January 1996

Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness

Patricia Mell

Follow this and additional works at: https://scholarship.law.berkeley.edu/btlj

Recommended Citation

Link to publisher version (DOI)
https://doi.org/10.15779/Z386X0B

This Article is brought to you for free and open access by the Law Journals and Related Materials at Berkeley Law Scholarship Repository. It has been accepted for inclusion in Berkeley Technology Law Journal by an authorized administrator of Berkeley Law Scholarship Repository. For more information, please contact jcera@law.berkeley.edu.
ARTICLE

SEEKING SHADE IN A LAND OF PERPETUAL SUNLIGHT: PRIVACY AS PROPERTY IN THE ELECTRONIC WILDERNESS

PATRICIA MELL †

TABLE OF CONTENTS

I. INTRODUCTION .................................................................................................................. 2

II. SOCIAL AND TECHNOLOGICAL CONTEXT GIVING RISE TO THE ELECTRONIC PERSONA .......................................................................................................................... 11
   A. An Historical Perspective of Society, Information Management and the Law .......................................................... 11
   B. The Parameters of the Electronic Wilderness ........................................................................... 21

III. THE RELATIONSHIP BETWEEN PRIVACY AND PROPERTY ................................................................................................................... 26
   A. Development of Common Law Protection of Informational Privacy .......................................................... 28
   B. Development of the Constitutional Right to Informational Privacy ........................................................................... 34
   C. Development of Statutory Protection of Privacy on the Federal Level ................................................................................................................ 41

IV. ASSESSMENT OF THE INTERESTS COMPETING FOR USE OF THE PERSONA ................................................................................................................... 42
   A. Overview .......................................................................................................................... 42
   B. The Individual's Interest in His Persona ........................................................................... 46

© 1996 Patricia Mell.

† Associate Professor of Law, Detroit College of Law at Michigan State University; A.B. with Honors, Wellesley College, 1975; J.D. Case Western Reserve University Law School, 1978. The author wishes to express her appreciation to those individuals who gave their assistance, technical and otherwise, to this project. Individuals deserving of special thanks include the author's mother, Thelma W. Mell, a constant source of support and inspiration, and her aunt, Dr. Leatrice Emeruwa. In addition, thanks are extended to her colleagues at Detroit College of Law at Michigan State University: Professors John Apol, Susan Bitensky, Cynthia Starnes, Alvin Storrs and Nicholas Revelos; Professor Eileen Cooper, Librarian, Widener University School of Law; Eric Martin, Director of Computing Services, Detroit College of Law at Michigan State University; Charlotte Bynum, Associate Librarian for Reference Services, Detroit College of Law at Michigan State University; and Dr. Roland M. Smith, Vice President of Student Life, University of Delaware.
In the diverse society of the late twentieth century, institutions frequently make decisions about individuals based on personal information stored in computer databases.1 While such decision making

1. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information . . . " Whalen v. Roe, 429 U.S. 589, 605 (1977). In 1976, it was determined that the federal government maintained 3.9 billion files on private citizens. 45 U.S.L.W. 2161 (Sept. 28, 1976). See also PRIVACY PROTECTION STUDY COMM’N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 4 (1977) [hereinafter PRIVACY PROTECTION STUDY]. See also Bruce Clark, Note, The Constitutional Right to Confidentiality, 51 Geo. Wash. L. Rev. 133, 133 n.1 (1982). By 1989, that number had grown to on the average of 18 files on each individual on the federal level and 15 on the state level. ROBERT E. SMITH, PRIVACY AND HOW TO PROTECT WHAT’S LEFT OF IT 82 (1980). Private industry maintains significant amounts of information on individuals as well. In 1988, TRW, Trans Union and Equifax (the Big
is efficient and economical, there is neither consistent and generalized protection of the information contained in the databases, nor uniform recognition of the data's relationship to a specific individual. Despite almost fifty years of experience with the information-management ability of computers, society has not yet reformulated traditional notions of privacy, which restrict third-party access to personal information, to accommodate the tremendous storage capacity and instantaneous retrieval ability afforded by computers. Concepts of privacy, property and the individual's rights to both, take on a new dimension when the use of computer-stored information allows images of the individual—the "electronic persona"—to be created and used by a variety of third parties without the individual's knowledge.

The term "persona," derived from the Greek term for the mask worn by theatrical performers, is generally used to describe the various ways by which a person can be identified by personal information about him. The term is also used with reference to the right of publicity to describe the bundle of commercial values embodied in the identity of a person. The right of publicity comprises a person's right to own, protect and commercially exploit his own name, likeness and persona.


2. This was pointed out in the statement of purpose of the Privacy Act: "[T]he increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur for any collection, maintenance, use or dissemination of personal information . . . ." Privacy Act of 1974, Pub. L. No. 93-579, § 2(a)(2) (1974). For a diagram of several federal statutes which ostensibly protect the individual's privacy in specific contexts, see the appendix to this article [hereinafter App.]. See also Clark, supra note 1, at 135.

3. The first computer, called ENIAC, was developed by the U.S. Army in 1946. The next generation computer, UNIVAC, was developed for use by the Census Bureau for the 1950 Census. Encyclopaedia of Computer Science and Engineering 532 (Anthony Ralston ed., 2d ed. 1983).


Information has been defined as knowledge, facts and data. Webster's Ninth New Collegiate Dictionary (1985). It comes in a variety of forms, many of which are interchangeable—pictures, works, speech, writing—and in varying formats. Here the word is used to include any information presented electronically in any form, embodied in any format and handled by any computer processor.

The term "personal information" refers to any information which identifies or relates to a specific individual. See Laurence Tribe, American Constitutional Law, §§ 15-17, at 966 (1978). With respect to the term "persona," see Melville B. Nimmer & David Nimmer, Nimmer on Copyright § 1.01[B][1][c] (1978).

5. Nimmer & Nimmer, supra note 4, § 1.01[B][1][c].

6. Id.
In the computer context, however, the persona is an electronic compilation of bits of personal information concerning the individual. The persona is personal in nature in that it can be associated with a specific individual by name or any other identifier. Identifiers are words or symbols which identify a specific person. Examples of identifiers include an individual’s name, social security number or account number. Since computer records are often filed under these identifiers, they are the key to accessing files which hold personal information concerning a specific individual. In this article, the term “persona” is used to signify a personal information file electronically stored, which, by virtue of at least one “identifier,” relates the personal information to a specific person.

The electronic persona can perform several functions simultaneously for different parties. It is a manifestation of an individual’s life—his identity. For government entities, the persona is the resource used as the basis of decision making about individuals and forecasting trends for groups of their constituents. As a consequence of its use by government, the persona becomes a public resource reflecting the operation of government. Finally, it can be the resource commercial entities use in decision making and as a source of revenue. These coextensive layers of interests necessarily blur the lines between that which can be restricted from public access and that which should be sheltered from unrestricted public view. This article will examine the manipulation of information in these contexts, focusing on the effect of this information transfer upon the individual. The lack of consistent rules governing its use makes the electronic wilderness a land of perpetual sunlight for the persona.

Uncertainty concerning the nature of the electronic milieu exacerbates the problem of determining the scope of protection to be afforded the electronic persona. The electronic wilderness created by computer technology lacks dimension in the usual sense, but it is vast and very real. The collection and dissemination of an individual’s personal information to third parties remains largely untamed by law.

We have not consciously created such images of our personae. They are a function of the electronic trail of the information we leave in the wake of our use of any service that electronically records and/or

10. Id. at 11-12.
stores information concerning our transactions. These separate images, stored by those with whom we deal directly, can be collected, compiled and matched with other pieces of information about us by third parties in a secondary information market. The same persona, being both public and private, is then used by institutions to make decisions about each of us.

In a "primary information market," the individual voluntarily discloses personal information in exchange for some benefit. For this reason, most of the early literature in this area dealt with the use of personal information as an issue of contract between the individual and the provider. By contrast, the "secondary information market" describes information collected from any information-producing sector, which is used either by organizations with which the individual has not dealt directly or for purposes which the individual could not have foreseen. This would include the activities of credit reporting agencies, employers, governments or any other organization or person who uses information services. The individual typically has no idea that this information makes its way into the secondary market to be used for

11. This would include such transactions as using credit cards; getting or losing a driver's license; taking standardized tests for school or for employment; getting employed or fired; contributing to charitable or political causes buying or selling; getting married or divorced; paying taxes or not; having children; paying bills promptly or not.

