Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?

Sandra Byrd Petersen(1)

The chilling effect of [the] loss of privacy is an undesirable incentive to conform to societal norms rather than assert one's individuality. Ultimately, what is lost is not only the private emotional releases we all need but, most importantly, the creativity that leads to human achievement.

Privacy makes possible individuality, and thus, freedom. It allows us to cope with the larger world, knowing there is a place where we can be by ourselves, doing as we please without recrimination.

—Robert S. Peck(1)

Introduction

As society becomes increasingly automated, individual privacy is threatened in ways unimaginable only a few years ago. The pervasive use of computers has enhanced society's ability to collect, store, retrieve, process, and disseminate data on individuals, quite often without the individual's knowledge or consent. Privacy laws in the United States have not kept pace with the technological developments of the past twenty years. In fact, virtually nothing to protects individuals from having their private lives peered into via computer. This Note addresses the threat to individual privacy inherent in the collection, processing, and dissemination of personal information by private sector organizations and individuals. This Note does not examine in-depth the regulation and control of government collection and use of personal data,(2) nor does it survey currently existing constitutional privacy rights such as those recognized in *Griswold v. Connecticut*(3) and *Roe v. Wade*.(4) Specifically, this Note examines the legal use of personal information often collected, compiled, and disseminated by private individuals or entities, without the consent or knowledge of the person the information concerns.

Information privacy is the right to control how information about oneself is used by those to whom it is disclosed. Congress needs to create a right to information privacy. Current protections are either inadequate or simply nonexistent. Neither the courts nor the legislatures have addressed the recent uses of technology that invade personal privacy. Regulations control governmental use of personal information,(5) but very little legislation has been enacted to address the use of personal information by the private sector.(6) Comprehensive federal legislation is necessary to curb the abusive collection and use of personal information. Acknowledgement of constitutional protections would be ineffective as any such protection would only apply against the government and currently, the greatest threat to personal privacy exists in the private sector. Current tort law is unhelpful, as courts have thus far been reluctant to recognize an invasion of privacy cause of action that includes dissemination of individual data without consent.(7) This problem exists partially because the legal system has been unable to develop a coherent and widely accepted definition of privacy. Furthermore, since the publication of Dean William L. Prosser's framework for privacy torts in 1960,(8) the legal community has accepted the fact that four distinct privacy torts exist, and an information privacy tort does not fit neatly within any of those preexisting frameworks.

Aside from the definitional difficulties encountered by a common law tort remedy for a violation of information privacy, a purely logistical concern exists in adopting a common law remedy. It takes years for a single case to move through the court system to establish a precedent upon which lower courts can rely. Furthermore, the various circuit courts have differing views on privacy. Therefore, a uniform rule governing information privacy would not develop for some time. Technology is changing too rapidly for the court system to develop effective parameters within which information brokers are able to operate.

Furthermore, contractual solutions alone are inadequate to deal with the invasion of privacy experienced when personal information is disseminated without consent. Legislative reactions to date have been inadequate. This demonstrates the need for uniform legislation which controls the collection and dissemination of information, the acquisition of individual consent before the dissemination of information, and damages which may be assessed against violators.

The right to information privacy has not been recognized within the protections afforded by the United States

Constitution. However, an express right to privacy exists in a number of state constitutions.(9) Yet, even if the right to information privacy were expressly recognized in the federal constitution, as well as in all state constitutions, the right would only limit the actions of government, not private actors. Similarly, tort law is ill-equipped to deal with the invasion into people's lives brought on by the vast collection and dissemination of personal information. Invasion of privacy torts have not been interpreted to include a right to information privacy. Likewise, contractual provisions alone do not provide an adequate remedy, because they necessarily leave the burden of deciding whether to disclose information on the individual instead of on the information broker, where it belongs. Finally, legislative action to date has been sparse and diffuse, addressing only immediate concerns and failing to focus on the effect that dissemination of personal information has on society.

Part I of this Note will examine what is meant by information privacy and how personal information is currently used by people other than those to whom it was disclosed. Next, Part II will discuss whether a current right to information privacy exists. Part III assesses whether current law—constitutional, tort, contractual, and legislative—is adequate to deal with invasions into personal privacy. Finally, Part IV proposes solutions which will afford the same level of protection to all who are affected by the invasion of information privacy.

I.Information Privacy

Imagine the horror Mallory Hughes of Florida experienced when he received the following letter from evangelist Oral Roberts, with whom Mr. Hughes had no previous contact:

Mallory, I am your Partner and your friend, and because I am so close to you in spirit, I feel I can say something very personal to you. . . . Mallory, it's time for you to get out from under a load of debt, that financial bondage that . . . makes you feel like you have nowhere to turn. The devil tells you, "You've made your bed of debt, now you've got to lie in it. You're going to be paying on your bills for the rest of your life. . . . You're doomed with debt!"

Mallory, does the horror of these thoughts keep you awake at night? The burden, oh the burden, sometimes is too much to bear. . . . If you could just suddenly receive a big lump sum of money, all your problems would be over.

Well Mallory, I don't have a magical answer for your pile of bills and financial bondage. But I do have a miraculous answer, direct from the throne of God to your home.(10)

The letter went on to encourage Mr. Hughes to send $100 to Oral Roberts so he could intercede with God on Mr. Hughes's behalf.(11) Oral Roberts purchased Mr. Hughes's name from a databank that targets those suspected of being in financial difficulty. Although Mr. Hughes was admittedly in a financial bind, he was understandably upset that a perfect stranger was able to peer into his private life.

