Journal of Technology Law & Policy

Volume 4 | Issue 1 Article 4

January 1999

The Digital Explosion Comes with a Cost: The Loss of Privacy

Suzanne M. Thompson

Journal of Technology Law & Policy
Volume 4 Spring 1999 Issue 1
Published by Students at the University of Florida College of Law

Return to Table of Contents	Comment on This Article

The Digital Explosion Comes With a Cost:
The Loss of Privacy

By Suzanne M. Thompson

Cite as: Suzanne M. Thompson, *The Digital Explosion Comes With a Cost: The Loss of Privacy*, 4 TECH. L. & POL'Y 3 <http://journal.law.ufl.edu/~techlaw/4/Thompson.html> (1999).

TABLE OF CONTENTS

INTRODUCTION

{1} The protection of privacy is being critically challenged by the explosive growth in network collection, storage and transmission of information circulating in cyberspace. [1] In the unbound world of the Internet nothing can completely stop information users from the surreptitious collection of

personal information. The following excerpt from Jeffrey Rothfeder's Privacy For Sale, [2] illustrates how the hidden picture of a person's secret life can be skillfully revealed through the manipulation of online information and the frightening effect the computer potentially has on personal rights.

{2} Rothfeder was asked by Christina Danvers' to find her husband, who recently ran off leaving her with a trail of debt including a $60,000 IRS lien on their property. Christina sought a court order to compel Michael to pay for half of the debt. The court issued a bench warrant for his arrest and payment of debt although, in essence, the case was closed.

{3} Jeffrey Rothfeder, with only the use of his computer and relying solely on the name of her husband, accessed databanks maintained by superbureaus and legitimate electronic public records.

{4} First he started with an on-line directory and ascertained the name of his wife, their present home address, length of residence and phone number, which allowed Rothfeder to obtain a credit report and their social security numbers. He discovered that Michael and Christina Danvers lived in a comfortably expensive home in Scarsdale, New York; Michael was an attorney in the Bronx and Christina was a television producer in Manhattan; and a few years before their salary reached the six-figure mark, they lived on 95th Street in Manhattan.

{5} By downloading public records Rothfeder also found out that the Danvers' three bedroom home cost $320,000 when they bought it in 1989 and that their mortgage is $1,500 a month; they drive a gray Mercedes and a white Jeep, which they lease for a total of $692 per month; they used to own an '85 Volkswagen and an '84 Porsche; and Christina has no credit cards in her name and uses Michael's social security number on several of her business transactions.

{6} Finally, Rothfeder cross referenced their recent long distance calls with a directory that supplies a person's name, address and household makeup from just a phone number; he was able to learn that Michael's parents, as well as Christina's, lived in Florida; and Michael's sister lives in Detroit. Within an hour on the computer Rothfeder was able to obtain information that was later used to trace Michael's movements to unearth his whereabouts. [3]

{7} While in the example above Christina Danvers' husband was brought to justice, there is a disquieting fear and confusion with the escalating use, misuse and abuse of personal information within the American public. Survey research conducted over the past twenty years documents deep concern among Americans about how personal information is being used in the Information Age. In a 1994 Harris Survey of Americans' attitudes about privacy and emerging interactive technologies, 82% of respondents stated that they were concerned about threats to their personal privacy. [4] According to the same survey, 78% of respondents believe that consumers have lost all control over how business circulates and uses personal information. [5]

{8} The accumulation of consumer data being collected is currently compiled, analyzed, reused, disclosed and sold in unimaginable ways with little or no legal restrictions, often without the consumer's knowledge or consent. [6] Clickstream data,[7] cookie technology [8] and distributed computing [9] disperses personal information while obscuring the identities of collectors of this information, thereby allowing little or no redress for unfair information practices.

{9} The globalization of an online marketplace benefits freedom of speech and the right to receive information. As information becomes a key aspect of the 21st Century, the evolution of the information infrastructure presents an ironic dilemma for a democratic society — enhanced economic value of personal information as opposed to invasion of individual privacy. The extensive collections of personal

information through network systems is jeopardizing the preservation of privacy and undermining both the First Amendment and the commercial potential of the global marketplace. [10]

{10} It is essential that privacy protection becomes a core element of computer networks so individuals can control the flow of their own personal information. The traditional approach to privacy protection has been regulation by an ad hoc sectoral approach, which has resulted in a purely context-specific response to privacy, thus leaving open many unregulated avenues for the collection and dissemination of personal information. It is necessary to develop and implement a comprehensive set of privacy safeguards within the global network so that consumers of the 21st century have confidence in technology and business and industry can flourish in an interactive global marketplace.

{11} This article will embody a discussion of the privacy implications in the digital age and the effect of mass compilation of personal data on an individual's ability to control their personal information. Part 1 will trace the development of informational privacy and discuss the threat of advanced network communication systems to individual privacy. Part 2 will set forth the U.S. framework regulating fair information practices of data protection. Part 3 will then explore U.S. legislation relevant to the protection of personal identifiable data in a context-specific manner. Part 4 will introduce the Clinton Administration's response to data protection in the Information Age. And finally, Part 5 will discuss the options for enhancing informational privacy.

I. BACKGROUND

{12} In the current era, often described as the Information Age, communication technologies that make possible the collection, storage, and transmission of enormous amounts of information are now expanding to engage the individual in a variety of activities. [11] More and more people are using interactive technologies to communicate through email, visit sites on the World Wide Web, browse and link to other sites, purchase products on the electronic marketplace, receive information from newsgroups, and gather and share information on topics of interest in chatrooms.

{13} Using these network communications the users disclose personal information about themselves in the form of name, address, phone number, marital status, employment information, financial information, and other personal identifiable information. [12] Many users voluntarily reveal personal information while on-line by registering in chatrooms and newsgroups. Internet users must register with a service provider. The registration process requires the user to disclose personal information relating to an individual's name, address, computer configuration, and email account. Many times personal information is required along with financial transactions such as purchasing goods on an on-line marketplace.

{14} Personal information is also generated involuntarily while on-line. An Internet browser records the trail of connections or websites an individual visits, referred to as clickstream data. Web technology called cookies can place information about a user's visits in a file on the user's computer that can only be read by that web provider. The electronic transmission leaves a personal profile, usually without the user's knowledge. [13] As a result of an individual traveling the information superhighway, "transactional data" [14] is generated and recorded by advance computer and communication networks as a byproduct of all these activities. The accumulation of these transactions can provide a comprehensive and detailed dossier about individuals' private lives. To varying degrees, people expect that this transactional data is "private." [15]

{15} Nearly all commercial companies are involved in collecting and maintaining information records on customers, employees, members and contributors. [16] The potential benefits to the consumer and

marketing industry are undisputed. The digital explosion has allowed private entities to generate, manipulate, transmit and store information with greater ease and speed. [17] The ability to manipulate computerized data is one of the most attractive benefits to using electronic format. The process of collection, storage, and dissemination of information in electronic format is dramatically lower in cost than the equivalent process using paper. Electronic data also has a greater value than its paper counterpart because by manipulating or correlating the data to many discrete lists, a physical transaction is no longer necessary. [18] Companies claim that the liberal exchange of financial data enables creditors to charge lower interest rates because they no longer have to bear the cost of acquiring the financial data. [19] Direct marketers argue that by targeting their audience, they conserve paper, drive down prices, and increase consumer choice. [20]

{16} Dealing in personal information in the private sector is a profitable industry. [21] Transactional data represents an efficient source of information that, when made available to direct marketers, can be a useful and valuable tool. [22] With the increase of personal computing in the last decade, it has been easier than ever to build a detailed profile of an individual's behavior, political views, product preferences, health status, and other personal identifiable information. [23] The compilation of this data results in targeted marketing by the direct marketing industry. Whether these companies buy lists from on-line service providers, grocery stores, credit card transactions, or bank transactions, the manipulation of these lists allows direct marketers to target the consumer's needs by mail solicitations or targeted advertisements.

