals. First, industry representatives argue that most people are not concerned about privacy; it is just a political or media created issue. This argument is made despite contrary public opinion polls and bi-partisan support of enhanced privacy protection.

Second, opponents argue that the various privacy proposals will chill the economy. Yet, at a hearing on a financial privacy bill in Minnesota (S.F. 3000), legislators pressed lobbyists to provide a specific example of how the privacy proposal would interfere with conducting business, but no person in the room could provide a specific

example. *See* Testimony of Subcommittee on Data Privacy of Minnesota Senate Judiciary Committee (Feb. 24, 2000).

Third, lobbyists claim that privacy is complex and thus deserves to be studied before any action is taken. To that end, Rep. Asa Hutchinson (R-Ark) recently proposed a $2.5 million dollar commission to study privacy. However, a study is unnecessary because it represents yet another excuse to delay substantive enforcement and legislative action and it duplicates what everyone knows--that companies collect a lot of information and disclose it without the consumer's knowledge or meaningful consent, and that people want real privacy protections now. *See* Minnesota Attorney General Mike Hatch, Testimony submitted to the U.S. House Subcommittee on Government Management, Information and Technology (May 15, 2000) [hereinafter Hatch].

[173] Zimmerman & Simpson, *supra* note 157, at A16.

[174] While critics of privacy legislation often point to the "democratization of credit" as a benefit to low-income and middle-income consumers, the availability of credit has also come at a cost. *See* FRED H. CATE, FIN. SERVS. COORDINATING COUNCIL, PERSONAL INFORMATION IN FINANCIAL SERVICES: THE VALUE OF A BALANCED FLOW 17 (2000) (writing in opposition to California privacy initiatives). The wide dissemination of consumer information touches upon the increasing prevalence of predatory lending practices. The subprime mortgage market has grown from $10 billion in 1993 to over $150 billion in 1998. Michael Schroeder, *Summers Calls for Legislation to Curb Predatory Lending in Mortgage Markets*, WALL ST. J., Apr. 13, 2000, at A2. Consumer organizations and HUD Secretary Andrew Cuomo are concerned that the growth in the subprime market is partially due to financial institutions pushing minorities into subprime loans when they actually qualify for the lower interest rates and fees typical of a prime loan. *Id.* Subprime loans accounted for the majority of home-loan refinancings in predominantly African-American neighborhoods in 1998, but only 9% in white neighborhoods. *Id.* African-Americans in *high-income* neighborhoods are also twice as likely to receive a subprime loan than families in *low-income* white neighborhoods. *Id. See also* Dee DePass, *Feds Likely to Target Wells Fargo's Web Site*, STAR TRIB., June 24, 2000 (alleging that bank uses information about customers' existing ZIP codes to direct them to certain other ZIP codes based on their current neighborhood's racial profile).

[175] U.S. GEN. ACCOUNTING OFFICE, IDENTITY FRAUD: INFORMATION ON PREVALENCE, COST, AND INTERNET IMPACT IS LIMITED 4 (May 1998) [hereinafter IDENTITY FRAUD]. The actual estimate of the costs of identity fraud is difficult to determine. *Id.* The IRS recently detected $137 million in fraudulent refund schemes. *Id.* The Secret Service estimates that actual losses to victimized individuals and institutions are $745 million. *Id.* Officials at VISA U.S.A., Inc. and MasterCard International estimate that it cost its member banks' $407 million in 1997. *Id.* The American Bankers Association reported that large banks had dollar losses averaging about $20 million per bank in 1996. *Id.*

[176] FED. TRADE COMM'N, IDENTITY THEFT: WHEN BAD THINGS HAPPEN TO YOUR GOOD NAME 2 (February 2000).

[177] *Id.*

[178] *Id.*

[179] Margaret Mannix, *Getting Serious About Identity Theft*, U.S. NEWS & WORLD REP., Nov. 8, 1999; Michelle Singletary, *Laws Are Failing to Keep Pace with Rate of Identity Theft*, SUN-SENTINEL, May 15, 2000, at 19. (citing California Public Interest Research Group (CALPIRG) and Privacy Rights Clearinghouse study regarding the victims of identity theft).

[180] Singletary, *supra* note 179, at 19.

[181] IDENTITY FRAUD, *supra* note 175, at 3-4.

[182] *Id.*

[183] *Id.* at 55.

[184] William Safire, *'Identity Theft' Demands Legislation*, HOUSTON CHRON., May 12, 2000, at A42.

[185] *Id.*; Singletary, *supra* note 179, at 19.

[186] IDENTITY FRAUD, *supra* note 175, at 5 (quoting representative from the Associated Credit Bureaus regarding revenue generated from sale of information).

[187] Michela, *supra* note 101, at 573-74.

[188] The AARP, Council of Better Business Bureaus' Foundation, Department of Justice, Federal Bureau of Investigation, Federal Trade Commission, National Association of Attorneys General, Security and Exchange Commission, and the U.S. Postal Inspection Service began a joint effort called the "kNOw Fraud" program. KNOW FRAUD, TELEMARKTING FRAUD: WHAT YOU NEED TO KNOW (1999) (pamphlet providing tips

consumer information). The kNOw Fraud program is designed to educate consumers about telemarketing and marketing fraud through videos and brochures. *Id.*

[189] Telemarketers may also purchase the ability to debit an individual's checking account or credit card account. Although the telemarketing firms may theoretically not possess the account numbers, in reality they have complete control over a consumer's account.