Margaret Davis of Burbank, California had a similar experience. Upon discovering she was pregnant, Ms. Davis ordered a maternity catalog. Shortly thereafter she began receiving more catalogs, free baby-related product samples, and offers to purchase baby-related services. Unfortunately, Ms. Davis had a miscarriage. However, the barrage of information and solicitations did not end. Despite her efforts to contact the solicitors by phone and letter, she continued to be inundated with mail and offers she did not want. She received phone calls close to the time her baby would have been due congratulating her on her new arrival, and she received birthday cards for the following few years. This experience was so upsetting for Ms. Davis that her husband had to open all the mail received by the couple and screen all phone calls.(12)

Such stories are abundant in modern society. Almost all business organizations of every conceivable size have some type of automated data system. Information that was formerly kept on paper and stored in filing cabinets is now stored in computers. This means that the most intimate, personal information about nearly every American adult is now recorded and preserved digitally. Add to this the fact that every time a consumer writes a check, uses a credit card, presents a grocery store check-cashing card, makes an ATM transaction, fills out a warranty card, applies for a loan, calls an 800- or 900-number, or engages in any other activity that leaves a data trail, the consumer reveals personal information which is permanently stored in computerized databanks. Almost any decent hacker with a computer, modem, and telephone can access the computerized record of this information.(13) Armed with as little information as an individual's Social Security number, address, or checking account number, a total stranger can access the vast

amount of personal information stored in computerized databanks.(14)

A. The Risk Involved

The threat from the collection of personal information used to be relatively innocuous. Prior to the technological revolution, it was relatively impossible for any one individual or organization to collect information from the many places it existed. However, the advent of the computer has made it both inexpensive and easy for anyone with a minimum amount of computer knowledge to compile information from many different sources. With the assistance of computer-matching programs, information can be gathered from many different sources, run through a computer, and assembled moments later into a complete and detailed personal dossier on virtually any individual. An individual or organization need only contact one of many companies specializing in compiling databases to obtain personal information.(15) Information can also be obtained by directly subscribing to the services offered by credit bureaus. For a fee, usually between $400 and $500, those with an appropriate need may obtain a password which allows access via personal computers to the vast amount of information collected and compiled by credit bureaus.(16) Then, by using matching software, the computer user is able to compile information gained from different sources and construct detailed and complete personal dossiers on individuals without their knowledge or consent.

Computerized information compiled in such dossiers is accessed by everyone from businesses' private investigators, insurance companies, employers, landlords, and doctors. As technology becomes more sophisticated, it becomes easier to detail the lives of individuals—their location at any given moment, what type of groceries they purchased, what books and magazines they read, where and with whom they travel, and whether they have ever sued a doctor or filed a worker's compensation claim. Virtually every activity in every person's life will be recorded in the near future.

Currently, most people are unaware of the type and amount of information collected about them. For example, grocery stores are now able to collect information about which items individuals purchase and the frequency with which consumers shop.(17) If customers use grocery store check-cashing cards, credit cards, or virtually any other cashless method of payment, the store then has a record of the customers and what they purchased. This information can then be used to target coupon or other promotional mailings to the customers.(18) This in itself seems relatively harmless, however, the information is used for other purposes. Insurance companies can purchase this information on a potential insured to determine a person's dietary habits—whether the person purchases red meat, cigarettes, or alcohol—to determine if the insured may be a greater risk to the company. An insurance company can combine this information with medical records that can be obtained from the Medical Information Bureau (MIB)(19) which has data on 15 million people.(20) The result is a very complete picture of a person's lifestyle, regardless of whether or not the information is accurate. Furthermore, although the information collected concerns some of the most intimate details of personal life, individuals may be unaware of its availability to the public and, therefore, unable to correct, any misinformation contained in these records.(21)

The majority of this information is contained in the databases of credit reporting agencies.(22) TRW, Equifax, and Trans Union, the three largest, reportedly have 500 million records on an estimated 160 million people.(23) It is estimated that information on each of the 160 million people is transmitted between computers an average of five times a day.(24) Federal and local governments are the largest gatherers of information in the country. The United States government reportedly has an average of fifteen files on every American.(25) In total, this adds up to approximately five billion records that describe the personal lives of Americans.(26) Although errors abound in computerized data,(27) the mere fact that the information is computerized makes it appear more authoritative and the results are rarely, if ever, questioned by those using it.(28) Furthermore, because of the relatively minor cost of storing information on a computer disc, information is kept much longer than its useful life. Therefore, important decisions may be made based on outdated, if not inaccurate, information.(29)

B. The Effect of the National Information Infrastructure on Information Privacy

The collection and exchange of information will become even easier and more pervasive if the Clinton Administration's vision of the National Information Infrastructure (NII) comes to fruition.(30) The Clinton Administration, through the National Telecommunications and Information Administration's (NTIA) *Agenda for*

Action, has called for the connection of the nation's businesses, residences, and schools with advanced high-speed networks.(31) Although the Adminstration realizes that in order for the NII to succeed it must be trustworthy and secure,(32) there is no mention of how this security should be accomplished. In fact, the *Agenda for Action* calls for "[a]pplications and software that allow users to access, manipulate, organize, and digest the proliferating mass of information that the NII's facilities will put at their fingertips,"(33) and further imagines a network that is "sufficiently `open' and interactive so that users can . . . exchange information among themselves."(34) The NTIA has called for comments regarding the privacy issues relating to private-sector use of personal information which is associated with the NII,(35) but no record of these comments has yet been published.

II.The Right to Information Privacy

Is there a right to information privacy? In light of the current lack of legislation in this area, the answer to this question is a resounding "no." One reason that society has not explicitly recognized a fundamental right to privacy is the failure, or inability, to coherently define this right. In 1890, Samuel Warren and Louis Brandeis defined privacy simply as "the right to be let alone."(36) Since the publication of Warren and Brandeis's seminal article on privacy, the right to privacy has been defined in many different ways. Privacy has been described as "encompass[ing] concerns about fair and reasonable information practices as well as confidentiality,"(37) and as the ability of "individuals and organizations . . . to determine for themselves what they want to keep private and what they want—or need—to reveal."(38) Additionally, privacy has been found to encompass "the unitary concept of separation of self from society,"(39) "the right to control the flow of information about oneself,"(40) and the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."(41) Because a single definition or concept of privacy has not evolved, it is difficult to determine exactly when the right to privacy has been violated.

Information privacy is a subset of the larger concept of privacy. Generally, personal information is originally gathered for a legitimate purpose, such as processing a loan or credit card application, filling out a warranty card, or applying for health or life insurance. However, once this information is collected, it is frequently sold to others for mailing lists or marketing schemes, to employers who use the information to make employment decisions, to insurance companies for use in determining whether an applicant is a good risk, and to landlords who want to know if a potential tenant has damaged past rentals or paid the rent on time. Even pro-life and fundamentalist Christian organizations and pro-choice groups send mailings to consumers who have recently purchased home pregnancy tests to discourage potential abortions.(42) Until society determines that our individual right to privacy outweighs the needs of businesses and others to pry into personal lives without consent, the lack of information privacy will continue to be a problem.