12. For the most part, the flow of information away from the individual to third parties is carried out almost without any involvement by the individual. The flow of information was described in the following manner:

The private and public bureaucracies are the repositories of the planning power in the economy. . . . The two bureaucracies coordinate with each other through a blizzard of forms and reports, and through the revolving door between industry and government. Expertise is exchanged through the purchase of R&D, consulting, and management, and . . . extracted by regulatory commissions, requested by Congressional committees, offered gratuitously through lobbying, or simply transferred as a result of people changing jobs.


13. Much of the information about the individual is collected by governmental agencies, both state and federal, pursuant to their administrative or regulatory function. In this respect, the information is "public," meaning that it is often freely available to any seeker. These personae can consist of any number of combinations of intimate, embarrassing or purely public, non-sensitive information about the individual. On the other side, there is some authority for the proposition that any attempt to distinguish between the private and the public is futile. See generally Howard Radest, The Public and the Private: An American Fairy Tale, 89 ETHICS 280 (1979); Duncan Kennedy, The Stages of the Decline of the Public/Private Distinction, 130 U. PA. L. REV. 1349, 1351-57 (1982).


15. See id.
Resolution of this problem becomes of acute concern as we begin to settle the wilderness with our electronic personae.\textsuperscript{17} Since personae are created for third parties' purposes, all individuals can have more than one persona, each one held by a different third party.\textsuperscript{18} Indeed, each user of personal information is free to manipulate the information into any desired configuration.\textsuperscript{19} The programmer's directives could require that certain information be given emphasis while other information be downplayed.\textsuperscript{20} The distorted persona goes to the wilderness. In pre-computer days, witnesses, various paper references and photographs could all effectively counter inaccurate references concerning the individual.\textsuperscript{21} As computer storage becomes increasingly inexpensive, relative to the cost of storing paper records, the individual may find himself unable to challenge a computer-compiled history.\textsuperscript{22}

On the other hand, centralization of private information and its preservation in computer memory may decrease illegitimate leaks of that information. Those with access to personal histories will see much more of them than was usually the case when the information was contained in printed records, but with computerization of access restrictions, fewer

\begin{footnotesize}

\begin{itemize}
  \item [16.] Id.
  \item [17.] See discussion \textit{infra} part V. concerning the nature of the electronic persona.
  \item [18.] This is particularly true since there is no central repository for all files. There have been at least two attempts to create a central repository for federal information files. Both were defeated. See \textit{Smith}, supra note 1, at 85. \textit{See also Ellen Alderman \& Caroline Kennedy, The Right to Privacy} 326 (1995).
  \item [19.] See discussion \textit{infra} part II.B. concerning how the information files are created.
  \item [20.] Michael, supra note 19, at 280.
  \item [21.] Id.
  \item [22.] Martin Lee Dement spent two years in a Los Angeles county jail because of a botched use of the California Automated Latent Fingerprint System, which uses a computer to identify the suspect's fingerprints. Manual checks of another suspect's fingerprints finally cleared Dement. \textit{Tom Forester \& Perry Morrison, Computer Ethics Cautionary Tales and Ethical Dilemmas in Computing} 137 (2d ed. 1994). \textit{See also Michael, supra note 19, at 274-76.}
\end{itemize}

\end{footnotesize}
curious eyes may have knowledge of any part of the private history of the individual.  

The electronic persona is then autonomous, commodified into the physical world, directing from the electronic wilderness the actions and transactions in which we are involved. It can survive our deaths, exist totally without our awareness and be unresponsive to sudden changes in our society and lifestyles. To the user of this information, who will seldom meet the individual face-to-face, the electronic persona becomes the "real person." The outsider will see and use the persona to make decisions about the individual's life. In effect, the individual becomes secondary to the accuracy of the persona. No one or two pieces of information can tell the entire story of the individual's life. Nor do the separate pieces of information necessarily identify the individual directly. At some point, however, the combinations of personal information can form seemingly complete "images" of the individual. At that critical moment, an electronic persona is born and its reality overtakes our own.

Much computer-stored personal information is used without the knowledge or consent of the subject individuals. While surveys suggest that Americans would prefer to control the use of information collected about them, as a society we have failed to successfully identify either the interest being infringed upon by nonconsentual access to personal information, or the proper balance to be assigned to those interests competing for use of it.

23. ALAN WESTIN & MICHAEL A. BAKER, DATA BANKS IN A FREE SOCIETY (1972). See also Harris, supra note 19, at 34-35 (discussing human resource managers' increasing awareness of the need to restrict access to personal employee information).
25. "If derogatory information is stored and used against a man long after an event," individuals could never have a "new start." "People tend to forget and forgive, computers do not." Toby Solomon, Personal Privacy and the "1984" Syndrome, 7 W. NEW ENG. L. REV. 753, 755 (1985).
26. See discussion infra parts IV.A-C. concerning the difference in treatment of solitary files and compilations of records.
27. See ALDERMAN & KENNEDY, supra note 18, at 326.
Largely unprotected by law, the persona seeks shade from the light of disclosure under the existing patchwork of protections based in the United States Constitution, statutes regulating government and private record collectors, and common law concepts of privacy which regulate the use of information by private industry and individuals. Many authors discuss the interest to be protected in personal information under the rubric of privacy. However, the fact that privacy is an evolving concept, burdened with several definitions, complicates this approach. For example, there is no consensus as to whether privacy is a property right or a personal one. Also, there is no definitive solution as to how

29. See infra App.


31. As stated by Professor Zimmerman, "[t]he phrase a 'right to privacy' as used in law has almost as many meanings as Hydra had heads." Diane Zimmerman, False Light Invasion of Privacy: The Light that Failed, 64 N.Y.U. L. Rev. 364, 364 (1989). The following definitions are but a few of the many penned during the last three decades:

- "[P]rivacy exists where the persons whose actions engender or become the objects of information retain possession of that information, and any flow outward of that information from the persons to whom it refers (and who share it where more than one person is involved) occurs on the initiative of its possessors."

- "[P]rivacy is the condition of human life in which acquaintance with a person or with affairs of his life which are personal to him is limited." Hyman Gross, The Concept of Privacy, 42 N.Y.U. L. Rev. 34, 36 (1967).

- "[P]rivacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967).

- "[P]rivacy is a limitation of others' access to an individual .... [A] person enjoys perfect privacy when he is completely inaccessible to others .... [I]n perfect privacy no one has any information about X, no one pays attention to X, and no one has physical access to X." Ruth Gavison, Privacy and the Limits of Law, 89 Yale L. J. 421, 428-29 (1980).

- "[P]rivacy denotes a degree of inaccessibility of persons, their mental states, and information about them to the senses and surveillance of others." ANITA ALLEN,UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY 34 (1988).

The traditional inquiry in the United States would separate alleged breaches of the individual's privacy into two camps: one for breaches by the government, and another for breaches by private concerns. Many of these definitions do not make such a distinction.

32. "Warren and Brandeis attempted to carve out an interest—viewed by some as a 'personality interest' and by others in more proprietary terms—without concomitantly attempting a clear description of that interest." Sheldon Halpern, The "Inviolate Personality"—Warren and Brandeis After One Hundred Years: Introduction to a Symposium on the Right of Privacy, 10 N. Ill. U. L. Rev. 387, 389 (1990). "The simple word 'privacy' has
privacy should be applied to a non-physical intrusion in an electronic medium and the appropriation of the information stored there. The use of privacy as the primary source of protection is particularly problematic because in this new electronic medium, an individual's privacy is alienable.

Society requires a definition of privacy that recognizes the fluid relationship between the electronic persona and traditional Western conceptions of privacy. Rapid societal changes produced by increased use of computer technology to manage the electronic persona exacerbate this dilemma. The technology of computer-mediated information management has confounded traditional discourse by the creation of a new dimension of human activity and interaction. Just as the real person wearing the Greek "persona" became the character depicted by the mask, the "facts" about the modern individual become lost in the presence of the electronic persona created by collectors of information about him.

The American pioneers tamed the wide open spaces of the western United States by erecting fences to determine the ownership of their private property. Boundaries must be established in the electronic wilderness delineating the public information that can be fully disclosed and the electronically-stored personal information that should be protected as the individual's private property.

While there is great disagreement as to what information should be protected from disclosure, there is a general consensus that individuals do have a right to some degree of privacy, even in the electronic

---

33. In the United States, the source of information privacy is the Fourth Amendment, which guarantees the individual's privacy in his home and papers. U.S. Const. amend IV. For a discussion of the Fourth Amendment, see generally Nelson Lasson, The History and Development of the Fourth Amendment to the United States Constitution (1970).