{17} At the same time, personal information is being misused. Personal data is being manipulated for purposes other than those originally intended when collected. [24] Credit reports established to track and determine credit-worthiness are being sold to direct marketers for promotional purposes. [25] In turn, direct marketers cross-reference lists of information with a desired set of criteria to establish detailed personal profiles. [26] The direct marketers engaging in such activities thrive on the secondary use of personal information and have no direct relationship to the individual about whom the information pertains. [27] Most citizens are unaware of how collected information is utilized, in part because the collection is being done without consent. [28] Many times the secondary disclosure of cross-referenced personal data ultimately results in potentially offending personal details, such as a list of women who wear wigs or impotent middle-aged men. [29] To privacy advocates, the release of information without one's consent is a serious breach of privacy, especially when the disclosure of the information has a negative impact. [30]

{18} The proliferation of computerized personal data also has other consequences beyond the misuse of personal information. The use and sale of personal identifiable information along with the extensive secondary use of such data facilitates error. The increased amount of information being collected and sold through the use of computers undercuts the accuracy and completeness of the information. [31] Once an error, such as an incorrect address, is collected and stored in a database, it is easily multiplied when sold to a number of buyers of personal data. [32] Although the marketplace might control the dissemination and propagation of incorrect data by refusing to deal with unreliable sources, the amount of error in current databases far outweighs the ability to use discretion in purchasing reliable lists of personal identifiable information. [33]

{19} More significantly, some errors have resulted in irreparable injury to consumers. [34] For example, Terry Rogan brought suit against the city of Los Angeles when his credit cards and identification were recently stolen, and mistakenly the FBI's computerized National Crime Information Center listed an arrest warrant for Rogan instead of the person who stole Rogan's I.D. [35] As a result, over the succeeding 14 months Rogan was arrested five times at gunpoint. [36] The fact is, these problems are not uncommon, although they are usually less serious than Rogan's situation. [37] Individuals "are handicapped in dealing with such organizations since there is no law, at any level of government, which

requires any organization that collects personal information to notify the people involved of that fact." [38] Only with great difficulty can individuals find out if they are part of a record or list. Even if an individual is lucky enough to find out he or she is included in a database, federal and state law may not give the individual the right to examine the file and make corrections. [39]

{20} The lack of laws protecting an individual's personal information may reflect the fact that the Constitution does not grant an express right to privacy, although the right to privacy has been inferred from the Constitution. Although privacy is never explicitly stated in the Constitution, various Constitutional guarantees create zones of privacy. [40] The First Amendment privacy values of freedom of expression, [41] association, [42] and religion; the Fourth Amendment's right to be free from unwarranted searches and seizures; [43] "fundamental decision making" in the penumbras of the Bill of Rights; and the Fourteenth Amendment's concept of personal liberty [44] provide the many forms of privacy within the Constitution. Even where the courts have provided limited protection for privacy, it must be balanced against the First Amendment's guarantee of free expression. [45] Any government effort to protect privacy, either directly or through the passage of laws permitting suits by private individuals, faces significant First Amendment obstacles. Practically, when privacy rights conflict with free expression the latter will prevail. [46]

{21} The Supreme Court has crafted a limited framework for protecting individuals' right to privacy in the context of government activities concerning personal information and no support at all for privacy rights outside the public sector. [47] In 1977 a new form of privacy emerged in *Whalen v. Roe*, [48] a case involving a New York statute requiring that copies of prescriptions for Schedule II drugs be provided to the state. The statute was challenged on the basis that the requirement would infringe on patients' privacy rights. [49] Writing for the majority, Justice Stevens wrote that the Constitutionally protected zone of privacy included two separate interests: independence in making certain kinds of important decisions and avoiding disclosure of personal matters. [50] The first interest is clearly grounded in *Roe v. Wade* [51] and *Griswald v. Connecticut.* [52] The second privacy interest is the creation of the individual interest in avoiding disclosure of personal information. [53] Thus, the Court began to view personal information as existing within the protected sphere of privacy.

{22} The U.S. Constitution offers little support for informational privacy-- defined by Alan F. Westin in *Privacy and Freedom*, as "the claim of individual, groups, or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others." [54] This concept of privacy entails the right to control information about oneself, which acknowledges the critical value of being able to step forward and participate in society without having to relinquish all control over personal information. [55]

{23} The rampant use of personal information, the growing public and private concerns about privacy, the advanced technologies and the lack of strong Constitutional privacy protection led Secretary of the Department of Health, Education, and Welfare, Elliot L. Richardson, in 1972, to appoint an Advisory Committee on Automated Personal Data Systems. [56] The Advisory Committee's published report in 1973, *Records, Computers, and the Rights of Citizens,* [57] (HEW Report) contained an enduring set of policies that defined the ethics of fair information practices and became the foundation of privacy protection in the U.S. The following section will discuss the intellectual and conceptual framework of privacy and its basis in the HEW report.

II. U.S. FRAMEWORK REGULATING FAIR INFORMATION PRACTICES

{24} The term privacy is used as a broad catch-all phrase covering activities in the home to telephone communications to individuals' right to control personal information about themselves. [58] The term "fair information practices" is a narrower phrase defined by the collection of legal rules, industry norms,

and business practices governing the control of personal information. [59] "Although fair information practices may be subsumed under the broad 'privacy' label, the standards represent a more narrow and distinct interest: maintaining the integrity of personal information and fairness to the individuals about whom the data relates. Specifically, such standards apply to the collection, use, and disclosure of personal information." [60]

{25} The United States regulatory scheme and the distribution of power between the state and federal level presents a complex framework for the control of personal information. The approach used by the U.S. to control personal identifiable information is context-specific in that the U.S. directs fair information practices at specific kinds of processing activities and are almost always directed at either the public or the private sphere. [61] Fair information practices target specific contexts of information processing such as financial records, credit reports, and telecommunications systems. In addition, citizens' rights may be protected separately under federal or state law or collectively through the combination of federal and state laws. [62] Moreover, most data protection regulations are in response to a perceived crisis such as the Driver Privacy Protection Act which was enacted by Congress after the stalking and murder of actress Rebecca Schaffer whose personal information was revealed through motor-vehicle records. [63]

{26} In addition to legal regulations for fair information practices in the private sector, industry norms provide standards for the control of personal information. Company policies and practices, internal codes of conduct, and contractual agreements also promote standards for the treatment of personal information. As a result of the various sources of informational privacy protection, fair information practices are generally targeted narrowly. [64] "Legal regulation usually protects a single activity or area and does not address all of the issues of collection, storage, use and disclosure." [65]

{27} While statutory privacy protection for personal information has been crafted on a sector by sector basis, many of these statutes are based upon the common set of principles developed by the Department of Health, Education and Welfare, Advisory Committee on Automated Personal Data Systems. In its 1973 report, the Committee addressed the harmful consequences of automated personal data systems and made recommendations for safeguards in the public and private sector that may protect against those consequences. [66] The Advisory Committee designed the Code of Fair Information Practices, based upon notice, consent, access, and integrity. [67] The fundamental provisions of the Code are:

1. there must be no personal data record keeping systems whose very existence is secret;
2. there must be a way for individuals to find out what information is in their file and how the information is being used;
3. there must be a way for individuals to correct information in their records;
4. any organization dealing in records of personally identifiable information must assure reliability for its intended use, and must take precautions to prevent misuse; and
5. there must be a way for individuals to prevent personal information obtained for one purpose from being used for another purpose without consent. [68]

{28} The Advisory Committee generally concluded that institutions should be held liable for unfair information practices through private litigation rather than criminal law. [69] Although there is a question of what data privacy rights an individual has on-line, the Code of Fair Information Practices provides a backbone upon which individuals may bring formal legal action to enforce the privacy interests of on-line users. The Committee's choice of enforcement through individual action was chosen in part to "create no obstacles to further development, adoption and application of a technology that, as we all know, has brought a variety of benefits to a wide range of people and institutions in modern society." [70]

{29} The Code of Fair Information Practices has important implications for data users in the Information Age. First, Congress has crafted many subsequent data privacy laws within the framework set forth by the Advisory Committee. Second, the Code provides the flexibility needed to adhere to contextual differences for personal data protection on network systems. Third, the Code of Fair Information Practices was created with the flexibility to adapt to the rapid technological advances of modern society. And fourth, it allows individuals to take an active part in controlling their personal information by providing individual legal action.

{30} However, the Code of Fair Information Practices has not been implemented as a whole into any subsequent bill. While the Code of Fair Information Practices represents an initial step in protecting individual privacy, an analysis of the U.S. current legislation will show the failure of current regulations to govern the use of personal transactional data on-line. The multi-layered regulatory framework in the U.S. necessitates a context-specific methodology to analyze fair information practices. This paper will next review four regulatory aspects of privacy legislation that have a significant impact on American life — (1) Public Sector, (2) Telecommunications, (3) Financial Data, and (4) Direct Marketing — and their impact on on-line transactional data in the private sector.