III.Current Protections

A. Constitutional Protections

The phrase "right to privacy" is almost invariably mentioned in tandem with the phrase "constitutional right." However, the term "right to privacy" does not appear anywhere in the United States Constitution. The United States Supreme Court has found that the right to privacy emanates from the penumbras of the articles of the Bill of Rights in certain circumstances.(43) In 1977, the Supreme Court handed down its decision in *Whalen v. Roe*(44), which held that medical patients' rights to privacy were outweighed by the government's need to publish their names in a database that contained information on persons who had been legally prescribed narcotics. (45)The Court determined that a state had a legitimate interest in the collection of the information and that the collection of the data did not "establish an invasion of any right or liberty protected by the Fourteenth Amendment."(46)

However, in dicta, the majority stated that it was "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks."(47) The majority further stated that it understood that much of the information collected is "personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures."(48) The Court then concluded that while sometimes the duty to avoid disclosures arises from the Constitution, it was not deciding a "question which might be presented by the

unwarranted disclosure of accumulated private data whether intentional or unintentional or by a system that did not contain comparable security provisions."(49)

In his concurrence, Justice Brennan made clear that the *Whalen v. Roe* decision was based on the fact that the reporting system was a legitimate state interest and that the system contained appropriate safeguards against unauthorized disclosures. He further expressed his concerns that "[t]he central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and [he was] not prepared to say that future developments will not demonstrate the necessity of some curb on such technology."(50) Despite Justice Brennan's explicit recognition that changing technology may necessitate a reexamination of this issue by the Court, this issue has not surfaced for reconsideration.

Critics of a right to information privacy have raised the First Amendment as a potential defense against any declaration of a constitutional right to information privacy.(51) These critics usually include businesses engaged in the sale of personal information, and marketers who find the detailed information available about individuals a valuable tool in promoting and selling their products.(52) They argue that the First Amendment's guarantee of free speech is superior to any information privacy rights of the data subject. Those with an interest in the for-profit dissemination of personal information have a legitimate First Amendment right in free speech. However, the Court has held that speech which does nothing more than propose a commercial transaction has a lower value and can be, therefore, subject to regulation.(53) The Supreme Court has held that commercial speech rights are in a "subordinate position in the scale of First Amendment values"(54) and that commercial speech is less likely to be deterred by regulation than core political speech.(55)

In fact, it has been determined that credit reports do not address a public concern and are, therefore, not protected by the First Amendment. The U.S. Supreme Court held, in a plurality opinion, that in order for commercial speech to be afforded full protection under the First Amendment, it must address a matter of public concern, and the "petitioner's credit report concerns no public issue. It was speech solely in the individual interest of the speaker and its specific business audience."(56) In this case, Dun & Bradstreet released an incorrect credit report to a client. Based on this report, the client denied credit to Greenmoss Builders. The report stated that Greenmoss had filed bankruptcy, which was untrue. Thus, the Supreme Court, in holding that credit reports are not the subject of public controversy, established a basis upon which to protect the privacy of purely private information of no public concern.

The Constitution does not provide a basis to protect information privacy because it applies only to the actions of the U.S. government and to actions of state governments as incorporated through the Fourteenth Amendment. It has no force with respect to actions of private actors. Therefore, use of constitutional principles—although theoretically feasible—would not solve the problem of what to do when a private individual or organization has collected and disseminated personal information about an individual without that individual's knowledge or consent.

Many states have expressly recognized the right to privacy in their state constitutions.(57) Others have recognized the right to privacy in conjunction with the right within the home to be free from unreasonable searches and seizures,(58) similar to the rights guaranteed by the Fourth Amendment of the U.S. Constitution. California has recognized a privacy right that exceeds the right to privacy recognized under the Constitution of the United States.(59) The legislative declaration and findings of this amendment state that:

The right to privacy is a personal and fundamental right . . . and that all individuals have a right of privacy in information pertaining to them. The legislature further makes the following findings:

(a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies.

(b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.

(c) In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits.(60)

In 1976, a California appellate court held that "[p]rivacy is protected not merely against state action; it is considered an inalienable right which may not be violated by anyone."(61) In so holding, the California courts took a step the U. S. Supreme Court has not taken—holding private actors to a constitutional standard of behavior.

B. Common-Law Protections

In 1960, Dean William L. Prosser classified the common-law tort of invasion of privacy as "four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff . . . `to be let alone.'"(62) Since the publication of the Warren and Brandeis article in 1890, Dean Prosser stated that he was not trying to define the four privacy torts but contended that all the judicial decisions of the past forty years fit into one of the four categories he discussed.(63)

The first of these four torts is "[p]ublicity which places the plaintiff in a false light in the public eye."(64) The second tort was defined as "[i]ntrusion upon the plaintiff's seclusion or solitude, or into his private affairs."(65) Third, Prosser identified "[p]ublic disclosure of embarrassing private facts about the plaintiff."(66) He categorized the fourth tort as, "[a]ppropriation, for the defendant's advantage, of the plaintiff's name or likeness."(67) Plaintiffs have had little or no success bringing actions under this scheme of privacy torts when the invasion is one of information privacy. However, these torts are defined broadly enough that courts could expand their application of them to the information privacy arena.

In terms of information privacy, publicly placing a person in a false light is the least helpful of the four Prosser torts, because the information published about the individual be untrue. Furthermore, the publisher must recklessly disregard the matter's untruthfulness.(68) Generally speaking, the information that is bought and sold among information brokers does not fit this pattern. The information is generally true or at least believed to be true. Therefore, this tort is not applicable in the context of information privacy.

"Intrusion upon a person's seclusion or solitude" is unhelpful as well. This tort requires an unreasonable intrusion into an area in which one has a reasonable expectation of being undisturbed.(69) Unauthorized dissemination of personal information arguably intrudes into the solitude or private affairs of the data subject. However, the historical application of this tort presents two major problems in the context of information privacy. First, the intrusion must be highly offensive to the reasonable person.(70) Because information privacy is a personal matter, what may greatly offend one person may be welcomed by another. Further, the *Restatement* concludes that there is no liability for the examination of a public record. The invasion must be of "a private seclusion that the plaintiff has thrown about his person or affairs."(71) Second, this tort has traditionally applied to physical intrusions and is used to fill the gaps left by trespass law.(72) Meeting the requirement of intrusion into private seclusion is a difficult test for those complaining of an invasion of information privacy since the disseminated information was once freely given by the data subject.