[190] The reading of a credit card number or providing written authorization symbolizes the "meeting of the minds" required by contract law. In the past, consumers would know that they are actually purchasing a product and will be billed for that product if they provide affirmative authorization. Pre-acquired account telemarketing eliminates that safeguard, and creates an environment where the consumer is at the mercy of the telemarketer.

[191] FTC ADVISORY COMM. ON ONLINE ACCESS AND SECURITY, FINAL REPORT 17 (May 15, 2000) (describing authentication of credit card purchases). The advisory committee notes that merely using an individual's maiden name, birth date, and Social Security number is a risky form of verification because they are so widely available. *Id.*

[192] Hatch, *supra* note 172.

[193] *Id.*

[194] *See* Hatch v. MemberWorks, Inc., Civ. Action No. MC99-010056 (D. Minn. Apr. 18, 2000).

[195] *Id.*

[196] *Id.*

[197] *Id.*

[198] *Id.*

[199] Federal Deposit Insurance Corporation, *Symbol of Confidence* (last modified July 27, 1999) <http://www.fdic.gov/about/learn/symbol/index.html>.

[200] *Id.*

[201] *Id.*

[202] Ed Mierzwinski, *New Bank Laws May Increase Threats to Consumers' Privacy*, U.S. PIRG, Fall 1999, at 4 ("Earlier this year, Congress had a golden opportunity to address the financial side of this [privacy] problem, as it enacted a sweeping rewrite of financial law that will allow banks, insurance companies and stock brokerages to merge with each other. Yet the law passed by Congress not only failed to better protect consumer privacy, it may have made things worse.")

[203] In the Matter of NationsSecurities and NationsBank, Admin. Proc. File No. 3-9596, Securities Act Release No. 7532, Exchange Act Release No. 39947, 67 S.E.C. Docket 143 (May 4, 1998).

[204] *Id.*

[205] *See* Mierzwinski, *supra* note 202, at 4. After the U.S. Securities and Exchange Commission (SEC) was alerted to the practice, it brought a claim against NationsBank. The SEC and NationsBank settled in 1998 for $7 million, because of a violation of investment laws. *Id.* The private class action lawsuit eventually settled for $40 million. *See* Leslie Wayne, *Privacy Matters: When Bigger Banks Aren't Better*, N.Y. TIMES, Oct. 11, 1998 (describing NationsBank case and settlement).

[206] Paul Beckett, *Comptroller Warns Banks on Practice of Giving Telemarketers Customer Data,* WALL ST. J., June 8, 1999, at A4.

[207] *Id.*

[208] Henry Gilgoff, *Private Matters: More Banks Now Selling Personal Consumer Data*, NEWSDAY, July 25, 1999 ("[T]he deals are widespread among the country's biggest banks, Hawke said in a recent interview.") A statement by a USBancorp spokesman said that the cooperative marketing programs are "common practices." *Id.*

[209] Hatch, *supra* note 172.

[210] *See* Hatch v. US Bank Nat'l Ass'n, Civ. Action No. 99-872 (D. Minn. June 9, 1999).

[211] *See* Hatch v. US Bank Nat'l Ass'n, Civ. Action No. 99-872 (D. Minn. Jan. 25, 2000). *See also* Dee DePass, *US Bank Kills Marketing Deals: But Still Plans to Fight State Lawsuit*, STAR TRIB., June 11, 1999, at D1.

[212] Marcy Gordon, *Chase Privacy Pact May Prompt Trend*, WASH. POST, Jan. 28, 2000 (stating that as many as 22 million consumers nationwide have been affected by Chase Manhattan's decision to disclose personal customer information).

[213] DePass, *supra* note 211, at D1, D4 ("Now Wells Fargo, which for three days after Hatch's suit didn't reveal details of its telemarketing relationships, said it is [suspending its relationship with telemarketers].").