III. THE U.S. PIECEMEAL REGULATORY FRAMEWORK

{31} The current protection of personal information is approached by an ad-hoc process —targeting personal information on a case-by-case basis in either the public or private sector, either at the state or federal level, and in differing contextual and jurisdictional conditions. [71] This targeted approach results in uneven, inconsistent, and often less than adequate protection for personal data. [72] There are no universal fair information guidelines or practices that can be applied to ensure the protection and privacy of personal information. [73] Under the U.S. scheme, no single standard cuts across boundaries of law or industry practice. Furthermore, with the technological advances of the Internet, targeted standards are problematic. The use of computers allows personal information to be disseminated across sectors thus defying the aim of context-specific regulations and practices. "Information technology renders data multifunctional and fluid. Once in digital form and available on electronic networks, personal information may be combined and shared across sectoral lines." [74] Current information practices challenge the U.S. piecemeal approach to informational privacy protection because there is widespread, cross-sectoral use of personal information. [75]

{32} This section will analyze the fair information practices most relevant to the protection of personal data in both the public and private sector. It will discuss the lack of protection informational privacy is given by the U.S. framework.

A. PUBLIC SECTOR REGULATIONS

{33} Since the development of the Code of Fair Information Practices, much of the subsequent privacy legislation enacted has been greatly influenced by these standards. [76] While the Code is not binding, it has been very influential in setting the tone and content of laws that limit access to and use of personal information. An early embodiment of the code can be found in the Privacy Act of 1974. [77] The Privacy Act is strikingly similar to the Code of Fair Information Practices and many of the Committee's proposals were enacted almost verbatim in it. [78]

{34} Congress passed the Privacy Act of 1974 [79] to "promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and databanks of the federal government." [80] This was one of the first national data protection laws that targeted the governmental misuse of personal information. [81] Consistent with

the HEW Code of Fair Information Practices, the Privacy Act prohibits government agencies from disclosing any record on any individual, for any purpose other than that originally intended, without that individual's consent. [82] The Privacy Act also grants individuals a right of access to their records, and the opportunity to amend their records if they can show a lack of accuracy, relevancy, timeliness, or completeness in the record. [83] Enforcement provisions allow for an individual to bring a civil action for damages or injunctive relief against the federal agency violating the statute based upon a showing of harm to the individual arising out of the agency's violation. [84]

{35} However, due to strong pressure from federal agencies and private sector industry groups, only public actions were covered by the statute; [85] it does not extend to cover actions by private entities. Although the act was originally intended to protect privacy concerns from the increasing use of computerized records, it failed to protect the biggest privacy intrusion today —the collection of personal identifiable information by private sector entities.

{36} The Privacy Act was amended by the Computer Matching and Privacy Protection Act of 1988. [86] The purpose of the amendment is to regulate the use of data matching procedures in the federal agencies. [87] Privacy advocates view data matching as an unnecessary intrusion into privacy interests, for data gathered by one agency may be disclosed to others without the individuals' consent. [88] From the government's perspective, data matching is a cost efficient way to allocate public resources and detect waste, fraud and abuse of programs by sharing personal information from databases across agencies. [89] The 1988 Computer Matching Act requires federal agencies that exchange personal data to publish advance notice of the computer matching program for public comment before taking action. [90] The act does not limit the type or number of records subject to matching; instead it sets forth a procedural framework requiring mandatory reporting requirements for government agencies that match records. [91]

{37} The Computer Matching Privacy Act falls short of protecting against detailed profiling of individuals in the private sector--this legislation only binds the computer matching of federal agencies. Private marketing enterprises profitably buy and sell customer lists, which indicate interests and purchasing habits, providing detailed profiles of individuals and families. Many of the direct marketing intrusions into privacy result from the matching of various customer lists, making detailed profiling a popular option. And with the proliferation of computers and transactional data generated from matching, the marketing industry's use of this cost efficient method of gathering information has run rampant.

B. PRIVATE SECTOR REGULATIONS

{38} The advanced technologies of the Information Age have changed the focus of data protection from government entities, who in the past have controlled the majority of personal information, to the private sector, which is now a major source for the widespread dissemination of personal data. [92] Privacy debates concerning the use of personal data are beginning to focus on the private sector's use of transactional data. [93] However, the ad-hoc approach to current legislation in the United States has failed to protect the extensive misuse of personal data by private entities. [94] The United States does not have comprehensive privacy rights that address the acquisition, use, transmission, or disclosure of personal information within the private sector. [95] Even less protection is given to transactions taking place over the global network. The advent of the Internet and other networked communications has challenged the effectiveness of past piecemeal regulations. [96]

TELECOMMUNICATIONS PRIVACY REGULATIONS

{39} The emergence of personal computers and networking in the 1980s contributed to a shift in power

to the commercial sector. Smaller private sector entities became involved in performing telecommunications functions, and the issue of protecting personal information became important. [97] In the course of subscribing to Internet service providers, individuals must provide personal information such as home address, home and work phone numbers, type of computer used, and credit card payment information to the service provider. Transactional information is also generated in the course of using a particular communication service, such as the trail of connections left as a result of browsing the Internet.

{40} The Electronic Communications Privacy Act of 1986 [98] (ECPA) amended the federal Wiretap Law, which protected unwarranted interception of wire and oral communications, [99] to include electronic communications. [100] The ECPA was enacted to protect interactive electronic communication systems. It prohibits unauthorized eavesdropping and interception of the "contents" of email, radio communications, data transmission, and telephone calls. [101] The ECPA's protections extend to data in transit and information being stored [102] by an electronic communication service provider. [103] Although the ECPA extended protections to the intrusion of computerized transmission of data and video, it does not protect against the collection of transactional data generated from this transmission. [104] An electronic communication service provider is even expressly permitted, without notice or subscriber consent, to disclose transactional information concerning the subscriber to any person, other than a government entity, for any purpose. [105]

{41} To address the gap in transactional data protection, Congress recently passed the Telecommunications Act of 1996, [106] which imposes several targeted transactional data protection obligations on communication service providers. Following the enactment of the Telecommunications Act, broad secondary use of transactional data and subscriber information by telecommunications carriers became illegal. [107] Common carriers [108] are required to document some customer proprietary network information (CPNI) [109] for interstate calls. However, the Telecommunications Act of 1996 prohibits the compilation of transactional data for any purpose other than that which is required and thereby eliminates the ability of common carriers to collect extensive amounts of customer data for secondary use.

{42} The law prohibits a telecommunications carrier that receives or obtains customer proprietary network information (CPNI) from *another* carrier from using such information for its own marketing efforts. [110] But, the law allows the carrier to use CPNI generated from its *own* service to provide inbound telemarketing, referral, or administrative services to its own customers as long as the customer approves of such use. [111] However, the law does not limit the amount of information being collected; thus, customers are at great risk of detailed profiling by their own carrier service. [112]

FINANCIAL DATA PRIVACY REGULATIONS

{43} In the context of financial data, privacy interests have been protected in the private sector for thirty years. The Fair Credit Reporting Act [113] (FCRA) regulates the disclosure of personal information in consumer's reports by credit reporting agencies. These agencies collect information pertaining to credit worthiness, credit capacity, character, reputation, or mode of living. [114] But the restrictions do not apply to the disclosure of such personal information by organizations other than credit reporting agencies. Any person buying a credit report of another from a credit reporting agency may disclose any information found in that report. Furthermore, the FCRA requires only that credit bureau customers have a permissible business purpose to purchase credit reports which leaves open a wide range of persons who may obtain these reports. [115] The FCRA does not contain regulations prohibiting the unnecessary collection of personal information and the credit reporting industry itself implicitly authorizes the extensive collection of personal information by credit reporting agencies. [116]

{44} The Electronic Fund Transfer Act (EFTA), [117] passed in 1978, regulates the use of electronic systems, including on-line banking, to transfer funds. This federal statute requires detailed documentation of each transfer which generates large amounts of transactional data and requires financial institutions to provide customers with periodic statements. [118] However, the EFTA has no restrictions on the disclosure of transactional data to third parties or regulations regarding the duration of storage of information.