The tort of public disclosure of private facts seems, at least from the standpoint of its title, to be exactly what is needed to protect against the intrusion of information privacy. The *Restatement* defines this tort as the dissemination of information that "would be highly offensive to a reasonable person, and is not of legitimate concern to the public."(73) However, this definition poses two significant problems for information privacy. First, the information must be disseminated to the public at large. This means that dissemination of information to one or a few persons is not actionable. Second, this tort applies only to a public disclosure that would be highly offensive to the reasonable person. Offensiveness is determined in relation to "the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbors and fellow citizens."(74) Unfortunately, the custom of our times is that it is acceptable to disseminate information about individuals without their consent. This is probably due to a lack of knowledge on the part of the vast majority of the American population as to what type of information is sold and for what purposes it is used.

The proliferation of information sold to others on the grand scale currently seen, however, may satisfy the first element of this tort. An information brokers who sells the collected personal information to a large number of persons may well violate this tort. The problem then becomes one of how many people need to access the information to satisfy this

element. If this element can be satisfied, and society in general becomes aware of, and offended by, the large scale on which confidential information is bought and sold, this tort could find new life as the protector of information privacy.

Appropriation of name or likeness may be the most useful of Prosser's four torts. The *Restatement* indicates that the interest contemplated here is "of the individual in the exclusive use of his own identity."(75) This is exactly what is being invaded by persons or entities who gather and transmit data on any given individual. This information is disseminated not to satisfy people's curiosity but to develop a personality or character profile of a certain individual. The information can be used to predict future behavior, grant or deny a benefit, send targeted mailings, or for any other number of reasons that are tied directly to the individual's behavioral characteristics.

Unfortunately, this tort traditionally has been applied almost exclusively to cases of advertising where a public figure's name or likeness has been used to sell a product or service that directly benefits the defendant without the consent of the public figure.(76) This tort recognizes that public figures have an interest similar to a property right in their names or likenesses. When information is disseminated about an individual, a third party profits from that individual's personal property. By recognizing that all individuals, not just public figures, have a property interest in their names or likenesses, this tort easily could be expanded to include the invasion of privacy through the dissemination of personal information.(77)

Applying these torts in the context of information privacy poses two problems. First, none of them traditionally has been viewed in terms of information privacy. There is a common attitude that an individual should not object to the dissemination of personal information unless there is something to hide. However, it is not the content of the information that is offensive but the fact that the information pertaining to an individual is disseminated without permission, and that someone else profits from the sale of that information. However, unless the data subject can demonstrate monetary damage as a result of the dissemination of personal information without consent, there may be no remedy for that injury. Furthermore, the personal distaste or anguish experienced by those whose privacy has been invaded may not be severe enough to recover pain and suffering damages under the common-law torts.

Second, since Dean Prosser wrote his article in 1960, there has been virtually no change to the common-law privacy torts. If a tort does not fit neatly within one of the four delineated causes of action, the plaintiff is unable to recover damages. Obviously, the law has not kept pace with the changing technology and values of modern times.

An alternative to the Prosser torts is recognition of a tort defined as commercial dissemination of private facts.(78) This tort would create liability for the transfer of information between business entities in certain situations that the courts deem appropriate.(79) The most likely scenario would be the unauthorized transfer of information. Jonathan Graham, the commentator who proposed this solution, left it to the courts to determine the quality of the information transferred.(80) However, his premise is flawed because, regardless of the amount or quality of information transferred, the decision to distribute personal information should always rest with the individual concerned. If this fact were recognized, the tort would provide a possible solution to the information privacy problem.

However, the biggest barrier to using the common law to address the problem of information privacy is not how or whether an information privacy tort is defined; it is the average amount of time it takes a lawsuit to proceed through the court system. This is an almost insurmountable barrier to the use of the common law as a tool for change in recognizing the tort of information privacy. Furthermore, if the common law were to be used as the sole mechanism for change, any solution would most likely become outdated before it was even reported. Moreover, cases that settle out of court and those that are not appealed would further hamper the efficacy of this solution since no precedent would be established upon which other courts could rely.

C. Contractual Protections

It has been argued that the problem of information privacy can be solved by allowing individuals to contract with those to whom they provide information as to what, if any, information the individual wants disseminated.(81) This approach entails providing "an opt-in or opt-out clause"(82) which indicates to the data gatherer whether or not the data subject wants information already disclosed to be disseminated in the future. The penalty for failing to provide this option

clause would correspond to the prevailing expectations of privacy in that industry. This would be determined by the dollar amount individuals attach to their privacy under certain circumstances.(83) This premise largely rests on the assumption that the only danger of dissemination of information comes from the information contained in credit bureau databanks.(84)

This assumption fails to recognize the existence and use of the vast number of databanks kept by people and organizations other than credit bureaus. This solution overlooks the fact that businesses are formed with the sole purpose of collecting data from various sources and compiling it into detailed personal dossiers. These businesses then sell this information to others who use it for vastly different reasons than those for which it was originally collected.(85)

This premise is further flawed because it assumes that the "information market" functions rationally from an economic standpoint. It assumes that those with favorable credit ratings want their credit reports disseminated to businesses or individuals with which they are not anticipating doing business. Individuals who receive stacks of junkmail and follow-up phone calls on a daily basis would probably disagree with this assumption. This premise assumes that these individuals should want this kind of attention because it makes credit cheaper and prices lower.(86) Aside from the fact that most people find this sort of "attention" annoying, this premise is flawed.

Dissemination of personal information without consent does not make credit cheaper or prices lower. Individuals with sound credit histories will still receive inexpensive financing when they want it. Credit reporting agencies serve a valuable function in society, and personal information needs to be accessible to creditors to insure they are lending to those most likely to pay them back. However, they should not be allowed to disseminate information about individuals without written consent. The information the creditor receives on the debtor would be just as accurate and beneficial to both parties if it were not obtained until the debtor wanted the creditor to obtain it. The accuracy and value of this information are not increased as a result of obtaining it prior to any indication that the debtor is interested in doing business with the creditor.

The contractual solution to the problem of information privacy could work in conjunction with federal legislation setting a minimum standard of privacy for all individuals and all information. Once legislation has been passed, and a minimum standard of privacy has been set, an individual can then contract away unwanted protection. This puts the burden on the person or organization who wants to sell the information to receive consent before doing so, rather than burdening the data subject with the task of tracking down all personal information collected and trying to stop its dissemination.

D. Statutory Protections

Thus far, legislative action regarding information privacy has been inadequate. This is partially because legislative responses have been reactive instead of proactive, and because of the existence of strong groups lobbying on behalf of businesses and credit reporting agencies. The first reaction of federal legislators to governmental abuse of information was the Privacy Act of 1974.(87) This Act was passed in response to the Nixon Administration's use of political opponents' tax information. However, this legislation restricts only the federal government's actions as to the information it collects. It has no effect on private individuals.