34. See discussion infra part V.A.2. Since the subject of a personal information file often does not know that an electronic persona concerning him is being either compiled or used, he can be divested of an electronic persona without his knowledge. Since the persona is identifiable to a specific individual, the electronic persona should be recognized as being "owned" by that person. In this respect, the electronic persona is similar to the name and likeness aspects recognized by the appropriation tort as delineated by Prosser. See William L. Prosser, Privacy, 48 Cal. L. Rev. 383, 406 (1960). The quality of being divested makes the persona personality—property. This ownership is not necessarily exclusive. See discussion infra part IV.F.

35. Each person is aware of the gap between what he wants to be and what he actually is, between what the world sees of him and what he knows to be his much more complex reality ... Every individual lives behind a mask in this manner, indeed the first meaning of the word "person" etymological was "mask," indicating both the conscious and expressive presentation of the self to a social audience.

Westin, supra note 31, at 33.
wilderness. That consensus was summarized in 1973 as five rights an individual would regard as basic in a consistent and generalized personal information protection plan. Those rights are: 1) the ability to discover the existence of personal information files; 2) the right to know how the record holder intends to use the personal information and how broadly the information will be disseminated; 3) the right to withhold consent if the record holder intends to disclose the information more broadly than originally contemplated; 4) the individual's ability to access personal information files and the opportunity to correct any inaccurate information; and 5) the right to adequate security and to update outmoded personal information. Implicit in these rights is an individual's right to control a record holder's disclosure of personal information. These five rights will be used in this article as the basic assumptions for conceptualizing the property right in the electronic persona.

Several privacy definitions recognize the individual's right to control personal information. In this article, privacy is the legally recognized power of an individual (group, association or class) to both 1) regulate the extent to which another individual (group, class, association or government) may access, obtain, make use of or disclose a persona concerning him, or concerning those for whom he is personally responsible; and 2) monitor and correct the accuracy of the persona compiled concerning him or those for whom he is personally responsible. This definition incorporates the five rights and demonstrates the situations in which the individual might want to control disclosure of personal information.

In this article, I describe the scope of the individual's right to privacy as being a type of property right in his electronic persona. To clarify the need for such a property right, I review the social and technological use of the individual's persona in its historic context. To define the parameters of that property right, I consider the traditional relationship between privacy and property as protection of the persona.

37. Id.
38. For examples of these definitions, see supra note 31.
39. This definition takes into consideration the individual's "control over... the intimacies of personal identity[i]... intimacy, identity, and autonomy" as limitations and applications of the concept of privacy. Tom Gerety, Redefining Privacy, 12 HARV. C.R.-C.L. L. REV. 233, 281 (1977).
The electronic persona, in its easily accessible and malleable form, presents many conceptual problems for the current law, which seeks to balance use of the persona among those groups competing for superior rights to it. I identify four entities with potentially conflicting priorities in the use of the persona: individual, government, public and commercial groups. The tension between these interests has created a cumbersome and ineffective system of personal information protection. The gaps in protection that the existing system affords the individual are diagrammed in the Appendix.

Finally, I describe a new property right in electronic personae by suggesting a joint evolution of our traditional notions of privacy and property. I recommend a solution to the primary impediment to this evolution that borrows from existing intellectual property traditions to resolve the public-private dichotomy of the electronic persona. This joint evolution should result in the individual's recognized property interest in personal information collected about him by public or private institutions, and the balancing of the interests in use or disclosure of such information by ranking the purpose of the disclosure in terms of its importance to society.

These recommendations suggest one way in which the individual can obtain uniform power to restrict both the collection and disclosure of his persona, and present a method to assure the information's contextual accuracy as it passes from primary collectors to secondary users.

II. SOCIAL AND TECHNOLOGICAL CONTEXT GIVING RISE TO THE ELECTRONIC PERSONA

A. An Historical Perspective of Society, Information Management and the Law

History indicates that one of man's perpetual battles has been the resolution of the discontinuity between advancing technology and man's ability to control it. At each stage of human society's development, new
technology forced re-evaluation of the premises under which society operated and the assumptions upon which society balanced the new technology with the perception of basic needs.\textsuperscript{44} The law generally developed to enforce those assumptions.

Technology changed society from an agricultural, pre-industrial stage to the present post-industrial, information society.\textsuperscript{45} Supported by a triad of different infrastructures—transportation, power and communication (information)—human society changed with the technological shift in predominant infrastructure.\textsuperscript{46} The economy of pre-industrial society was based on the extraction of natural resources and their market distribution. Industrial society’s economy was based on goods-producing industries; the extraction of resources was necessary for the production of goods but was not itself the focus of this economy. The increased interaction between energy and transportation systems allowed the expansion of U.S. industries along rivers and the Great Lakes regions.\textsuperscript{47} This made society solidly industrial; wealth and economic growth was based upon the energy-consuming manufacture of goods and their wide distribution through a well developed transportation system.\textsuperscript{48} In contrast, the post-industrial economy is based not on the production of goods but upon the selling of services, such as education, health, social services, professional services and scientific research and development.\textsuperscript{49}

While information has always been a core resource\textsuperscript{50} until the present stage it was largely relegated to the position of supporting other resources. However, in the present service economy, information has become an increasingly valuable commodity. This shift has put pressure

\textsuperscript{44} Id.

\textsuperscript{45} \textit{See generally} Daniel Bell, \textit{The Coming of the Post-Industrial Society} 47-119 (1973). Bell cites three stages in the development of society: the pre-industrial, the industrial and the post-industrial or information society. \textit{Id.} For the purposes of this article, which investigates the status of personae in the United States, these three periods correlate roughly to the years 1750 to 1850 for pre-industrial; 1850 to 1950 for industrial; and 1950 to the present as the post-industrial or information age.


\textsuperscript{47} \textit{Id.} at 22.

\textsuperscript{48} For a more detailed account of this development, see Bell, \textit{supra} note 45, at 47-120.

\textsuperscript{49} Each stage of society required a different type of service. Pre-industrial society was based in large part on physical labor, while the industrial society used services, such as transportation or financial services, to support the production of goods. The human services that comprise the basis of post-industrial society, however, are human services based on the codification of human knowledge. \textit{Id.}

\textsuperscript{50} \textit{See} Anthony G. Oettinger, \textit{Information Resources: Knowledge and Power in the 21st Century}, 209 Science 191, 191 (1980). The society of each stage of development was “an information society and every organization an information organization...” \textit{Id.}
on the maintenance of the individual's privacy, in that information about the individual has itself become increasingly valuable.\textsuperscript{51} The computer has exacerbated this problem through its capacity to disclose a large amount of personal information to a large number of unrelated individuals in a very short amount of time.\textsuperscript{52} Property law had balanced the potentially conflicting needs for information and privacy.\textsuperscript{53} Consequently, the concepts of privacy and property as barriers to societal intrusion became inexorably entwined.\textsuperscript{54} Philosophical and legal conceptions of privacy reflected society's attempt to adjust to technological changes. As society intruded more into the lives of its citizens, the number of laws protecting the individual's privacy proliferated.\textsuperscript{55}

In contrast, pre-industrial society's need for information was comparatively limited and purely local. The economy was dependent upon the value and quality of its natural resources, which were reaped through manual labor.\textsuperscript{56} Its primary needs for information were based on agriculture.\textsuperscript{57} The majority of citizens did not live in cities or pursue an

\textsuperscript{51}. In 1988, the three largest credit bureaus generated the following revenues from selling credit information about private citizens: TRW, $335 million; Trans Union, $300 million; and Equifax, $259 million. For Equifax, the sale of credit information constituted only 35% of its overall revenues but made up 75% of its profits. Rothfelder, supra note 1, at 80. See also Oettinger, supra note 50, at 194 (comparing gross revenues of information industries over a seven-year period).

\textsuperscript{52}. Cf. Jim Seymour, PC MAG., August 1991, at 89 ("[P]rivacy is not a 'computer problem,' but a human and societal one, amenable to exactly the same kinds of remedies we apply to other societal problems.").

\textsuperscript{53}. See discussion infra part III.B. concerning the premises of Fourth Amendment protections against warrantless search and seizure as protection of the persona. Unauthorized access to information in a "protected" area is founded in recognized tenets of possession and ownership of the information. Ownership of the information necessarily makes the information property. See also Wendy Gordon, On Owning Information: Intellectual Property and the Restitutional Impulse, 78 VA. L. REV. 149, 150-51 (1992) (discussing the initial reluctance of the courts to create common law property rights in intangibles).