DIRECT MARKETING PRIVACY REGULATIONS

{45} As more and more people use the Internet and other networks for commercial activities, direct marketing is occurring on-line. According to the Direct Marketing Association [119] (DMA), more than half of direct marketers are using the Internet for advertising and 48% are "mining the membership rosters of major computer on-line services for email addresses." [120] The industry ardently promotes self-regulation through the DMA. [121] Recently, it issued a Manual for Fair Information Practices [122] to discourage formal legal regulations and to promote the industry's commitment to self-regulation. [123]

{46} However, the polls suggest that less than 25% of the industry is willing to initiate self-regulatory practices. [124] The DMA guidelines state that personal data should be collected by "fair and lawful means for a direct marketing purpose." [125] While the DMA guidelines indicate that personal information should be transferred between direct marketers only for direct marketing purposes, companies seem to construe the meaning of direct marketing purposes rather broadly [126] — that all personal information can be used for the purpose of marketing. [127] Furthermore, many people in the industry advocate secondary use of personal information for the purpose of direct marketing. [128] Although some of the direct marketing practices are merely annoying, such as intrusive phone calls marketing products, others are a more serious invasion of privacy, such as the distribution of a list of men who buy fashion underwear. [129]

{47} There is no overarching law governing the collection, use and disclosure of personal information by direct marketers, although there are several narrow, context-orientated laws in the area of telecommunications services and home entertainment services that regulate the disclosure of personal identifiable information to direct marketing companies. [130] For example, the Cable Communication Privacy Act of 1984 [131] was passed to restrict the collection, use, and dissemination of subscriber viewing habits by cable systems operators. [132] The 1984 Cable Act permits operators to sell their mailing lists to third parties only if they have given the subscribers an opportunity to "opt-out" of such disclosure, and the information does not reveal the viewing habits of the consumer. [133] The Cable Television Consumer Protection and Competition Act [134] (the 1992 Cable Act) extends protections of the 1984 Cable Act to new wire and radio services that may be provided over cable facilities. In addition, the 1992 Cable Act requires cable operators to take those actions necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator. [135]

C. SUMMARY

{48} The United States provides an incoherent and nonsystematic approach to the management of existing privacy concerns, making fair information practices difficult to ascertain. The globalization of information processing networks leaves companies in the United States free to explore the Internet to gather personal transactional data for commercial uses.

{49} As has been shown, even when there has been an attempt to codify fair information practices through statute, regulations, or industry guidelines, it has generally fallen short of the desired goal of

privacy advocates — to have individuals control the collection, use and disclosure of personal information. [136] There is no statute that gives an individual simple, meaningful, up-front control over personal information. [137] The sector by sector approach of existing law has slowed progress toward comprehensive informational privacy rights, and many gaps remain. Without consistent rights for privacy protection, it is difficult for individuals to assess their informational privacy rights and enforce fair information practices for the treatment of personal information. This suggests that the legal approach to commercial data processing activities needs to be reconstructed.

{50} With the onset of the vast new marketplace in cyberspace and global Internet access, United States citizens are faced with additional risks and opportunities. Consequently, new gaps in the protection of personal information emerge with the growth of network communication systems. In 1993, the National Information Infrastructure [138] (NII) was established; it provided a seamless web of communications networks, computers, databases and continuing advances in telecommunications technologies. These advances came with a cost: the loss of privacy. To address this concern, the Information Infrastructure Task Force [139] (IITF) was instituted to ensure the NII achieved its full potential while at the same time protecting information privacy. [140]

IV. PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION

{51} Due to the interactive network systems, personal information flows are not confined to state or national borders. Fair information practices must cut across geographical and industry lines to address the collection, use and dissemination of personal information across jurisdictions. Thus, it may be most appropriate to adopt any new practices at the federal level. While network communications are not bound by national boundaries, informational privacy could be protected at the international level; however, a complete analysis of various international responses to personal privacy is beyond the scope of this article.

{52} To keep pace with the rapidly evolving technological and informational processing activities, a comprehensive set of rights or legal principles is needed. In addition, the complexity of the information economy requires a flexible method to adhere to differences in informational privacy rights. [141] If the mechanism that is ultimately chosen does not allow sufficient flexibility, informational privacy may frustrate future technological advances. [142]

{53} A proper balance between informational privacy concerns and commercial needs is an important consideration for any new framework. [143] Industries are properly worried that constraints on processing of personal information may impose burdens on legitimate activities and may encumber the development of informational processing networks. [144] A balance must exist if the business environment is to be conducive to the development of new information networks. [145]

{54} In 1993 the Clinton Administration established the Information Infrastructure Task Force (IITF) to articulate and implement the Administration's vision for the National Information Infrastructure (NII). [146] The task force's Information Policy Committee created the Privacy Working Group to consider ways in which the NII might affect individual privacy. [147] The Privacy Working Group drafted a set of principles entitled *Principles for Providing and Using Personal Information* to articulate the elements of fair information practices needed to ensure continued development of the NII. [148] The *Principles for Providing and Using Personal Information* incorporates the basic standards for the treatment of personal information as set forth by the HEW Code of Fair Information Practices discussed in Part 3, *infra*.

{55} The Privacy Working Group first identified three values to govern the way in which information is

acquired and used on-line: *information privacy* - an individual's reasonable expectation of privacy regarding access to and use of his personal information should be assured; *information integrity* - personal information should not be altered or destroyed; and *information quality* - personal information should be accurate, timely, complete, and relevant for the purposes for which it is provided and used. [149] Using these values as fundamental standards for informational privacy, the Privacy Working Group established eleven principles to guide participants of the NII. [150]

{56} *Informational Privacy Principle*- personal information should be acquired, disclosed, and used only in ways that respect an individual's privacy. [151] The level of privacy to be respected should be a reasonable expectation of privacy; subjectively held by the individual and objectively reasonable by society. [152] An individual's expectation of privacy depends not only on an objective standard held by society, but on what the individual reasonably expects is private information.

{57} While the Information Privacy Principle is broad enough to apply to the contextual differences in information processing activities, it seems to have some problems. The appropriate use of personal information must be considered on a case-by-case basis if information users must assess the individual's expectation regarding the use of the information. Another problem could arise with what an individual expects is "private information." A bookstore may record on computer the title of books that a customer purchases at a particular bookstore. Soon enough a profile is made of that individual's reading habits. Although some people may expect that their reading habits are private information, the Supreme Court has held that information in the "public domain" in no longer private. [153] The title of a book could be considered within the public domain if it was purchased in a public bookstore where the title could be observed by a public person.

{58} The Electronic Frontier Foundation [154] (EFF) also commented on the inherent flaws in the Privacy Working Group on the Privacy Principles. It pointed to the difficulty in determining and applying a "reasonable expectation standard" in an interactive electronic environment. [155] The EFF believes that the reasonable expectation standard may need to be determined by each context-specific regulation. [156] It further stated that such a standard will depend on the legal and regulatory protections set by Congress. [157]

{59} *Information Quality Principle*- personal information should be accurate, timely, complete, and relevant for the purpose for which it is provided and used. [158] The information quality principle was developed to maintain the integrity of the NII. The Privacy Working Group stated that participants should be able to rely on the integrity and quality of personal information; thus all users should take reasonable steps to make sure the information is accurate, complete, and not improperly altered or destroyed. [159] This is an important principle for users to adhere to because it will reduce error and the risk of harm to consumers that error may cause.

{60} Although the Privacy Working Group sets important goals for information suppliers to uphold the quality of information, the Information Quality Principle allows information users to use broad discretion in maintaining the quality of personal data. There is little incentive for companies to police themselves and company policies are usually non-transparent, therefore it may be troublesome to ensure that individual information is being upheld to the quality that the Information Quality Principle calls for. [160]

{61} *Acquisition Principle*- information users should assess the impact on privacy in deciding how to collect and use personal information, and should acquire and keep only information reasonably expected to support current or planned activities. [161] The Privacy Working Group expressly noted in its commentary that once privacy is lost, it can rarely be restored; thus privacy should not be addressed as a mere afterthought. [162] Rather, information users should consider the impact of privacy and gauge their

activities accordingly, hence the Acquisition Principle.

{62} This principle requires information users to assess the impact of privacy intrusions before taking action. [163] However, many companies are completely unaware of the impact information collection has on customers' privacy rights. It is inappropriate, according to this principle, to collect or store volumes of personal information just because it may be of some value in the future. [164] Libraries are gathering and storing volumes of information because librarians are certain it will have a future value; often as soon as the information is available, users find a way to incorporate it into their work. It is unclear whether the Acquisition Principle makes this practice unfair.

{63} *Notice Principle*- information users should provide individuals with adequate relevant information about the purposes for collection, the use of the information, what steps will be taken to protect confidentiality, and any rights of redress. [165] Individuals should have notice as to the purpose of the collection, use, or dissemination of their personal data from the information user. Those who collect information directly from the individual should give the individual sufficient information to make an informed decision about his or her privacy. [166]

{64} However, the Notice Principle also applies to information users who collect personal information through a secondary source rather than directly from the individual. [167] Many collectors of transactional data do not have a direct relationship with the individual to whom the information pertains and cannot give direct notice to the individual at the time of collection. [168] In this situation, the Privacy Working Group stated that "transactional facilitators" would ordinarily provide notice at the time they establish an account, or bill a customer. [169] For example, if an individual purchases flowers with a credit card through an on-line shopping mall, the Notice Principle would require notice be given to the customer from the florist when the product was bought, from telephone company supplying the modem service when the customer established the account, and from the credit card company when the customer was billed. [170]

{65} *Fairness Principle*- information users should not use personal information in ways that are incompatible with the individual's understanding of how it will be used, unless there is a compelling public interest for such use. [171] In deciding whether a particular use of information is "compatible" with an individual's understanding, information users should evaluate whether the use is consistent with the notice. [172] Any use beyond these conditions is prohibited.