Congress next took action in this arena in 1978. The Right to Financial Privacy Act(88) was enacted as a reaction to the Supreme Court's decision in *United States v. Miller*.(89) *Miller* held that a bank depositor has no legitimate expectation of privacy in the contents of checks and deposit slips held by a financial institution. It held that there can be no such expectation without possession or ownership.(90) The Financial Privacy Act restricts governmental access to information contained in financial records of customers of financial institutions without the consent of the customer or proof of an appropriate subpoena, summons, or search warrant in which the financial records in question must be reasonably described.(91) Congress further mandated that any information transferred must be for law enforcement purposes, and the individual must be informed of any such disclosures.(92)

The first attempt by Congress to control the actions of private entities was the Fair Credit Reporting Act of 1970.(93)

This Act responded to perceived abuses of the credit reporting industry. Congress recognized that credit reporting bureaus had "to exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy."(94) The legislation allows credit reporting agencies to release information to those (1) it believes intend "to use the information in connection with a credit transaction involving the consumer on whom the information is to be furnished . . . or otherwise has a legitimate business need for the information in connection with a business transaction involving the consumer," or (2) for employment, insurance, or government benefits issued on the basis of financial status.(95) This broad definition of who is entitled to receive information regarding consumers almost negates the reason for the law in the first place. Virtually anyone can, and has, fit through the broad loophole of "legitimate business need." Therefore, the category of those eligible to receive the information collected by credit agencies is almost limitless.

Congress again acted to protect individual privacy rights in 1988 when it passed the Video Privacy Protection Act.(96) This legislation was passed in response to the Senate confirmation hearings of Supreme Court Justice nominee Robert Bork. This Act restricts the release of information or public dissemination regarding the videos individuals rent.(97) During Judge Bork's confirmation hearings, records of his recent video rentals were obtained and released to the media. Fortunately for Judge Bork, his taste in movies was not socially stigmatic, namely Westerns and family films. However, if controversial titles had been revealed—for example pornography—the situation could have been quite embarrassing for Judge Bork. A similar provision is included in the Cable Communications Policy Act,(98) which prohibits the dissemination of information regarding the viewing habits of cable television subscribers.

The most recent congressional response is the Driver's Privacy Protection Act of 1994.(99) This provision, which was sponsored by Sen. Barbara Boxer (D-Cal.) of California, limits the access and dissemination of records held by a state's department of motor vehicles (DMV). This legislation was passed in response to the murder of actress Rebecca Schaeffer in 1989. Ms. Schaeffer was killed by an obsessed fan who obtained her address from a private investigator, who gained access to her address through her DMV records. The problem with this legislation is that it contains many loopholes. These include an exemption for private investigators, such as the one who obtained Ms. Scheaffer's address, as well as a general provision allowing DMVs to disclose information to outside entities provided drivers are given clear and conspicuous notice of possible disclosures on license renewal forms, vehicle registrations and titles, and identification cards.(100)

Legislative responses to the Bork confirmation hearings and the Schaeffer murder are unfortunately typical. When evidence of a large problem arises, Congress commonly reacts with the quickest possible remedy. Therefore, instead of taking the opportunity to examine the entire issue of information privacy, Congress has looked only to the problem immediately facing it. This has resulted in solutions that are far too shortsighted and reactionary.

State reaction to the problems posed by the burgeoning use and misuse of computer technology has been equally diffuse. A few states have passed a variety of laws but no state has passed comprehensive legislation to curb the abuse of the invasion of information privacy. In general, states have reacted by enacting legislation that deals broadly with the regulation of credit bureaus,(101) information collected by insurance companies,(102) library and video records,(103) communications,(104) and other transmission of personal data.(105)

However, because the problem of regulating the dissemination of information is a national one, the most effective response will have to come from the Congress. If Congress is slow to act in this area, states can fill the gap by passing legislation protecting the rights of their citizens against the intrusions of information sellers. The fact that the largest dealers of information conduct business on a nationwide basis will force them to adopt the safeguards of the state with the most protective mandates to insure that they do not violate anyone's rights.

IV.Solutions to the Problem

Congress needs to act. Ironically, those who have opposed federal legislation the most are those who have the most to lose if no federal legislation is enacted. American businesses stand to lose the ability to transfer data across foreign borders if appropriate federal legislation is not enacted. The European Union Council of Ministers adopted the Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.(106) This directive places special conditions on the transfer of data to nonmember states that do not

adequately protect personal information.(107) United States businesses stand to lose a great deal of business because this directive was enacted. This fact, along with the fact that individual privacy and autonomy are greatly valued by most Americans, necessitate federal legislation that protects every citizen's right to information privacy.

Some commentators have suggested legislative amendments to existing federal laws such as the Privacy Act and the Fair Credit Reporting Act.(108) However, amending these pieces of legislation will not provide the appropriate level of protection to insure against unnecessary dissemination of personal information. Existing federal legislation already has many loopholes; these increase the chance that courts would then interpret any amendments with the same deference the legislation has been given in the past. More drastic, comprehensive solutions are necessary.

Any legislation enacted must give control over personal information to the individual. The new legislation should only permit the collection of information which is needed for the particular situation. For example, loan and credit card applications should only ask for information that is relevant and necessary to process that application. Extraneous questions must be deleted. This does not mean that individuals cannot consent to offer additional information if they so choose. However, this should be done only after a full and informed disclosure of the inquirer's intentions and cannot be a condition of doing business with any organization.

Additionally, restrictions need to be imposed upon the permissible dissemination of information after it has been collected. Dissemination should not be allowed without the data subject's consent. Before consent is given, the individual should be told exactly who will receive the information and how it will be used. Furthermore, consent forms should not resemble forms that are commonly used today. Often, insurance companies use consent forms that never expire and give the same force and effect to photocopies of the form as to the original form. Therefore, insurance companies are able to use the same release forms year after year for as many information disclosures as they deem necessary simply by having the individual sign one release. This allows insurance companies and others who follow the same practice to access information that the data subject might not have consented to if these companies were required to obtain a new consent form each time information is requested. Alternatively, consent forms should expire after one year. Current practices allow these organizations to access information for years after the data subject has signed the form, possibly obtaining information even after the data subject terminates the use of the company's services.