\textsuperscript{55}. The vast majority of laws passed to protect the individual's privacy have been passed during the last 30 years. These years correspond to the time during which institutional intrusion into the individual's life has reached an unprecedented frequency. See infra App.

\textsuperscript{56}. Bell, supra note 45, at 124 (citing HISTORICAL STATISTICS OF THE UNITED STATES 14, 74 (1960)).

\textsuperscript{57}. In 1860, approximately 42% of labor was in agricultural industries and 5% in information industries. In 1980, the positions occupied by the two industries were reversed, with information industries holding 46% and agricultural only 2%. Porat, supra note 12, at 189 fig. 7.2.
education beyond grade school. Military registration was not compulsory and there was no federal income tax. As such, there was little contact between the average citizen and the federal government. commercially, it was a cash and face-to-face transaction society. Very few people owned property, and local banks and merchants relied on the community reputation of the individual to guide them in the few consumer or commercial credit transactions of the time. Very few people carried insurance of any kind, and medical records rarely existed beyond the doctor's office. If records needed to be exchanged, they were paper records sent by mail. Records were maintained by the organization with which the individual dealt, and there was no substantial market for the exchange of information between different organizations.

Until the end of the Revolutionary War, there was no federal government to collect records and very little organized credit was extended by institutions. With the exception of the U.S. Census, there was no centralized governmental collection of information regarding individual U.S. citizens. Record collection was purely a local matter. People rarely left the town in which they were born. The absence of a need for record collection provided effective protection for the individual's privacy.

Despite the lack of interpersonal privacy during the pre-industrial period, privacy was considered to be an attribute of man in nature. John Locke stated that "every Man has a Property in his own Person. This no Body has any Right to but himself." This suggests that an individual has exclusive rights to the use of his person and can preclude its use or

58. The current system of compulsory education in the United States is the product of a system of state laws which require attendance for children at either a public school or at some other learning institution. Lawrence Kotin & William F. Aikman, Legal Foundations of Compulsory School Attendance 9 (1980). The universality of the requirement has been traced to the early 20th century and the perceived "need to integrate foreign immigrants quickly and to the subsequent 'Americanization' movement of the early 20th century," id. at 26-27.

59. The federal government's ability to tax the income of U.S. citizens was authorized by the enactment of U.S. Const. amend. XVI.

60. The first credit reporting agency was not created until 1869 when post-Civil War migration made it a necessity. See James B. Rule, Private Lives and Public Surveillance 180-81 (1973).

61. The United States Census was first taken in 1790. The authority to take the census was provided by Article I, Section 2 of the U.S. Constitution which provided for the taking of a population census "within three Years after the first Meeting of the Congress of the United States, and within every subsequent Term of ten Years." U.S. Const. art. I, § 2. It was the first of the modern censuses to be conceived as an integral part of the machinery of government. 6 The Encyclopaedia Americana: International Edition 169 (1981).


63. John Locke, Two Treatises of Government 328-29 (Peter Laslett ed. 1965).
even knowledge of it from third persons. Locke continues, “that with which he mixes his labor becomes his property.”

Locke did not consider the individual to be isolated and without interaction with society. Rather, “all that [the person] becomes and all that he makes are part of his own person.” The pre-industrial period witnessed a “growth of individuality” and fostered “the belief that one’s actions and their history ‘belonged’ to the self which generated them and were to be shared only with those whom one wished to share them.”

Industrial society required a greater quantity and quality of information than did pre-industrial society. The need for labor centered in urban areas, whose burgeoning industries encouraged the abandonment of the frontier’s wide open spaces for the city’s concentrated living spaces. The information needed was more complex and technical in nature and required greater reliance on machines to boost production and efficiency. Ralph Waldo Emerson recognized the difficulty of maintaining control over one’s identity when actively involved in society. He stated, “[p]erson makes event, and event person . . . . The event is the print of your form . . . . Events are the children of [one’s] body and mind . . . . [They] grow on the same stem with persons; are sub-persons.” One commentator interpreted this to mean that “[o]nce man’s power of self-transcendence is posited, it becomes impossible to confine the self within marked-off limits and to say positively, ‘This is the self, this is a man’s “own person,” and the rest is not self.”


65. This was the interpretation suggested in Konvitz’s article. Id.


67. See Bell, supra note 46, at 22.

68. In a sense, the individual’s loss of physical seclusion was a double-edged sword, one that provided both more and less privacy. Western pioneers had privacy born of their physical seclusion from others in the vast spaces of the West. As people left the family farm for the city and factory jobs, however, this seclusion was no longer possible. Robert Copple described this forced exposure as “the impetus for the creation and adoption of . . . legal means to protect personal privacy and to officially recognize the right to a . . . degree of social distance.” Robert F. Copple, Privacy and the Frontier Thesis: An American Intersection of Self and Society, 34 AM. J. JURIS. 87, 88 (1989). A similar phenomenon, reflected in the loss of the extended family and population mobility of the 20th century, was cited by Alan Westin as creating “greater situations of physical and psychological privacy.” WESTIN, supra note 31, at 21.

69. See Bell, supra note 46, at 22.

70. Ralph W. Emerson, Essay on Fate, in THE CONDUCT OF LIFE 40-41 (1899).

71. Konvitz, supra note 64, at 275.
The development of the telegraph in 1844 exacerbated this trend, since neither distance nor time encumbered this means of information transfer. By the time Warren and Brandeis wrote The Right to Privacy in 1890, the individual’s ability to shield information about himself from the public was beginning to erode in response to society’s increased need for more information. The invention of the telephone in 1876 was followed by the inventions of the radio, television and computer. All of these modes of collecting and distributing information were in use by the first half of the twentieth century. As society became more adept at manipulating these communications technologies, it developed new ways of observing the individual. The increasing ability of information technology to pervasively intrude during this period led to the first modern cases concerning government surveillance.

By the turn of the century, the largest collector of personal information concerning individuals was the federal government pursuant to its decennial census. But approximately forty percent of the population continued to work on the family farm, twenty-eight percent worked in the developing industries and the remaining thirty-two percent worked in services and in the budding information sector. Commercial agencies specializing in the collection of personal information about individuals began to grow in earnest, as did government information with the passage of the national income tax amendment. However, despite institutional encroachment upon the

72. The invention of the telegraph has been referred to as the birth of modern society’s information infrastructure. See, e.g., Bell, supra note 46, at 20.
73. See id.
75. Oettinger, supra note 50, at 191.
76. The result was a merging of the computer and communications industries in powerful ways that challenge society’s traditional notions of public versus private information. Id. at 192.
77. See infra text accompanying notes 204-07(discussing Olmstead v. United States, 277 U.S. 438 (1928)).
79. See Porat, supra note 12, at 189 fig. 7.2.
80. By 1971, there were at least 2,000 credit bureaus and TRW held over 30 million files. Rule, supra note 60, at 181. The first modern credit card was Diners’ Club card issued in 1950. Diners’ Club was followed shortly by American Express and Carte Blanche in 1958. Id. at 226. By 1971, American Express and Diners’ Club had 3.5 million and 2 million cardholders, respectively. BankAmericard (predecessor to VISA) was the earliest bank-based credit card, starting in 1959. By 1971, BankAmericard had over 28 million cardholders. Id. at 230. For a general discussion of credit bureaus, see also Smith, supra note 1, at 42-43.
81. U.S. Const. amend. XVI.
individual’s solitude, the individual’s privacy was protected from mass collection, matching and disclosure by cumbersome technological limitations associated with information management. For example, in the paper-based record keeping system, pragmatic file-management issues deterred organizations from endeavoring to compile vast quantities of information about individuals.

This period saw the development of tort theories of privacy, intellectual property doctrines governing the commercial exploitation of the persona, and an increased use of the Fourth Amendment to restrict the government’s right to invade the individual’s domain. The consequence of the increased institutional need for information made its possession the determining factor in the right to use the information. With few exceptions, the individual’s ability to prevent collection and disclosure of the information ended once the information was in the hands of a third party.

In its third stage of development, society has experienced a shift in its economic base from industry to information. The basis of the economy is now the selling of human and professional services. This transformation has given rise to such labels as the “Information Revolution,” the “Information Society,” or the “Post-Industrial Society” to describe the late twentieth century. In this society, institutions administer to the needs of a widely divergent population. The drive for the efficient determination of needs and allocation of resources mandated the replacement of personal face-to-face evaluation with information-based decision making. The magnitude and diversity of

---


83. Miller, Challenge, supra note 82, at 1108-09.

84. See infra parts III.A.-B. for a discussion of the origins of constitutional, common law and intellectual property theories in the United States for protection of the persona.