{66} The problem with the Fairness Principle arises because an "incompatible use is not necessarily a harmful use; there are some incompatible uses that will produce enormous benefits and have at most a trivial effect on the individual's information privacy interest." [173] Research studies are the best example in which data collection will not negatively affect the individual and will provide great future benefits to society as a whole. [174] Obtaining consent of the individual for new statistical uses of existing data will be costly and impair research projects. [175]

{67} *Protection Principle*- information users should use appropriate technical and managerial controls to protect the confidentiality and integrity of personal information. [176] In protecting personal privacy, information users should adopt a multi-faceted approach that includes both technical controls such as encryption and managerial controls such as the procedural safeguards of notice and consent. [177]

{68} *Empowerment Principle*- individuals should be able to safeguard their own privacy by having a means to obtain and correct their personal information, using "appropriate" safeguards to protect the confidentiality of personal information, and remaining anonymous when appropriate. [178] Individuals should be able to access their own personal information to ensure "fairness in its use." [179] Individuals

should also have the opportunity to use tools such as encryption to safeguard their privacy. [180] Further, individuals should have the opportunity to remain anonymous in situations such as browsing a public library to avoid leaving a data trail of transactional records. [181]

{69} The problem with the Empowerment Principle occurs with the difficulty in correcting an error in a computer database. An individual may not be aware of an error in their personal information until they are turned down for a credit application, or a job, or insurance. Moreover, most individuals don't know which databases contain their personal information, which makes it very difficult to access and correct. It may be difficult to determine how and in what situations an individual may use technical controls or remain anonymous, but it remains to be seen how this option may become viable for individuals. The Privacy Working Group notes that some individuals will abuse technical controls such as encryption, and in the process will harm others. [182] The abuse of technologies is beyond the scope of the Privacy Working Group's commentary on the Privacy Principles, however, both of these issues need to be addressed for network communication systems to achieve their full potential. [183]

{70} *Awareness Principle*- individuals themselves should obtain adequate, relevant information about the collection, use, and confidentiality of their personal information being collected. [184] The Awareness Principle requires that individuals acquire notice of the use and dissemination of their personal information by obtaining any relevant information for themselves. It recognizes that individuals also have the responsibility for understanding the implications of providing others with personal information. [185] When individuals have a choice regarding disclosure of their personal information, they should take an active role in deciding whether to disclose information and under what terms. [186]

{71} "{I}f individuals are to be held responsible for making these choices, they must be given enough information to make intelligent choices." [187] This principle works in conjunction with the Notice Principle which allows individuals to make informed choices and enables individuals to take responsibility over how their personal information is disclosed and used. [188] However, individuals do not always have a choice in the disclosure of their personal information. Many times, information users collect personal data as a byproduct of transactions or from secondary sources such as direct marketers.

{72} *Education Principle*- information users should educate themselves and the public about how information privacy can be maintained. [189] "The Education Principle [is] a significant addition to traditional principles of fair information practice[s]." [190] Many NII participants may not recognize how their lives are affected by networked information. Such education could minimize the risks to privacy by making individuals aware of the hazards of providing personal information. [191]

{73} Even if individuals do take the opportunity to educate themselves about the various collection strategies of information users, they can never be fully aware of all the possible means of collection or the numerous potentially harmful uses of the personal information. In addition, the Privacy Working Group noted that individuals may not be able to rely on legal and institutional controls to protect their personal information because many users will operate outside of these controls. [192]

{74} *Redress Principle*- individuals should have a means of redress if they are harmed by an improper use or disclosure of their personal information. [193] The Privacy Principles set forth individual rights of redress if individuals are harmed by unfair information practices. Various forms of redress include mediation, arbitration, civil litigation, regulatory enforcement and criminal prosecution. [194] Allowing an individual or a private entity to pursue a remedy for unfair information practices will require information users to give informational privacy the attention that is needed to protect individual interests in the Information Age.

{75} However, the Privacy Working Group notes that redress is an option only when an individual is harmed. [195] It did not determine in any particular case whether harm has occurred at all, or whether enough harm has occurred to warrant redress. [196] Furthermore, the EFF reported that in reality, it is extremely difficult for an individual to obtain relief under existing laws even if actual harm occurs. [197] To address this problem, the EFF proposed the addition of a new provision that provides damages or injunctive relief for harms, including intangible harms, without requiring a showing of an adverse effect to the potential plaintiff. [198]

{76} The Privacy Principles developed by the Privacy Working Group offer a basis for future fair information practices regulating informational privacy. The principles establish benchmark standards for individuals seeking to control their personal information and for users of personal information. The broad approach taken by the drafters allows the Privacy Principles to extend across sector lines, governing fair information practices in both the public and private sectors. The Privacy Principles were crafted with the flexibility to adhere to future technological advances and to govern actions by the data collector, user, and individual dealing in personal identifiable information. They suggest that each actor take a heightened concern and awareness of privacy intrusions through collection, use or dissemination of personal data. Thus, the Privacy Principles provide a strong framework guiding fair information practices that should be implemented across the board, governing all information processing activities.

{77} The Empowerment, Awareness, and Education Principles, when taken together, require that each member of society have a heightened awareness of and concern for the implications that information privacy may present. The process of empowering individuals to act on behalf of privacy protection by assessing and correcting their own personal information or opting-out of any actions they deem intrusive, is a method that can be adhered to across the nation, in every context. In turn, the principles guide individuals and information users to take a substantial step in conquering the growing public fear of informational privacy intrusions.

{78} While the Privacy Principles are intended to guide all NII participants, the Privacy Principles do not have the force of law behind them in that they do not create any substantive or procedural rights. [199] The Privacy Working Group stated that the Privacy Principles should be used by those who are drafting laws and regulations, creating industry codes of fair information practices, and designing private sector and government programs that use personal information. [200] They provide the basic framework from which specialized principles can be developed. The Privacy Working Group concluded that trade-offs will be inevitable in implementing the Privacy Principles because privacy interests are not absolute and must be balanced against the needs of a democratic society. [201]

{79} The Center for Democracy and Technology (CDT) submitted an executive statement before the Federal Trade Commission in June 1996 commenting on the Privacy Principles and its vision for informational privacy protection in the 21st century. [202] The CDT commented that "despite the clear articulation of Privacy Principles that would, if implemented, preserve individual privacy, individuals are still experiencing an erosion of privacy." [203] The CDT believes empowerment solutions can provide individuals with the information and tools to make decisions with independence and flexibility. [204] The CDT further promotes individual empowerment and self-regulation by stating that all members of the Internet community must come together to build an infrastructure that supports policies and applications. [205] "Policies that support and encourage the development of technologies that give individuals control over the ideas and beliefs to which they are exposed, and the collection, use and disclosure of their personal information, will lay the foundation for a robust, thriving democracy in the Digital Age." [206]

V. OPTIONS FOR ENHANCING PRIVACY PROTECTION

{80} Currently, individuals may not participate in the NII for fear that costs to their privacy will outweigh the benefits. [207] This risk must be addressed to ensure the protection of privacy to individuals and allow the NII to reach its full potential. [208] "The adoption of principles of fair information practice is a critical first step in addressing this concern." [209] Thus, the question becomes: what is the best way to implement fair information practices in both the public and private sector in order to balance the needs of an Information Age and the protection of informational privacy. [210]

{81} Those who advocate the sectoral approach to the protection of informational privacy concede that there is room for improvement to current U.S. legislation. [211] Similarly, they believe that new action needs to be taken to preserve informational privacy. [212] One option would be for an enhanced sectoral approach to informational privacy by the federal government ensuring that data collections in each sector remain consistent with the Privacy Principles. [213] If the decision is made by the federal government to enhance privacy protection using a sectoral approach, the federal government could appoint the Office of Management and Budget (OMB) as an oversight agency, which, for example, might review privacy statutes in light of the Privacy Principles. [214] The OMB could promote an enhanced sectoral approach operating in a more cohesive fashion. [215] The OMB could report its findings and recommend legislation, regulation, or administrative orders to keep existing fair information practices consistent with the Privacy Principles. [216] Nonetheless, an enhanced sectoral approach will not solve the problem of context-specific laws that fail to provide the individual with adequate, identifiable, enforceable fair information practices. "The sectoral approach, even enhanced, may continue to produce inconsistent privacy protections, or fail to anticipate further developments in a comprehensive, thoughtful way." [217]