Further restrictions should be implemented regarding the time period that information can be retained on an individual. Since it is often cheaper for organizations to keep information than to dispose of it, the tendency has been to continue to disseminate old data about individuals. This practice encourages reliance on information that is outdated and often no longer an accurate indication of the individual it describes. Congress needs to impose regulations on collectors of data that require all information that is kept on an individual to be disposed of after a specified number of years. The specific number of years should vary depending on the information at issue. For instance, typical credit information such as payment history and amount of debt should be restricted to a retention period of five years, while information regarding bankruptcy or criminal embezzlement charges would have a longer retention period. This allows individuals who have made mistakes in the past to correct these mistakes instead of being continually haunted by them.

Finally, Congress needs to implement stiff penalties for violation of the legislation it enacts. Compensatory and punitive damages should be imposed for collection of unnecessary information, nonconsensual dissemination, dissemination of outdated and inaccurate information, and dissemination of purposefully falisfied information. Monetary penalties will be most effective, because individuals and organizations in the information brokerage business sell personal information for profit. Therefore, the only way to curb abuses is to make unscrupulous business practices unprofitable.

By enacting legislation, Congress would set a minimum standard of conduct for information brokers. The courts would then fine tune the details. This will be especially necessary if individuals are able to contract away their rights to information privacy.(109) A statutory minimum amount of protection and a recognition of the individual's ability to contractually waive these rights will result in more informed, better educated consumers. Consumers will finally understand the pervasiveness of the collection and dissemination of personal information. Furthermore, this solution would put the power over personal information into the hands of the individual to whom it pertains instead of in the hands of powerful information brokers. Allowing individuals to contract away their legislatively given rights will

permit those individuals that are "flattered" by the attention they receive from unsolicited business to continue to receive this information. It will also allow individuals who may be interested in receiving only certain types of information to contract to receive the information in which they are interested. Most importantly, this solution allows those individuals who would rather be left alone to do so, sacrificing their privacy only when they choose to do so and on their own terms.

CONCLUSION

The legal community has paid little attention to the threat to individual privacy posed by modern computer technology. Recognition of the threat posed by the uncontrolled dissemination of personal information is an idea whose time has come. If information is allowed to be freely traded, the threat to personal autonomy is imminent. Individuals will begin to conform with what they believe to be societal norms. Societal conformity on such a grand scale will have untold detrimental effects on the cherished values of individuality and freedom upon which the United States was founded.

> [A person] who is compelled to live every minute of . . . life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of . . . individuality and human dignity. Such an individual merges with the mass. His opinions, being public, . . . tend always to be conventionally accepted ones; . . . feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every [person]. Such a being, although sentient, is fungible, [and] is not an individual.(110)

A democratic society has a duty to "foster the moral autonomy of citizens so they have the ability, the will, and the freedom to make valid decisions."(111) Additionally, human dignity and individuality need to be recognized as substantive personal interests, the violation of which are compensable. Once this is accomplished, the next step—protection of individual privacy and, thus, information privacy—should follow as the only natural solution.

(1)B.S. (business) Indiana University—Bloomington, 1993; candidate for J.D. Indiana

University—Bloomington, 1996. Thanks to Charles for his unwavering love and support.

(1)Robert S. Peck, *The Right to be Left Alone*, 15 Hum. Rts. 26, 27 (1987).

(2)See generally Gary R. Clouse, *The Constitutional Right to Withhold Private*

Information, 77 Nw. U. L. Rev. 536 (1982); Louis Henkin, *Privacy and Autonomy*, 74 Colum. L. Rev. 1410 (1974); Jed Rubenfeld, *The Right of Privacy*, 102 Harv. L. Rev. 737 (1989); Bruce D. Goldstein, Comment, *Confidentiality and Dissemination of Personal Information: An Examination of State Laws Governing Data Protection*, 41 Emory L.J. 1185 (1992); E. Maria Grace, Note, *Privacy vs. Convenience: The Benefits and Drawbacks of Tax System Modernization*, 47 Fed. Comm. L.J. 409 (1994); John Shattuck, Comment, *In the Shadow of 1984: National Identification Systems, Computer-Matching, and Privacy in the United States*, 35 Hastings L.J. 991 (1984).

(3)381 U.S. 479 (1965).

(4)410 U.S. 113 (1973).

(5)See The Privacy Act of 1974, 5 U.S.C. § 552a (1994); The Right to Financial

Privacy Act of 1978, 12 U.S.C. § 3402 (1978).

(6)See Fair Credit Reporting Act of 1970, ch. 6, sec. 601, 84 Stat. 1128 (codified as

amended at 15 U.S.C. §§ 1681, 1681a-1681t (1988)); Video Privacy Protection Act of 1988, (also known as the Federal Videotape Privacy Protection Act), 102 Stat. 3195 (codified as amended at 18 U.S.C. § 2710 (1988)); Driver's Privacy Protection Act of 1994, 108 Stat. 2099 to 2102 (codified at 18 U.S.C. § 2721 (1994)); Cable Communications Policy Act, 98 Stat. 2779 (codified as amended at 47 U.S.C. § 551 (1988 & Supp. IV 1992)). However, all of this legislation deals with only a small niche of the privacy problem and is inadequate to deal with the problem on the scale

to which it has escalated.

(7)See, e.g., Shibley v. Time, Inc., 341 N.E.2d 337 (Ohio Ct. App. 1975).

(8)William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383 (1960). The four torts are

appropriation, false light, intrusion, and the public disclosure of private facts.

(9)See Alaska Const. art. I, § 22; Ariz. Const. art. II, § 8; Cal. Const. art. I,

§ 1; Fla. Const. art. I, § 23; Haw. Const. art. 1, § 6; Mont. Const. art. II, § 10; Wash. Const. art. I, § 7.

(10)Jeffrey Rothfeder, Privacy for Sale: How Computerization Has Made

Everyone's Private Life an Open Secret 23-24 (1992).

(11)Id. at 24.

(12)R.J. Ignelzi, *Mail and Telejunk: U.S. Marketers Have Your Number; Your Age and*

Shoe Size, Too, San Diego Union-Trib., July 4, 1995, at E1, E4.

(13)Vic Sussman, *Policing Cyberspace*, U.S. News and World Rep., Jan. 23, 1995,

at 55, 57. *See also* Pat Shellenbarger, *Privacy Pirates: The Curtain's Open, The Blind Is Up and Any Peeping Tom, Dick or Harry Can Look into Your Life Through a Computer Window*, Grand Rapids Press, Mar. 19, 1995, at J1.