85. Theories used to prevent the use of personae varied from agency to contract and trust theories. The tort concept of privacy could compensate individuals under certain circumstances. For a discussion of privacy and government agencies, see infra part IV.C.

86. See generally Bell, supra note 45, at 47-119.

87. “Services exist in all societies, but in pre-industrial societies, they are primarily domestic services. In industrial societies, these are ancillary to the production of goods, such as transportation, utilities, and financial services. In post-industrial societies, the emphasis is on human services (education, health, social services) and professional services . . .” Bell, supra note 46, at 22.

88. See generally id. See also Oettinger, supra note 50, at 192.

89. Since its invention in the 1940s, the computer has become a fundamental tool in the operation of government, commercial and academic industries. Institutions as varied as the Federal Reserve Bank, the Department of Defense, the local community college and department stores all base their information management upon a computer or a system of computers. The growth of the technology in this field has made it possible for the office or
the population has isolated the government from its constituents while requiring greater contact from the government in the form of government-backed support.\footnote{See Smith, supra note 1, at 90.} A significant consequence of the variety and concentration of institutional relationships with individuals has been the pervasiveness of persona collection and maintenance.\footnote{See Countryman, supra note 30, at 837-39.} The balance between the institution seeking better information and the individual seeking to control his persona has shifted in favor of the institutions due to the anonymity with which the institutions operate.\footnote{Bell, supra note 46, at 21.} This imbalance prompted post-industrial society’s label, the “dossier society.”\footnote{Id.}

The merging of telephone and television with computers has resulted in the development of a flexible and diverse international information-exchange system that allows the nearly instantaneous transfer of information through cables, satellites, microwave relays and fiber optics.\footnote{“In 1951, Univac I, the first commercial computer, cost $701,000 and occupied 10 cubic feet; the same amount of computing power today can be stored in a one centimeter square silicon chip that costs $19.” James V. Vergari & Virginia Shue, Fundamentals of Computer—High Technology Law 247 (1991).} This system has five major aspects: data processing networks, information banks and retrieval systems, teletext systems, facsimile systems and interactive on-line computer networks.\footnote{Id.} While each aspect can divest the individual of control over his persona, this article will focus on information banks and retrieval systems.

Just as the advent of mechanized industry and the subsequent rise of the bourgeoisie once transformed Western societies, the consistent downward spiral in the pricing of information technology and of access to information entails a pervasive and profound social transformation.\footnote{90. The federal government collects an average of 18 files on each man, woman and child in the United States. SMITH, supra note 1, at 85.} Since the system is driven by the need for information disclosure, the resource user assumes a great deal of power over the substance of the persona. With the exception of anti-discrimination laws and First...
Amendment protections, the persona user makes his own determination as to what information may be relevant to his purposes. If the individual has requested a service from the persona user, he is generally obliged to either disclose the information or forego the desired benefit, whether or not the information request is objectionable. Consequently, "unless an agency or private organization chooses to restrain itself in the public interest, no one is in the position of answering whether the benefit of having the information outweighs the intrusion upon privacy of getting it."  

The anonymity of the information system's operation divests the individual of any real power over the use of his persona and shifts to the user the ability to shape the individual's "public identity" to the institution's specifications. Operating on the theory that more information is always better, the record-keeping institution is not necessarily driven to assure the personal information's substantive accuracy. Consequently, in the absence of specific statutory authority, a false persona may continue to exist—to the individual's detriment. In *Tarver v. Smith*, information concerning Mrs. Tarver was collected by the state office of social services when Mrs. Tarver became ill and was hospitalized. The Juvenile Court, after reviewing a report by her caseworker that contained "assertedly derogatory contents," including an allegation of child neglect, placed her children temporarily in the custody of the Department of Public Assistance. A second hearing exonerated Mrs. Tarver and returned her children to her, but the caseworker's report remained in her file at the Department of Public Assistance. The Washington Supreme Court determined that the individual had no power to eliminate a false record not directly related to the function of the agency-record user. Thus, the individual had no right or legal ability to prospectively prevent damage from inaccurate records. Such a policy...
fails to protect the individual in his efforts to limit the impact of records on his life. The United States Supreme Court refused to review her case and the caseworker’s report remained in her file.\textsuperscript{104}

Reposing unfettered power in the record keeper divests the subject of the record of any ability to protect his interest in preventing the record’s disclosure. The individual therefore has no power to control or prevent disclosure of personal information held by third parties to other institutional information-seekers.\textsuperscript{105} \textit{United States v. Miller} exemplifies this problem; here the United States Supreme Court held that a bank customer had no legitimate “expectation of privacy” in his bank records and thus no protectable interest for the Court to consider.\textsuperscript{106} Miller was suspected in two instances of illegal liquor violations. Pursuant to a grand jury subpoena, and without Miller having been notified, copies of his checks and bank statements were either shown or given to Treasury agents. Miller’s attempt to have the evidence excluded was unsuccessful. The Court reasoned that because checks were an independent record of an individual’s participation in the flow of commerce, they could not be considered confidential communications.\textsuperscript{107} The account record, moreover, was the property of the bank, not of the individual account holder.\textsuperscript{108} The majority of the current privacy-protection statutes were enacted to counter such perceived intrusions.\textsuperscript{109}

\begin{flushright}
\textsuperscript{104} See \textit{id.} at 176.
\end{flushright}

\begin{flushright}
\end{flushright}

\begin{flushright}
\textsuperscript{106} Miller also argued that the requirement in the Bank Secrecy Act, 12 U.S.C. § 1829b(d) (1994), that banks maintain microfilm copies of the checks for two years was an unconstitutional invasion of his Fourth Amendment right against unreasonable search and seizure. The district court rejected Miller’s arguments and he appealed. \textit{425 U.S.} at 438-40.
\end{flushright}

\begin{flushright}
The Fifth Circuit Court of Appeals also rejected Miller’s claim that the Bank Secrecy Act was unconstitutional, as that issue had already been resolved by the U.S. Supreme Court in 1974 in California Banker’s Ass’n v. Schultz, 416 U.S. 21 (1975). The court of appeals agreed, however, that Miller’s rights as well as the bank’s were threatened and that he should be accorded the right to challenge the validity of the grand jury’s subpoenas. The court of appeals saw Miller’s interest in the bank records as derived from the Fourth Amendment protection against unreasonable searches and seizures, which protected him against the “compulsory production of a man’s private matters to establish a criminal charge against him.” \textit{United States v. Miller}, 500 F.2d 751, 757 (5th Cir. 1974), rev’d, \textit{425 U.S.} 435 (1976) (quoting Boyd v. United States, 116 U.S. 616 (1886)).
\end{flushright}

\begin{flushright}
\textsuperscript{107} 425 U.S. at 440-46.
\end{flushright}

\begin{flushright}
\textsuperscript{108} \textit{id.} at 440-41.
\end{flushright}

\begin{flushright}
\textsuperscript{109} See infra App.
\end{flushright}
B. The Parameters of the Electronic Wilderness

To understand the issues underlying the protection of the individual's interest in the collection and disclosure of personal information, one must comprehend the environment in which these activities occur. During the last thirty years, the number of computers, computer databases and systems linking them has proliferated.\(^{110}\) Computers rapidly and accurately process information, and they can interact through the use of any number of media. Such connections, called networks, allow transfer of information from one computer to another.\(^{111}\)

Information networks are not set up to prevent disclosure. Indeed, their very purpose is to provide easy access to information in the system.\(^{112}\) From the database collector's viewpoint, there are both procedural and substantive components of each phase of a computer network system—manual initiation of data, conversion into computer-readable form, computer processing and output distribution—which must be protected.\(^{113}\) The procedural component concerns access to programs and corresponding files stored within the system and linked to other systems.\(^{114}\) The substantive elements embrace the collection of data for processing and regulate the accuracy of data collection and its availability to the user.\(^{115}\) These concerns are totally divorced from the interests of the individual, whose record is but a chattel to the collector or user.

Computers do have a physical component that can be subject to intrusion. In this sense, informational privacy involves the protection of the computer system itself. Most state statutes protect information by protecting the computer system under computer-security-type statutes. Such statutes generally prohibit “unauthorized access” to the computer system itself.\(^{116}\) These statutes limit access to personal data files, but they

---


111. A computer network consists of data communications systems and associated management software. See VERGARI & SHUE, supra note 96, at 23-24.