{82} A second option to protect informational privacy would be for the federal government to formally adopt the Privacy Principles; although to date, neither the executive nor legislative branch has formally adopted them as official policy. [218] Congress might also consider the formal adoption of the Privacy Principles as an omnibus privacy legislation. For example, "Congress might direct the Federal Trade Commission to undertake rule making to ensure that the collection and use of personal data in the commercial setting occurs in a manner consistent with the core principles of fair information practices — notice, choice, access and integrity." [219] The Office of Management and Budget could either direct all federal agencies to incorporate the principles in their information practices or use their powers of persuasion to encourage state and local governments, as well as business leaders, to adopt and implement information practices set forth in the Privacy Principles. [220]

{83} Another option to protect informational privacy would be for the government to promote enhanced self-regulation within each industry. [221] Under this scenario, the marketplace itself could protect privacy without any formal legislative action. In the Information Age, privacy may become a market commodity by providing contractual agreements that will protect an individual's personal information. Companies may use the promise of privacy as a way to compete for consumers. The demand for privacy by an individual from each company could develop a competitive market for privacy protection. Privacy scholar, Joel Reidenberg stated that to achieve this self-regulatory method, individuals and businesses both must be afforded a high degree of involvement in the decisions about the circulation of personal identifiable data. [222] Each interested side must be involved in setting rules for fair treatment of information on network communication systems. [223] Thus, there is a need for heightened awareness about informational privacy for all NII participants.

{84} Although market forces may play a role in protecting privacy, relying heavily on market forces is a mistake. [224] Some argue that free market forces will not discipline commercial practices, especially in instances where there is no direct relationship between the customer and the entity collecting or using personal information. [225] Furthermore, many companies do not wish to implement any self-regulatory standards. [226] Even the few company policies that exist to protect personal information are often

invisible; citizens are not aware of them and cannot use them to access, check, or correct their personal information.

{85} Along with any of the options for enhancing privacy explored above, a federal oversight agency may be useful. To facilitate a better understanding of fair information practices the government could create a federal privacy entity to achieve and maintain the optimal balance between the benefits and harms associated with the unrestrained flow of personal data in the information age. [227] Such an entity would oversee public and private sector data use. It would also have the responsibility for informing, coordinating, or directing government data practices in accordance with applicable law. [228] The goal of a federal privacy agency would be to implement the Privacy Principles or other articulation of fair information practices at the national level. [229] The privacy entity could take any form, such as an independent federal regulatory agency, a federal agency without regulatory authority, or a non-government advisory entity. [230] Proposals for a public federal privacy agency have been articulated beginning with the HEW's recommendations for a federal privacy agency to regulate the use of all automated personal data systems. [231] However, to date, no such action has been taken.

{86} The federal government could take its cue from the *European Union Directive.* [232] The Council of Ministers of the European Commission adopted a directive "on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (the *European Union Directive*) [233] This approach to fair information practices in Europe has a significant structural difference from the Privacy Principles in that it transforms fair information practices into a framework of laws where member states must provide judicial remedies and adopt enforcement mechanisms for infringements of the privacy laws. While the United States' Privacy Principles provide for fundamental privacy protection, they are not founded in law.

{87} The cross-sectoral framework of the *European Union Directive* sets forth a consistent agenda for good business practices across all sectors, while the U.S. defines the adequacy of fair information practices on a case-by-case basis with sporadic legal rights and remedies for information privacy. The *European Union Directive* has transformed its fair information practices into a global implementation so that all member states establish laws to provide fair treatment of personal information. [234]

{88} The obligatory character of the basic principles of the *European Union Directive* provide a sound basis for collection of personal data for specified and legitimate purposes that are "not processed in a way incompatible with those purposes." [235] Although the U.S. Privacy Principles also articulate principles for determining, in any particular circumstance, whether an information practice is fair, the strengths of the *European Union Directive* lie in its comprehensive legal foundation and establishment of supervisory authorities to monitor the application of law pursuant to the *European Union Directive* and its application to transborder data flow.

VI. CONCLUSION

{89} The Principles for Providing and Using Personal Information offer a flexible method for enhancing informational privacy protection that can be adhered to across industry lines. Thus, to provide the most comprehensive set of fair information practices for personal information, the Privacy Principles should be used to guide legislators in drafting omnibus legislation that can be implemented in both the public and the private sector, to govern all information processing activities. The core principles of notice, consent, access, and integrity that the Privacy Principles promote offer a basis for individuals seeking to control their personal information. The Privacy Principles also provide the sensitivity to commercial needs of an information society by giving business the discretion to provide notice and obtain consent in a way that is adaptable to their industry.

{90} Electronic commerce will flourish only if we are able to agree to and implement fair information practices. [236] Different standards and varying jurisdictional approaches for the manipulation of personal information in the 21st Century will pose conflicts for data processing transactions. As long as the American privacy regulation advocates a targeted sectoral approach, comprehensive data protection in the U.S. will not exist.

{91} The obligation to maintain fair information practices in the Information Age is critical and a global solution must be adopted. The globalization of information processing activities and the European Union Directive have provided the U.S. with an impetus to action. Society must move forward beyond the debate over the intrusive nature of technological information systems to implementation of privacy protection on a national level. [237] Now is the time to seize the opportunity and take some form of action to ensure that privacy protection is a core element of advanced network communication systems.

ENDNOTES

[1] *See* MICHAEL ROGERS RUBIN, PRIVATE WRONGS, PUBLIC RIGHTS: THE COMPUTER AND PERSONAL PRIVACY 3 (1988).

[2] *See* JEFFREY ROTHFELDER, PRIVACY FOR SALE 106-110 (1992). The facts are based upon a true story from Jeffrey Rothfeder. Christina Danvers is a pseudonym. She requested anonymity to protect her privacy. *See id.*

[3] *See id.*

[4] *See* Louis Harris and Associates, Inc. *Interactive Services, Computers, and Privacy,* Doc. No. 11, at 70 (1994) (conducted for Privacy & American business).

[5] *See* 1994 Harris Survey, *supra* note 4, at 73-75.

[6] *See* Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?,* 44 FED. COMM. L. J.195, 205 (1992); *See* Jerry Berman et al., *Statement of the CDT,* before the Federal Trade Commission (1996).

[7] A series of electronic markers (trail) at each website or page generated by a user's browsing activities, including every page of access, newsgroups participated in, distribution lists received, e-mail addresses sent and received.

[8] Allows a Web site's server to place information about a user's visits on the user's machine in a file only that Web site can read.

[9] Programs, i.e. plugins, that run online and send and receive data from the user's environment; for example, in order for an ActiveX program to run on the Internet, the user must download code that will send information about the user's computer back to the ActiveX program.

[10] *See* NATIONAL INFORMATION INFRASTRUCTURE TASK FORCE (IITF). INFORMATION POLICY COMMITTEE, *Options for Promoting Privacy on the NII* (1997), *See* www.iitf.nist.gov/ipc/ipc-pub.html

[11] *See* Reidenberg, *supra* note 6, at 197-198.

[12] *See* RUBIN, *supra* note 1, at 60-61.

[13] *See* Joshua B. Sessler, *Computer Cookie Control: Transaction Generated Information and Privacy Regulation on the Internet*, 5 J.L. & POL'Y 627, 628 (1997).

[14] *See id.* at 628-629.

[15] *See* Reidenberg, *supra* note 6, at 203.

[16] *See id.* at 200.

[17] *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 14 (1997).

[18] *See id.* at 15.

[19] *See* Judith Beth Prowda, *Privacy and Security of Data*, 64 FORDHAM L. REV. 738, 751.

[20] *See id.*

[21] *See id.* at 740.

[22] *See* Sessler, *supra* note 13, at 639.

[23] *See* Prowda, *supra* note 19, at 740.

[24] *See* Joel R. Reidenberg and Francoise Gamet-Pol, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105, 112.

[25] *See* Rubin, *supra* note 1, at 65.

[26] *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES PRIVACY PROTECTION 314 (Charlottesville, VA: Michie, 1996).

[27] *See id.* at 320.

[28] *See* Reidenberg, *supra* note 6, at 202.

[29] *See* Reidenberg and Gamet-Pol, *supra* note 24, at 121-122; *See* Schwartz & Reidenburg, *supra* note 26, at 321.