(14)See generally Sussman, *supra* note 13, at 55; Peter F. Eder, *Privacy on Parade:*

Your Secrets For Sale!, The Futurist, July-Aug. 1994, at 38, 39.

(15)See Schellenbarger, *supra* note 13, at J1.

(16)See Rothfeder, Privacy for Sale, *supra* note 10, at 18-19.

(17)Sue Landry, *A Private Matter? Don't Count on it.*, St. Petersburg Times, Dec.

14, 1994, at 14A. *See also* Susan E. Fisher, *What Do Computers Know About You?*, PC Wk, Feb. 11, 1991, at 156.

(18)Fisher, *supra* note 17, at 156.

(19)Jeffrey Rothfeder, *Dangerous Things Strangers Know About You*, McCall's, Jan.

1994, at 88, 94. Medical records are not private. The MIB is an insurance consortium that collects information regarding Americans and Canadians from physician and hospital records. No federal law restricts the dissemination of medical records to anyone who requests them. *Id.* at 94.

(20)Shellenbarger, *supra* note 13, at J1.

(21)Consider, for example, the story of Tommy Robinson, a 1990 Arkansas GOP

gubernatorial candidate who would have faced then-Governor Bill Clinton for the state's top job had he won the primary election. During a physical examination, Robinson told his doctor that he consumed approximately one pint of bourbon a week. The doctor inadvertently recorded that Robinson consumed one pint of liquor a day. Robinson's incorrect medical records were printed in the *Arkansas Democrat*, ruining his reputation. He was defeated in the primary election. Rothfeder, Privacy for Sale, *supra* note 10, at 175-76.

(22)See generally Eder, *supra* note 14, at 38.

(23)Rothfeder, *Dangerous Things Strangers Know About You*, *supra* note 19, at 90.

(24)Steven Bibas, *A Contractual Approach to Data Privacy*, 17 Harv. J.L. & Pub.

Pol'y 591, 593 (1994). *See also* Eder, *supra* note 14, at 38.

(25)Richard Lacayo, *Nowhere To Hide*, Time, Nov. 11, 1991, at 34, 39.

(26)Bibas, *supra* note 24, at 593.

(27)Approximately 35 percent of those who pay to see their credit reports find that their

report contains someone else's data. Joshua D. Blackman, *A Proposal for Federal Legislation Protecting Informational Privacy Across the Private Sector*, 9 Santa Clara Computer & High Tech. L.J. 431, 434 (1993).

(28)Rothfeder, *Dangerous Things Strangers Know About You*, *supra* note 19, at 88.

(29)Jonathan P. Graham, Note, *Privacy, Computers, and the Commercial Dissemination*

of Personal Information, 65 Tex. L. Rev. 1395, 1400 (1987).

(30)The National Information Infrastructure: Agenda for Action, 58 Fed. Reg. 49,025

(1993).

(31)Id.

(32)Id. at 49,025 and 49,029 (acknowledging the threats to privacy inherent in the

gathering, sending, and receiving of personal information).

(33)Id. at 49,026.

(34)Id. at 49,029.

(35)Inquiry on Privacy Issues Relating to Private Sector Use of Telecommunications-Related Personal Information, 59 Fed. Reg. 6,842 (1994).

(36)Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193,

195 (1890).

(37)Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for*

Individual Rights?, 44 Fed. Comm. L.J. 195, 201 (1992).

(38)Alan F. Westin, *Science, Privacy, and Freedom: Issues and Proposals for the*

1970's: Part II—Balancing the Conflicting Demands of Privacy, Disclosure, and Surveillance, 66 Colum. L. Rev. 1205, 1210 (1966).

(39)John T. Soma & Richard A. Wehmhoeffer, *A Legend and Technical Assessment of*

the Effect of Computers on Privacy, 60 Denv. L.J. 449, 450 (1983).

(40)Rochelle Cooper Dreyfuss & David W. Leebron, *Foreword: Privacy and*

Information Technology, 2 Ann. Surv. Am. L. 495, 496-97 (1986).

(41)Alan F. Westin, Privacy and Freedom 7 (1967). This definition of privacy is

the one at greatest risk in the area of information privacy.

(42)Blackman, *supra* note 27, at 433.

(43)See, e.g., Roe v. Wade, 410 U.S. 113 (1973); Griswold v. Connecticut, 381 U.S.

479 (1965); and Pierce v Society of Sisters, 268 U.S. 510 (1925).

(44)Whalen, 429 U.S. 589, 603-04 (1977).

(45)Id.

(46)Id. at 606.

(47)Id. at 605.

(48)Id.

(49)Id. at 605-06.

(50)Id. at 607.

(51)Bob Geske, *Protecting Our Privacy Through the Electronic Keyhole of the 90's,*

Businesses are Peeping into Our Lives as Never Before, Virginian-Pilot (Norfolk, VA), Oct. 13, 1993, at C1. *See also* Jeanne M. Hauch, *Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris*, 68 Tul. L. Rev. 1219, 1225 (1994).

(52)Geske, *supra* note 51, at C1.

(53)Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 64-65 (1983).

(54)Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456 (1978).

(55)Virginia Pharmacy Bd. v. Virginia Citizens Consumer Credit Council, Inc., 425

U.S. 748, 771-72 (1976).

(56)Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 762 (1985).

(57)See Alaska Const. art. I, § 22; Ariz. Const. art. II, § 8; Cal. Const. art. I,

§ 1; Fla. Const. art. I, § 23; Haw. Const. art. I, § 6; Mont. Const. art. II, § 10; Wash. Const. art. I, § 7.

(58)See Ill. Const. art. I, § 6; La. Const. art. I, § 5.

(59)"All people are by nature free and independent and have inalienable rights. Among

these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const. art. I, § 1 (amended 1972).

(60)Cal. Civ. Code § 1798.1 (West 1985).

(61)Porten v. University of S.F., 134 Cal. Rptr. 839, 842 (1976).

(62)Prosser, *supra* note 8, at 389.

(63)Although Dean Prosser said he was not trying to define the law of privacy torts, his

definitions have been almost wholly accepted by the *Restatement (Second) of Torts* and are virtually the only privacy torts recognized today. *See* Restatement (Second) of Torts § 652A (1977).

(64)Prosser, *supra* note 8, at 389. The *Restatement* defines this tort as "publicity that

unreasonably places the other in a false light before the public." Restatement (Second) of Torts § 652A (1977).

(65) Prosser, *supra* note 8, at 389. The *Restatement* defines this tort as "unreasonable

intrusion upon the seclusion of another." Restatement (Second) of Torts § 652A (1977).