112. Sharing is the common function of all networks. Information sharing takes place when a communications program allows one computer to “talk” to another. *Id.*

113. See *id.* at 24-25.


115. See *id.* at 450-51.

116. By 1988, 46 of the 50 U.S. states had statutes prohibiting “unauthorized access” to computers. ROBERT E. SMITH, *Compilation of State and Federal Privacy Laws* 8-9 (1988). By contrast, only 24 of these states had specifically provided a right to privacy to their
leave unresolved the question of what can be done with the information once it is accessed.\textsuperscript{117}

Like the right to privacy, laws against unauthorized access are based on the concept of trespass and the ability of the “owner” of certain property to restrict access to such property from others.\textsuperscript{118} While unauthorized-access statutes collateral protect the privacy of the information in the system, the core of these statutes is not protection of the persona and the subject’s interest in it. There is, in fact, no statutory protection for a persona subsequent to its disclosure through lawful access.

The use of computers to manage information has considerably blurred the demarcation between the private and public realms.\textsuperscript{119} Once an item has been recorded in an on-line computer system, there are no consistent rules establishing the boundaries of private ownership of information not already protected by copyright or other existing intellectual property law.\textsuperscript{120} While a paper record can be destroyed by shredding, “deleting” a computer-stored file may not necessarily destroy it.\textsuperscript{121}

Before computer matching, an individual’s personal records were scattered among the various organizations that had dealt with the individual directly.\textsuperscript{122} Today’s computer matching, however, allows various fragments of information about an individual to be combined and compiled to form a much more complete profile. These profiles then can be collected, maintained and disclosed to organizations with which the citizens. \textit{id.} at 28-29. While the interests of the individual and the collector are the same on both the procedural and substantive levels, a discussion of the procedural aspects is beyond the scope of this article.

\textsuperscript{117} See \textit{id.}

\textsuperscript{118} See Mell, \textit{supra} note 89, at 28.

\textsuperscript{119} “[I]t is essential to expose the ways computer technology is magnifying the threat to informational privacy—a threat that we have faced in some form ever since man began to take notes about himself and his neighbors.” \textit{MILLER, ASSAULT}, \textit{supra} note 30, at 23.

\textsuperscript{120} See \textit{infra} App.

\textsuperscript{121} Jan C. Greenburg, \textit{E-mail Leaves Legal Trail}. \textit{DET. FREE PRESS}, Sept. 26, 1995, at 1A. The retrieval of deleted files recently cost a company $250,000 when its supposedly deleted computer files were retrieved and revealed derogatory remarks about a fired employee. \textit{id.}

The “delete” function works in the following manner: a file is identified by the computer by the first byte (character) of its file name. If the computer is directed to “forget” something, it responds by marking the first byte of the file with a special code, which indicates that the file has been erased. Then the computer clears the file’s entries from the file allocation table. Thus, an individual who knows the “code” can retrieve the deleted file. \textit{VERGARI & SHUE, supra} note 96, at 13-14.

individual has no direct contact or to which the individual would prefer to prevent disclosure. Using computer-matching programs, the government can obtain data from private data compilers to assist in the government's regulatory role. In a statement to Congress on the topic "Computer Matching: Taxpayer Records," then Commissioner of the Internal Revenue Service Lawrence Gibbs stated:

Commercial lists can reflect a variety of information, but typically they would show such things as the names of households and estimates of household incomes. Private companies prepare these lists using publicly available records, such as telephone listings, motor vehicle registrations, real estate transactions and public/aggregate census data.... The IRS is attempting to determine if commercial lists can supplement a variety of other efforts to identify persons who fail to file returns.

The distinction between government information collection and information collection by the private sector is increasingly difficult to justify, given this ability to share information.

The procedural manner in which information is stored and the manner in which it is referenced for retrieval can make it difficult for an individual to discover either the existence or nature of information held about him. A programmer generally arranges the information storage system (i.e., database) pursuant to the specifications of the user of the records. This means that the information-retrieval system likewise will be set up to function in only a certain number of ways. The


124. Hearings, supra note 123, at 25.


126. To understand the interests involved, one must comprehend the parameters of the environment in which they occur. There are four universal stages of each network system: 1) manual initiation of data, 2) conversion of data into computer-acceptable format (i.e., data capture), 3) computer processing and input and 4) distribution of output. See, e.g., ENCYCLOPEDIA OF COMPUTER SCIENCE AND ENGINEERING, supra note 3, at 370-72 (discussing major hardware components of computer systems). Each of these stages has two aspects in the computer context: the procedural aspect and the substantive aspect. The procedural aspect deals with issues of access to and security of the information and is beyond the scope of this article. The substantive aspect deals with issues of information accuracy, the power to prevent disclosure (privacy), and the power to limit disclosure (confidentiality). This system is not limited to national borders; the telecommunications system allows global access. This indicates the need for guidelines establishing the parameters of the individual's rights versus those of a private or public information-gathering organization, domestic or foreign. See Oettinger, supra note 50, at 196-97.
individual's request for information may be outside the computer's usual parameters.

A recent Ninth Circuit decision exemplifies this dilemma. In *Baker v. Department of Navy*, Baker had been investigated pursuant to a grievance filed about her by a subordinate. The investigation report was indexed under only the subordinate's name and was not cross-referenced to Baker. Baker was exonerated in the grievance but sought to see the report and determine its contents. This request was denied. In construing the Privacy Act, the court held that the Act applied only to the correction or retrieval of records retrieved by the individual's name. Any other request fell outside the Act's disclosure mandate. Even though the plaintiff in *Baker* had been named in a report, the file was not accessible to her because the record was not indexed under her name. An information request under these circumstances likely will be denied. The creation of special computer programs to fill the individual's request would require additional expense of time and labor on the part of the organization. Such efforts by the record keeper are rarely mandated.

In contrast, the result was more favorable to the individual when the request had sought disclosure of public records. In *Miller v. Department of State*, the court interpreted the Freedom of Information Act (FOIA) as requiring the agency to make a reasonable effort to search its records for the requested information.

Currently, the law places the primary right to control the disclosure and use of information upon the party in possession of it. This means that the third-party users of personae dictate the amount of information, and to whom, when and how personae are further disclosed. The organizations with which we directly deal record and store information about our transactions. Unfortunately, neither the law nor technology

127. 814 F.2d 1381 (9th Cir. 1987).
128. Id. at 1383.
129. Id.
130. Id.
131. Some statutes specifically exempt states from filling requests that are unduly burdensome. See, e.g., Ill. Rev. Stat. ch. 116, para. 203(f) (1985). Many an individual has been faced with the following words concerning the computer's purported inability to perform in a particular manner: "It [the computer] doesn't do that." See also McGhee v. Central Intelligence Agency, 697 F.2d 1095, 1110 (D.C. Cir. 1983), modified in part on reh'g, 711 F.2d 1076 (D.C. Cir. 1983); Founding Church of Scientology v. National Sec. Agency, 610 F.2d 824, 834 (D.C. Cir. 1979).
132. 779 F.2d 1378, 1383 (8th Cir. 1985).
134. Most of the authors in the original debate in the 1970s focused their attention on only this "primary" use of information. COMPTER-BASEDNATIONAL INFORMATION SYSTEMS, supra note 14, at 76. Viewed in that context, the transfer of the information becomes a part of the contract between the individual and the service provider. See id. This article goes
consistently provides the individual with a means of protecting his interests in the records collected and maintained about him.135

Once an individual has disclosed personal information and it is entered into a computer database, few limitations preclude an organization with no direct relationship to the individual from collecting, maintaining or disclosing the information.136 Verification of information in these records typically involves comparing the record to other records, not consultation with the individual who is the subject of the record. Since the individual may not have notice of any inaccuracy in the original record, such an error is now compounded. In this system, once the persona is recorded it achieves more credence than the individual.137

beyond the initial transaction to focus on the “secondary use” of information. Secondary use is the collection and manipulation of information by parties with whom the individual has not dealt directly. As such, the contract theory proposed in the 1970s does not apply to secondary use of information.

135. In a very few instances, federal and state agencies will combine efforts to combat widespread privacy abuses. In 1991, TRW settled a lawsuit with the Federal Trade Commission and 19 states for alleged violations of consumer privacy and for making reporting errors that damaged the credit ratings of thousands of consumers. TRW was required to change several of its procedures and to pay $300,000 to the states. 17 SOFTWARE ENGINEERING NOTES 12 (1992).