[30] *See* Reidenberg, *supra* note 6, at 203; Schwartz, *supra* note 26, at 203.

[31] *See* Reidenberg, *supra* note 6, at 204.

[32] *See* Rubin, *supra* note 1, at 3.

[33] *See* Prowda, *supra* note 19, at 741.

[34] *See* Rubin, *supra* note 1, at 66.

[35] *See Rogan v. Los Angeles,* 668 F. Supp. 1384, 1388 (C.D. Cal.1987).

[36] *See id.*

[37] *See* Rubin, *supra* note 1, at 3.

[38] *See id.*

[39] *See id.* Discussed in Part 3 of text, *infra*.

[40] *See Griswald v. Connecticut,* 381 U.S. 479, 485 (1965)

[41] *See Stanley v. Georgia* 394 U.S. 557 (1969) (overturning a conviction under Georgia law for possessing obscene material in the home based upon an individual's right to privacy in their own home).

[42] *See NAACP v. Alabama* 357 U.S. 449 (1958) (striking down an Alabama ordinance requiring the NAACP to disclose its membership lists).

[43] *See Katz v. United States* 389 U.S. 347 (1967) (holding that the use of an electronic listening device attached to a phone booth violated his Fourth Amendment privacy right to unwarranted search and seizures).

[44] *See Roe v. Wade*, 410 U.S. 113 (1973) (recognizing that the right to privacy is broad enough to encompass a woman's right to terminate her pregnancy); *Griswald*, 381 U.S. at 479 (recognizing a right to privacy involving decision making about contraception).

[45] *See* Cate, *supra* note 17, at 56. The Supreme Court has continually held that when information is true and obtained lawfully, the state may not restrict its publication without showing a public interest. *See Smith v. Daily Mail Publ'g Co.*, 443 U.S. 97 (1979) (finding that a newspaper can constitutionally publish the name of a juvenile defendant if it is truthful and obtained lawfully); *Florida Star v. B.J.F.*, 491 U.S. 524 (1989) (holding that a newspaper can constitutionally publish the name of a rape victim if it is truthful and obtained lawfully).

[46] *See id.*

[47] *See* Schwartz & Reidenberg, *supra* note 26, at 7.

[48] *See Whalen v. Roe*, 429 U.S. 589 (1977).

[49] *See id.*

[50] *See id.*

[51] *See Roe v. Wade*, 410 U.S. 113 (1973).

[52] *See Griswald,* 381 U.S. at 479.

[53] *See id.*

[54] *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (Atheneum, 1967).

[55] *See id.* at 39.

[56] *See* U.S. DEPT. OF HEALTH, EDUCATION & WELFARE, SECRETRARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, *Records, Computers and the right of Citizens viii* (1973). The Advisory Committee was established in 1972 by Health, Education and Welfare Secretary Elliot Richardson in response to the growing public and private use of automated data systems containing information about individuals. Richardson was concerned that automated data systems presented a serious potential for harmful consequences, including an infringement of personal liberties.

[57] *See id.*

[58] *See* Joel R. Reidenberg, *Setting Standards For Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 498 (1995).

[59] *See id.* at 497. "Legal rules" refers to statutory mandates, regulatory obligations, and court decisions. "Industry norms" come from business sector aspirations and expectations. "Business practices" describes the actual treatment of information in commercial contexts rather than a legally mandated treatment. *See id.*

[60] *See id.* at 498.

[61] *See* Schwartz & Reidenberg, *supra* note 26, at 7.

[62] *See* Reidenberg, *supra* note 6, at 201.

[63] *See* Driver Protection Privacy Act, 18 U.S.C. § 2721 (1994); *See* Sessler, *supra* note 13, at 654.

[64] *See* Schwartz & Reidenberg, *supra* note 26, at 10; *See* Reidenberg, *supra* note 58, at 500.

[65] *See id.*

[66] *See* Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions,* 6 SOFTWARE L. J. 199, 209.

[67] *See* HEW Report, *supra* note 56, at 47. The provisions on the Code are based upon the notion that an information user should give an individual notice, and subsequently get their consent to use the personal information, and an individual should have the ability to access their file to correct false information to make sure the integrity of their personal information is being upheld. *See id.*

[68] *See id.*

[69] *See id.* at 42-44; *See also* Gellman, *supra* note 66, at 211.

[70] *See id.* at 43.

[71] *See* Reidenberg, *supra* note 6 at 201.

[72] *See id.* at 236-237.

[73] *See* Reidenberg, *supra* note 58, at 507-508.

[74] *See* Schwartz & Reidenberg, *supra* note 26 at 20 n1.

[75] *See* Reidenberg, *supra* note 58, at 528.

[76] *See* Gellman, *supra* note 66, at 211.

[77] *See* Privacy Act of 1974 Pub. L. 93-579, 88 Stat. 1896 (1974) (current version codified at 5 U.S.C. § 552a (1994)).

[78] *See id.* Both the House and Senate Committee that reported the legislation that become the Privacy Act of 1974 cited the HEW Advisory Committee's report.

[79] *See* 5 U.S.C. § 552a (1994).

[80] *See* S. Rep. No. 1183, 93rd Cong., Sess.1 (1974).

[81] *See* Gellman, *supra* note 66, at 206.

[82] *See* 5 U.S.C. § 552a(b) (1994).

[83] *See id.* at § 552a(d)(2)(B)(1).

[84] *See id.* at § 552a(i).

[85] *See* Sessler, *supra* note 13, at 658.

[86] *See* Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507-14 (current version codified at 5 U.S.C. § 552(a)(1994)).

[87] *See id.*

[88] *See* Raymond T. Nimmer, *The Law of Computer Technology* p 16.09 at 1628 (2d ed. 1992).

[89] *See* Jerry Berman & Janlori Goldman, Benton Foundation Project on Communications and Information Policy Options, *A Federal Right of Informational Privacy: the Need for Reform* 1, 14 (1984).

[90] *See* 5 U.S.C. § 552 (a).

[91] *See id.* at § 552 (p)(1).

[92] *See* Reidenberg, *supra* note 58, at 532; *See* Reidenberg, *supra* note 6, at 202-203.

[93] *See* Reidenberg, *supra* note 58, at 499; *See* Sessler, *supra* note 13, at 629; *See* Reidenberg, *supra* note 6, at 198; *See* Schwartz, *supra* note 26, at 220.

[94] *See* Reidenberg, *supra* note 6, at 210-211.

[95] *See id.* at 208; Prowda, *supra* note 19, at 751; *See* Reidenberg, *supra* note 58, at 500.

[96] *See* Schwartz, *supra* note 26, at 220-221.

[97] *See id.* at 220.

[98] *See* Electronic Communication Privacy Act, Pub. L. No. 99-508 100 Stat. 1848 (current version codified at 18 U.S.C. §§ 2510-2522, 2701-2711 (1994)).

[99] *See id.* at §§ 2510-2522.

[100] *See id.* §§ 2510-2522, 2702-2711.

[101] Transactional data is specifically excluded from the regulation's definition of "contents" and thus is not subject to the restrictions of the ECPA. *See* 18 U.S.C. § 2511(2). *See also* Schwartz, *supra* note 27 at 244 n74.

[102] *See id.* at § 2510(17).

[103] *See id.* at §§ 2701(b), 2702(a),(b).

[104] *See id.* at § 2510. Under the ECPA a provider of public communications services cannot disclose the contents of an email message without the consent of at least one of the parties. *See id.* at § 2511(3)(b). However, there is no specific restriction against the collection of personal information gathered from transactional data, nor is there a restriction against the duration of storage of such data. *See* Reidenberg, *supra* note 38, at 115.

[105] *See* 18 U.S.C. § 2703(c)(1)(A).

[106] *See* Telecommunications Act of 1996, Pub. L. No. 104-104, 11 Stat. 56 (1996) (current version codified at 47 U.S.C. § 222).

[107] *See id.* at § 222(c), 222(e).

[108] A common carrier has been defined as "any person engaged as a common carrier for hire in interstate or foreign commerce by wire or radio or an interstate or foreign transmission of energy." *See* 47 U.S.C. § 153 (1993).

[109] Common carriers are required to document caller identification information for interstate calls. *See id.* Customer Proprietary Information is defined as information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service that is made available to the carrier by virtue to the carrier-customer relationship and information contained in the bills pertaining to the service. *See* 47 U.S.C. § 222 (1)(A)(B).

[110] *See* 47 U.S.C. § 222.