(66)Prosser, *supra* note 8, at 389. The *Restatement* defines this tort as "unreasonable

publicity given to the other's private life." Restatement (Second) of Torts § 652A (1977).

(67)Prosser, *supra* note 8, at 389. The *Restatement* defines this tort as "appropriation

of the other's name or likeness." Restatement (Second) of Torts § 652A (1977).

(68)Restatement (Second) of Torts § 652E (1977).

(69)Id. at § 652B.

(70)Id. at cmt. a.

(71)Id. at cmt. c.

(72)Prosser, *supra* note 8, at 392.

(73)Restatement (Second) of Torts § 652D (1977). According to Prosser, the

elements of this tort are: (1) the "disclosure of the private must be a public disclosure, and not a private one"; (2) "the facts disclosed to the public must be private facts, and not public ones" and (3) "the matter made public must be one which would be offensive and objectionable to a reasonable man of ordinary sensibilities." Prosser, *supra* note 8, at 393-96.

(74)Restatement (Second) of Torts § 652D (1977).

(75)Id. at § 652C.

(76)See White v. Samsung Electronics America, Inc., 971 F.2d 1395 (9th Cir. 1992),

cert. denied, 113 S. Ct. 2443 (1993); Midler v. Ford Motor Co., 849 F.2d 460 (9th Cir. 1988). *See also* Graham, *supra* note 29, at 1412.

(77)Invasion of privacy through the dissemination of private information recently has

been recognized as a tort by the *Restatement (Third) of Unfair Competition*. However, as with the appropriation of

name or likeness, the *Restatement (Third) of Unfair Competition* also recognizes this right for public figures. Restatement (Third) of Unfair Competition §§ 46-49 (1995).

(78) *See* Graham, *supra* note 29, at 1428.

(79)Id. at 1429.

(80)Id. at 1430.

(81)Bibas, *supra* note 24, at 592.

(82)Id. at 606.

(83)Id. at 608.

(84)Id. at 595.

(85)See supra notes 15-29 and accompanying text.

(86)Bibas, *supra* note 24, at 608.

(87)Privacy Act of 1974, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a

(1994)).

(88)Right to Financial Privacy Act of 1978, 92 Stat. 3697 (codified as amended at 12

U.S.C. §§ 3401-3422 (1994)).

(89)Miller, 425 U.S. 435 (1976).

(90)Id. at 440.

(91)12 U.S.C. § 3402 (1994).

(92)Id. at §§ 3405-3407 (1994).

(93)Fair Credit Reporting Act of 1970, ch. 6, § 601, 84 Stat. 1128 (codified as

amended at 15 U.S.C. §§ 1681, 1681a-1681t (1988)).

(94)15 U.S.C. § 1681(a)(4) (1988).

(95)Id. at § 1681(b)(3).

(96)Video Privacy Protection Act of 1988 (also known as the Federal Videotape Privacy

Protection Act), 102 Stat. 3195 (codified as amended at 18 U.S.C. § 2710 (1988)).

(97)Id.

(98)Cable Communications Policy Act, 98 Stat. 2779 (codified as amended at 47

U.S.C. § 551 (1994)).

(99)Driver's Privacy Protection Act of 1994, 108 Stat. 2099-2102 (codified at 18

U.S.C. § 2721 (1994)).

(100)Id. at § 2100.

(101)Cal. Civ. Code §§ 1785.1, 1785.32, 1786, 1786.52 (West 1985); Kan. Stat.

Ann. §§ 50-701-722 (1994); Md. Code Ann., Com. Law II § 14-1207 (1990 & Supp. 1994); Mass. Ann. Laws ch. 93 §§ 50-59, 105 (Law. Co-op. 1995); Mont. Code Ann. § 31-3-101 (1993); N.H. Rev. Stat. Ann. §§ 359-B:2 to -:21 (1995); Wash. Rev. Code § 19.182.005-902 (1994).

(102)Ariz. Rev. Stat. Ann. §§ 20-2106 to -2107, 20-2111 to -2112, 20-2119 (1990);

Cal. Ins. Code §§ 791, 791.06 to .07, 791.21 (West 1993); Conn. Gen. Stat. §§ 38a-981, -982, -996 (1994); Ga. Code Ann. §§ 33-39-1 to 33-39-23 (1990); Ill. Ann. Stat ch. 215, §§ 5-1001 to -1024 (Smith-Hurd 1993); Mass. Ann. Laws ch. 175 I §§ 6 - 7, 21 (Law. Co-op. Supp. 1995); Minn. Stat. Ann. § 72A.505 (West 1986); Mont. Code Ann. §§ 31-19-101 to -409 (1993); N.C. Gen. Stat. §§ 58-39-1 to -120 (1994).

(103)Ariz. Rev. Stat. Ann. § 41-1354 (1992); Ark. Code Ann. §§ 13-2-704 to -705

(Michie 1987, Supp. 1993); Colo. Rev. Stat. § 24-90-119 (1990); Mass. Ann. Laws ch. 93 § 106 (Law. Co-op. 1995); Mich. Comp. Laws Ann. §§ 397.603 to .604, (West 1988), 445.1713 to .1714 (Supp. 1995); Mont. Code Ann. § 22-1-103 (1993).

(104)Conn. Gen. Stat. § 53-422 (1994); D.C. Code Ann. § 43-1845 (1981); Me.

Rev. Stat. Ann. tit. 35-A, § 1701-A (West 1988 & Supp. 1995).

(105)Cal. Civ. Code §§ 1798.1, 1798.63 (West 1985); Fla. Stat. Ann. § 540-08

(West 1988); Miss. Code Ann. § 35-7-49 (1990); Neb. Rev. Stat. § 20-202, 20-204 (1991); Wash. Rev. Code Ann. § 46.12.380 (West 1987 & Supp. 1995).

(106)Council Directive of 24 July 1995 on the Protection of Individuals with Regard to

the Processing of Personal Data and on the Free Movement of Such Data. (copy on file with the *Federal Communications Law Journal*).

(107)Id. at art. 26(1).

(108)Graham, *supra* note 29, at 1423. Amending the Privacy Act was also suggested by

Rep. Robert Wise (D-W. Va.) in H.R. 685, 102d Cong., 1st Sess. (1991).

(109)See supra notes 81-86 and accompanying text.

(110)Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to*

Prosser, 39 N.Y.U. L. Rev. 962, 1003 (1964).

(111)Graham, *supra* note 29, at 1411.