136. The Privacy Act requires each agency to publish in the Federal Register “notice of the existence and character of the system of records it holds.” 5 U.S.C. § 552a(e)(4) (1994). This provision would give the public such information as the categories of individuals whose records are held. Ostensibly, this provision would allow the individual to object if he did not want his records disclosed.

The General Accounting Office (GAO) investigated federal compliance with the public notice requirements and found that 292 of 910 federal databases were in violation of the provisions. To further compound the problem, the report noted that “78% of th[e] computer systems [studied were] interconnected,” which GAO interpreted to mean that “data collected on individuals without their knowledge or consent [was] widely available to go[vernment] and commercial users.” Big Brotherism Feared: GAO Report Raises New Computer Privacy Concerns, COMM. DAILY, Aug. 31, 1990, at 6.

137. Two cases are illustrative of this issue. Terry Dean Rogan lost his wallet, which held his driver’s license and credit cards. An imposter then committed two murders and two robberies. These crimes resulted in a warrant for Rogan being placed in the National Crime Information Center (NCIC) database. After the first arrest, Rogan attempted to get the problem corrected. Despite his efforts, he was arrested another four times during the next fourteen months. Finally, Rogan sued the Los Angeles police department and won $55,000. PETER G. NEUMANN, COMPUTER RELATED RISKS 194-95 (1995).

Also note the case of Clinton Rumrill III, who had credit card and traffic problems resulting in civil and criminal charges against him. A childhood “friend” was impersonating him by using his name and social security number. Police were informed of the problem but had failed to distinguish between Rumrill and the imposter. The computer continued to operate as if Rumrill and the impostor were the same person. Rumrill was told that the easiest solution would be for him to change his name and his Social Security number. Id. at 195.
The information, as a valuable commodity, is collected and resold to any interested third party. 138 It is a valuable resource both to the entity relying on the persona to render efficient decision making, and to the organization that specializes in collecting such information for repackaging and resale. 139 This method of information management has accentuated the dual public-private nature of the electronic persona, but this issue merely reflects the historic search for balance between society's need for information and the individual's need to prevent disclosure of his persona. This dual nature of the persona becomes a search for an accommodation between the public self and the individual's private identity. While not always apparent, the balance was traditionally sought in the recognition of varying property rights in the resource of the persona.

III. THE RELATIONSHIP BETWEEN PRIVACY AND PROPERTY

Although privacy originated in property concepts, 140 privacy and property have had an uneasy relationship as bases for protecting the individual's interest in personal information collected about him. 141 Due
to historical views on the relative inability of the individual to protect himself from the government’s overwhelming ability to intrude, privacy’s development in the United States followed two basic paths: one for governmental intrusions, another for nongovernmental ones.\textsuperscript{142} Common law contract, tort, trust and property theories developed to punish nongovernmental intrusions.\textsuperscript{143} The U.S. Constitution evolved to prohibit governmental violations of privacy.\textsuperscript{144}

Recently, scholars have suggested that the traditional distinction between the privacy tort and privacy under the Constitution is void or at least considerably blurred.\textsuperscript{145} A comparison of constitutional privacy and intrusion tort cases demonstrates the degree to which the two doctrines align.\textsuperscript{146} Identical treatment of the issues is supported by the fact that data collection by private industry can be just as pervasive as governmental data compilation.\textsuperscript{147} Therefore, this traditional distinction may have outlived its usefulness.

Even those doctrines that recognized a property interest in certain personal information largely declined to recognize the individual’s ownership of his various personae spawned by the manipulation of bits of personal information collected on him.\textsuperscript{148} Some authority indicates that the attempt to reconcile the myriad of interests has resulted in an overinclusive view of privacy as a concept and an overextensive view of its function.\textsuperscript{149}

\begin{footnotesize}
\begin{itemize}
\item and the term ‘property’ has grown to comprise every form of possession—intangible, as well as tangible.
\item Warren & Brandeis, \textit{supra} note 74, at 193.
\item There is some disagreement as to whether any common ground can be found between the protection of privacy under tort law and that found under constitutional law. \textit{See, e.g., McCarthy, supra note 4, § 5.7[B]} (finding no substantial similarity between the two theories). On the other side of the inquiry, see Edward J. Bloustein, \textit{Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser}, 39 N.Y.U. L. Rev. 962, 976-77 (1964).
\item Intellectual property rights protected the persona in certain contexts but were not extended to protect the non-literary, non-copyrightable and non-commercial aspects of the persona. \textit{See discussion infra} part III.A. concerning the inapplicability of most current intellectual property doctrines to the protection of persona in the informational privacy sense.
\item See discussion \textit{infra} part III.B.
\item Turkington, \textit{Privacy Cases}, supra note 145, at 19.
\item TRW, Trans Union and Equifax held a combined 410 million individual files in 1988. Rothfelder, \textit{supra note} 1, at 81.
\item \textit{See discussion} \textit{infra} part V. concerning current views on the property interest in personae.
\item True, there is no instant formula for clearly marking the fuzzy boundaries
\end{itemize}
\end{footnotesize}
A. Development of Common Law Protection of Informational Privacy

Current notions of informational privacy originated in the courts of Victorian England. Those cases based the protection of personal information in property concepts. In *Gee v. Pritchard*, the Court of Chancery restrained the publication of a private letter on the basis of protecting a property right. The court recognized a common law copyright in a private, nonliterary letter: "[B]ut if mischievous effects of that kind can be apprehended in cases in which the Court has been accustomed, on the ground of property, to forbid publication, it would not become me to abandon the jurisdiction which my predecessors have exercised, and refused to forbid it."  

Likewise, in *Abernethy v. Hutchinson*, the Court of Chancery prevented a medical student from publishing for profit a surgeon's lectures. The court recognized that the surgeon had a common law copyright in the verbal rendering of his lectures. To prevent Hutchinson from profiting from the publication of Abernethy's lectures, the court had to recognize that Abernethy had a property right in those lectures. It was not until the 1849 case of *Prince Albert v. Strange* that the interest protected was labeled one of privacy. In that case, pictorial engravings made by the Prince were appropriated by a printer's employee. The employee produced a few copies for himself and gave the prints to Strange, who published a catalogue describing them. The Prince sued both to recover the prints and to enjoin distribution of the catalogue. The defendant argued that no law existed that would prevent him from describing to the public either orally or in writing what of what we call the "private," but there are sound theoretical and practical reasons for not conflating privacy with established public freedoms that are frequently associated with it . . . . What the Court has found in those hazy penumbras of some constitutional amendments has sometimes to do with privacy, but other times merely with personal autonomy, personal sovereignty, or what the Court calls "personal liberty." . . . . It is true that in most accounts the protection of privacy has something to do with inviolate personhood; but everything that is either personal or fundamental or both, is not necessarily private . . . .


151. Id. at 678. See also Woolsey v. Judd, 11 How. Pr. 49, 53-55 (N.Y. 1855) (emphasizing that a property right must be violated for the court to take jurisdiction). See also Zimmerman, supra note 54, at 698 (noting that labor theory justified a property right in a product of the human mind).
he himself knew concerning the property held by another person. The Prince prevailed on breach-of-trust and implied-contract theories, but the court also indicated that common law copyright protected the individual’s property rights in personal information having commercial value. The doctrine gave the Prince legal power to withhold art and to prevent its description from reaching the public without his consent.

In determining the application of common law copyright protection, each of these British courts considered the commercial value of the personal information to a third party. This left open the question of whether noncommercially exploitable personal information could be protected in like manner. *Prince Albert v. Strange* also cited contract, trust and property bases for recovery for the nonconsentual disclosure of personal information when the individual had dealt directly with the third party.

The genesis of the extra-constitutional right to privacy in the United States was the 1880 treatise by Judge Cooley of Michigan, in which he coined the phrase “the right to be let alone.” One year later, the Michigan Supreme Court became the first state high court to recognize a privacy right to redress the emotional injury suffered by the nonconsentual disclosure of intimate facts. In *DeMay v. Roberts*, the court considered the plaintiff’s right to exclude another from her home during childbirth. The court held that the plaintiff had a legal right to the privacy of her apartment at such a time; the law secured this right by requiring others to observe it. By recognizing the plaintiff’s right to exclude others from her apartment, the court tied the right to privacy to a trespass or property doctrine. Early in 1890, the right of a light opera performer to prevent the publication of photographs taken without her consent was upheld in an unreported decision of a lower level New York Court.

Although not the first to declare the right to privacy, Warren and Brandeis were the first to discuss privacy as both a property and personal

155. *Id.* at 299.