[214] Gilgoff, *supra* note 208, at F07 (describing Citibank's decision to implement a moratorium on information exchanges with telemarketers).
[215] Gordon, *supra* note 212.
[216] *See* Tania Padgett, *Report Says Good Merger Targets in Short Supply*, AMER. BANKER, June 1, 2000 ("On average, the five largest players hold 73.2% market share in the 40 attractive growth markets. In 13 of the areas, deposit market share held by the top five is 80% or more.")
[217] Gilgoff, *supra* note 208, at F07 (quoting Comptroller Hawke, "Although financial conglomerates may profit from the cross-marketing opportunities and consumers may benefit from the availability of a broader array of custom-tailored products and services…there is a serious risk that these developments may come at a price to individual privacy.")
[218] Beckett, *supra* note 206, at A4. In 1997, the OCC logged 16,000 consumer complaints. *Id.* In 1998, the number of complaints rose to more than 68,000 and in 1999 it reached over 100,000. *Id.*
[219] Jeff Leeds, *Bank Sold Credit Card Data to Felon*, L.A. TIMES, Sept. 11, 1999.
[220] *Id.*
[221] *Id.*
[222] *Id.*
[223] *Id.*
[224] In articles and testimony in front of legislators, opponents have claimed that privacy legislation will raise the price of financial services, reduce the availability of credit, and interfere with a person's ability to make purchases with a check. *See* CATE, *supra* note 174, at 17 (claiming severe economic hardship). They fail to mention that the State of South Dakota has had an "opt in" law for banks for over 15 years and has experienced no difficulty with the system.
[225] Hatch, *supra* note 172.
[226] *Id.*
[227] William Safire, *America Hasn't Gone Far Enough to Protect Privacy Rights*, STAR TRIB., Sept. 26, 1999.
[228] William J. Fenrich, *Common Law Protection of Individuals' Rights in Personal Information*, 65 FORDHAM L. REV. 951, 963 (1996) ("[S]ecrecy surrounding how personal consumer information is used limits the potential for consumer action…")
[229] *Id.*
[230] Barbara A. Rehm, *B of A Chief: Privacy Shields Harm Customers*, AMER. BANKER, May 3, 2000. *See also* Richard A. Barton, Testimony at the Financial Privacy Hearings before the Subcommittee on Financial Institutions and Consumer Credit of the Committee on Banking and Financial Services, 106th Cong., 1st Sess. (July 21, 1999) (stating that less than three percent of the U.S. population utilizes the Direct Marketing Association's opt-out system).
[231] Robert O'Harrow, Jr., *Data Firms Getting Too Personal?*, WASH. POST, Mar. 8, 1998, at AO1.
[232] William Safire, *Stop Cookie-Pushers*, N.Y. TIMES, June 15, 2000 ("The word choice is used by banks, hospitals, and Internet companies to conceal their intrusions into the personal lives of their consumers.")
[233] Sovern, *supra* note 109, at 1104-05.
[234] Robert K. Heady, *Don't Let Anyone Sell Your Privacy,* PIONEER PRESS, Oct. 3, 1999.
[235] David J. Klein, *Keeping Business Out of the Bedroom: Protecting Personal Privacy Interests from the Retail World*, 15 MARSHALL J. COMPUTER & INFO. L. 391, 398 (1997).
[236] Sovern, *supra* note 109, at 1075.
[237] Peter Bowal, *Reluctance to Regulate: The Case of Negative Option Marketing*, 36 AM. BUS. L. J. 377, 384 (1999); Dennis D. Lamont, *Negative Option Offers and Consumer Service Contracts: A Principled Reconciliation of Commerce and Consumer Protection*, 42 UCLA L. REV. 1315, 1330 (1995).
[238] Bowal, *supra* note 237, at 378.
[239] FRED H. CATE, PRIVACY IN THE INFORMATION AGE 21 (1997).
[240] SENATE, *supra* note 116, at 12.
[241] Bowal, *supra* note 237, at 389.
[242] Lamont, *supra* note 237, at 1350.
[243] *Id.*
[244] *Id.* at 1351.
[245] Safire, *supra* note 232.

[246] An opt-in system does not mean that information may never be shared, it only means that there should be consent. Once there is consent, then a commercial interest can share information pursuant to that consent. An opt-in also has the beneficial effect of providing a business with a list of individuals who are actually interested in what is being sold.
[247] Deron H. Brown, Book Note, *Privacy in the Information Age by Fred H. Cate*, 22 Thomas Jefferson L. Rev. 251, 254 (2000).
[248] *Id.*
[249] Cost is always an issue that is raised with an opt-in system, but these concerns are unwarranted. The picture drawn by most industry representatives is a mailbox filled with hundreds of notices asking an individual to consent to the sharing of their information. This picture is incorrect for two reasons. First, a well-crafted opt-in will not require consent for every transaction. Individuals will be asked once, and if they grant permission then the consent will last for a specific period of time. Second, an opt-in will only apply if the commercial entity wants to go beyond the scope of a consumer's reasonable expectations. If a bank or retailer does not share information with non-related affiliates or third parties, then no consent is required.
[250] Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2406-08 (1996).
[251] *Id.*
[252] *Id.*
[253] *Id.*
[254] Carol Patton, *Weaving your E-mail Marketing Web: Mass Mailing Done Right Can Be Golden, but Done Wrong, It's Just Spam*, CRAIN'S DETROIT BUS., June 12, 2000, at E1.
[255] *Id.*
[256] *Id.*
[257] *Internet Marketers Vote In Favor of Opt-In Email: NetCreations Inc. Sponsors Key Internet Marketing Surveys*, BUS. WIRE, Mar. 9, 2000.
[258] *Id.*
[259] *Id.* ("The second poll, an informal survey of attendees taken at the Direct Marketing Association's (DMA) Internet marketing show in Seattle last week, also found that marketers overwhelmingly favored opt-in email marketing services as the right means to reach consumers.") At the same marketing show, the DMA's own Association for Interactive Media publicly stated its preference for "opt out" as the industry's best practices for email marketing despite the opinions of its members and evidence to the contrary. *Id.*