[111] *See id.*

[112] *See id.*

[113] *See* Fair Credit Reporting Act, 18 U.S.C. § 1681b (1994).

[114] *See* Reidenberg, *supra* note 6, at 210.

[115] *See* 15 U.S.C. § 1681(b). The FCRA defines permissible purposes broadly encompassing employers, landlords, private investigators, and others. *See id.*

[116] *See* Reidenberg, *supra* note 6, at 211.

[117] *See* 15 U.S.C. § 1693 (1994).

[118] *See id.*

[119] "The Direct Marketing Association is the largest trade association for business interested in database marketing with more than 3600 member companies form the U.S. and foreign nations." The Direct Marketing Association, The Direct Marketing Association- Reception (visited Jan. 1998) <http://www.the-dma.org/lobby_pages/lobby-reception.html>

[120] *See* Sessler, *supra* note 13, at 638.

[121] *See* Reidenberg, *supra* note 58, at 518.

[122] *See* Direct Marketing Ass'n, Manual for Fair Information Practices (1994).

[123] *See id.*

[124] *See* Louis Harris & Ass'n., Equifax Report on Consumers in the Information Age 101 (1990).

[125] *See* Direct Marketing Ass'n, *Guidelines for Personal Information Protection*, at Art. 1 (1990).

[126] *See id.* at Art. 5.

[127] *See* Reidenberg, *supra* note 58, at 519.

[128] *See* Schwartz & Reidenberg, *supra.*note 26, at 321.

[129] *See* Reidenberg, *supra* note 58, at 519.

[130] *See id.*

[131] *See* 47 U.S.C. § 551 (1988 & Supp. V. 1993).

[132] *See* Prowda, *supra* note 19, at 757. Cable systems are a threat to consumer privacy because they have the capacity to collect and store information about the behavior, information needs, and entertainment preferences. *See* Nimmer, *supra* note 88, at p. 16.21.

[133] *See* 15 U.S.C. § 551 (1988 & Supp. V. 1993). *See also* Prowda, *supra* note 19, at 757-758.

[134] *See* Cable Television Consumer Protection and Competition Act, Pub. L. No. 102-385 § 20, 106 Stat. 1460, 1497 (1992) (current version codified in sections of the Communications Act of 1934, 47 U.S.C. §§ 151-613.

[135] *See id.* at 106 Stat. 1498.

[136] *See* Jerry Berman et al., *Statement of the CDT*, before the Federal Trade Commission (1996).

[137] *See id.*

[138] The National Information Infrastructure is more popularly known as the Information Superhighway.

[139] *See* NATIONAL INFORMATION INFRASTRUCTURE TASK FORCE (IITF). INFORMATION POLICY COMMITTEE, *Options for Promoting Privacy on the NII* (1997).

[140] *See id.* at 2.

[141] *See* Reidenberg, *supra* note 6, at 242-243

[142] *See id.*

[143] *See id.* at 239.

[144] *See id.*

[145] *See id.*

[146] *See* IITF, *supra* note 139, at 2.

[147] *See id.*

[148] *See* NATIONAL INFORMATION INFRASTRUCTURE TASK FORCE, PRIVACY WORKING GROUP, *Principles for Providing and Using Personal information* (1995).

[149] *See* IITF, *supra* note 139, at 2-3.

[150] *See* Principles, *supra* note 148, at 3. NII participants are any individual using network communication systems.

[151] *See id.* at 5. In some situations where the individual lacks sufficient bargaining power—purely contractual agreements between individuals and information users—privacy may not be respected adequately. In this case, "society should ensure privacy at some basic level in order to satisfy the Information Privacy Principle." *See id.*

[152] *See id.* "Not all subjectively held expectations will be honored as reasonable. For example, an individual who posts an unencrypted personal message on a bulletin board for public postings cannot reasonably expect that personal message to be read by only the addressee." *See id.*

[153] *See Cox Broadcasting v. Cohn*, 420 U.S. 469 (1975) (holding that a Georgia statute that made the

publication of a rape victim's name a misdemeanor is unconstitutional because the victim's name existed in official court records open to inspection). *See id.* at 495.

[154] *See* Letter from Electronic Frontier Foundation to Working Group on Privacy (July 6, 1994). The Electronic Frontier Foundation, formed in July 1990, is a nonprofit interest group "dedicated to preserving and enhancing civil liberties in digital media...focusing on privacy issues in the new electronics age." *See id.* at 1.

[155] *See id.* at 4-5.

[156] *See id.* at 6.

[157] *See id.*

[158] *See* Principles, *supra* note 148 at 5.

[159] *See id.*

[160] *See* Reidenberg, *supra* note 58, at 531.

[161] *See* Principles, *supra* note 148 at 6.

[162] *See id.*

[163] *See id.*

[164] *See id.*

[165] *See id.* at 6-7.

[166] *See id.* at 7.

[167] *See id.*

[168] *See id.*

[169] *See id.*

[170] *See id.*

[171] *See id.* at 9. A compelling public interest could be first amendment rights or law enforcement purposes. *See id.*

[172] *See id.*

[173] *See id.*

[174] *See id.*

[175] *See id.*

[176] *See id.* at 8.

[177] *See id.* The Privacy Working Group notes includes encryption as a technical control while including education and company policies against unfair information practices as managerial controls. *See id.*

[178] *See id.* at 11. Individuals should also be able to remain anonymous when browsing an electronic database to minimize a trail of transactional records. *See id.*

[179] *See id.*

[180] *See id.*

[181] *See id.*

[182] *See id.* at 12.

[183] *See id.*

[184] *See id.* at 10.

[185] *See id.* at 11.

[186] *See id.* For example, an individual can choose not to reveal their address, telephone number, or social security number by purchasing a product with cash.

[187] *See id.*

[188] *See id.*

[189] *See id.* at 10.

[190] *See id.*

[191] *See id.*

[192] *See id.* at 10.

[193] *See id.* at 12.

[194] *See id.*

[195] *See id.*

[196] *See id.*

[197] *See* EFF, *supra* note 154, at 8.

[198] *See id.*

[199] *See* Principles, *supra* note 148, at 3.

[200] *See id.* at 2.

[201] *See id.* at 3. The Privacy Working Group stated that the Principles will have to be balanced against societal benefits recognized in law such as, adherence to the First Amendment and law enforcement needs. *See id.*

[202] *See* Berman, *supra* note 136 at 2.

[203] *See id.* at 5.

[204] *See id.* at 8.

[205] *See id.* at 2.

[206] *See id.*

[207] *See* Principles, *supra* note 148, at 2. A hospital in a remote location will be able to send x-rays for review by a radiologist at a teaching hospital in another part of the country. The potential benefits are obvious. Yet, such benefits will not be gained if individuals refuse to send such sensitive data because they fear that the NII cannot insure that sensitive medical data will remain confidential or altered. *See id.*

[208] *See id.*

[209] *See id.*

[210] *See* IITF, *supra* note 139, at 50.

[211] *See id.* at 51.

[212] *See id.*

[213] *See id.* at 52.

[214] *See id.*

[215] *See id.* The Office of Management and Budget ("OMB") has statutory oversight responsibilities with respect to the Privacy Act of 1974 and could be used in the same way with regard to the Privacy Principles. *See* OMB, Privacy Implementation: Guidelines and Responsibilities, 40 Fed. 28951 (1975).

[216] *See id.*

[217] *See id.* at 53.

[218] *See id.* at 52.

[219] *See id.*

[220] *See id.*

[221] *See id.* at 53.

[222] *See* Reidenberg and Gamet-Pol, *supra* note 24, at 109.

[223] *See id.*

[224] *See* IITF, *supra* note 139, at 53.

[225] *See id.* at 54. In cases where the consumer does not have equal bargaining power with the company the consumer cannot negotiate to keep personal information private. For example, individuals cannot choose which credit bureau will maintain their credit reports and they do not have arms-length negotiation. *See id.*

[226] *See* Reidenberg and Gamet-Pol, *supra* note 24, at 120.

[227] *See* IITF, *supra* note 139, at 54.

[228] *See id.*

[229] *See id.*

[230]*See id.* at 54-62.

[231] *See* HEW Report, *supra* note 56, at 42; Gellman, *supra* note 66, at 212.

[232] *See* Directive 95/46/EC (1995). Directive of the European Parliament and the Council of Ministers of the European Commission on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[233] *See id.*

[234] *See id.*

[235] *See id.* at Art. 6(1)(b).

[236] Without fair information processes businesses and individuals will be reluctant to use network communication systems to send or receive sensitive data for fear that the data will not remain confidential or unaltered.

[237] *See* Berman, *supra* note 136.