156. Zimmerman, *supra* note 54, at 697. This approach is similar to that taken by the U.S. Supreme Court in *United States v. Carpenter*, 484 U.S. 19, 26-27 (1987), in which the Court recognized that confidential business information could be misappropriated. Misappropriation is a property concept. See *id.*

157. See *THOMAS COOLEY, COOLEY ON TORTS* 29 (2d ed. 1880).


159. *Id.* at 149.

160. The actress’s name was Marion Manola. The case was apparently unreported but appeared in the newspapers of the time. Warren and Brandeis referred to the case in their article, *The Right to Privacy*, to illustrate the proprietary aspect of the right to privacy. See Warren & Brandeis, *supra* note 78, at 195 n.7; Dorothy Glancy, *The Other Miss M*, 10 N. Ill. U. L. Rev. 401, 417 (1990).
right. It has been suggested that Warren and Brandeis presented a "hierarchical" relationship between privacy and property, in which intellectual property was a subcategory of the more general right to privacy. Warren and Brandeis did not distinguish between the labor that went into the creation of a work of art or literature and the labor expended by an individual in the conduct of his life. Both theorists recognized the individual's ownership of his persona, as well as the individual's difficulty in maintaining control of this property when he interacts with others in an ostensibly public sphere.

The most frequently cited phrase of this article labels the right to be protected as "inviolable personality," not property. The article's sole purpose was not to describe a new right that could redress the emotional injury suffered when the individual's "inviolable personality" had been made public without the individual's consent. Warren and Brandeis actually viewed privacy as an umbrella concept covering a series of related rights, some best protected by property concepts and others by tort law. A careful reading of the article indicates the full scope of the right of privacy as envisioned by Warren and Brandeis.

In every such case the individual is entitled to decide whether that which is his shall be given to the public.... [I]f privacy is once recognized as a right entitled to legal protection, the interposition of the courts cannot depend on the particular nature of the injuries resulting.... It is like the right not to be assaulted or beaten, the right not to be... defamed.... [T]here inheres the quality of being owned or possessed... as property.... The principle which protects... is in reality not the principle of private property, but that of an inviolate personality.

"Having established an hierarchy in the types of privacy," however, "Warren and Brandeis did not necessarily make privacy superior to property concepts as protection of the individual's anonymity." In reference to the fact that the then-new methods of photography allowed pictures to be taken of the individual surreptitiously, Warren and Brandeis rejected the trust and contract bases relied upon in *Abernethy*. Instead, they stated:

163. Warren & Brandeis, supra note 74, at 207.
164. Id. at 205.
165. Glancy, supra note 160, at 417-19
166. Warren & Brandeis, supra note 74, at 205.
167. Id. at 199, 205.
168. Glancy, supra note 160, at 417-19
[T]he doctrines of the contract and of trust are inadequate to support the required protection, and the law of tort must be resorted to. The right of property in its widest sense, including all possession, including all rights and privileges, and hence embracing the right to an inviolate personality, affords alone that broad basis upon which the protection which the individual demands can be rested.170

It has been suggested that Warren and Brandeis conceptualized privacy interests as forming a personal right rather than a property right in order to facilitate remediation.171 According to Warren and Brandeis, property could not be used as a basis for recovery "unless that word be used in an extended and unusual sense."172 In 1890, the law did not recognize property rights in personal information, or intangible items not protectable by copyright or patent.173 Since the individual's privacy was considered an inalienable attribute of personhood, it could not be considered a property right in the traditional sense.174

After Warren and Brandeis' article was published, the courts were not unanimous in recognizing the privacy right. In 1902, Roberson v. Rochester Folding Box Co.175 illustrated the diversity of values included in the right to privacy. Robertson brought suit because her photograph had been printed on defendant's flour advertisements without her permission. The court refused to restrain the unauthorized use of her picture for advertising purposes, arguing that simply no legal right was being infringed. An ordinary individual apparently had no property interest in the use of her own likeness. Judge Gray, writing for the dissent, found it inconceivable that there was no remedy under common law or in natural justice in keeping with "the progress of civilization . . . made possible as the result of new social or commercial conditions."176 While the court recognized the antagonism between commercial interests and the individual's interests in this property, it

170. Warren & Brandeis, supra note 74, at 211.
171. Zimmerman, supra note 54, at 699. "Warren and Brandeis were less interested in remedying particularized injuries than in giving individuals exclusive control over their 'inviolate personalit[ies].’ " Id.
172. Warren & Brandeis, supra note 74, at 213.
173. In their article, Warren and Brandeis track the development of the law toward the recognition of this right and document the fact that, until Cooley's designation of the right to be let alone in 1880, there was no cognizable interest in personal information. Id. at 193-213.
174. See Zimmerman, supra note 54, at 699 n.250. The advances in personal information management technology now allow privacy to be alienated just like any other chattel. This difference now justifies a new "sense" of property concepts to protect the individual's interest in personae.
175. 64 N.E. 442 (N.Y. 1902).
176. Id. at 449. The decision was highly criticized, and Judge O'Brien, a member of the majority, felt obliged to write a justification of the court's decision in a law review article. See Denis O'Brien, The Right of Privacy, 2 COLUM. L. REV. 437 (1902).
incorrectly gave the commercial interests preference. The New York legislature followed Judge Gray's lead by enacting a comprehensive statute protecting the individual's privacy. This statute prohibited the use of a person's name, portrait or picture for advertising purposes without that person's written consent.

On similar facts, the Georgia Supreme Court became the first American court to recognize a common law right to privacy in *Pasevich v. New England Life Ins. Co.* This court's decision was based more on property concepts than on tort theory. The court stated:

One who desires to live a life of partial seclusion has a right to choose the times, places, and manner in which and at which he will submit himself to the public gaze... The body of a person cannot be put on exhibition at any time or any place without his consent. The right of one to exhibit himself to the public at all proper times, in all proper places, and in a proper manner is embraced within the right of personal liberty. The right to withdraw from public gaze at such times as a person may see fit, when his presence in public is not demanded by any rule of law, is also embraced within the right of personal liberty.

Decided in 1905, *Pasevich* was the first case to recognize an individual's common law right to keep the persona private. Modern courts have accepted this concept and allowed recovery for the commercial exploitation of an individual's likeness.

In 1960, Professor Prosser identified four categories of tort relief under the heading of privacy: appropriation of name or likeness; intrusion upon an individual's seclusion, solitude or private affairs; public disclosure of private or embarrassing facts; and publicity that places a person in a false light in the public eye. As common law concepts, these torts reflected society's consensus as to what information

---

177. One year later, the state legislature of New York enacted a statute which created the right in the individual to control the use of his "name, portrait, or picture" for "advertising purposes." 1903 N.Y. Laws ch. 132 §§ 1, 2.


179. Id.

180. In *Pasevich v. New England Life Ins. Co.*, 50 S.E. 68, 69 (Ga. 1905), the court decided that a plaintiff whose photograph and name had been used in advertisements without his consent had stated a cause of action.

181. Id. at 70.


should be considered private and what recourse should be allowed when private information is exposed without the consent of the subject. Since the electronic persona is a relatively new phenomenon, courts have yet to significantly apply these torts to protect electronic privacy. However, using the torts to prevent against the nonconsentual use of electronic persona by either the news media or private industry presents certain conceptual problems.\textsuperscript{184}

In the 1970s, privacy protection for the persona was considered to exist in the nature of a contract between the individual and the third party.\textsuperscript{185} The individual divulged personal information to the third party, who conferred a benefit to the individual in exchange.\textsuperscript{186} The assumption was that the exchange bound the record keeper from "misusing" the information.\textsuperscript{187} However, the record keeper's post-use obligations were not formalized, and there was no monitoring of the record keeper's bargain. In addition, there was little or no law establishing the ownership or disposition of the information when its use was contrary to the individual's understanding of its use.\textsuperscript{188} In \textit{Salinger v. Random House},\textsuperscript{189} Salinger sought to prevent letters he had written to third parties from being used in an unauthorized biography. The recipients of the letters had donated them to various university libraries. Since the information provided in the letters was available to the public, it was considered to be "public information." Consequently, traditional copyright protection could not be invoked to prevent the use of the letters. In recognizing Salinger's interest, the appellate court characterized the biographer's act as one of taking Salinger's "property"; that is, Salinger's economic interest in safeguarding a future market for the letters should he or his successors later decide to publish them.\textsuperscript{190}

\begin{itemize}
\item[\textsuperscript{184}.] See discussion infra part IV.F. concerning the regulation of commercial interests, which analyzes the applicability of Prosser's torts to the protection of the electronic persona.
\item[\textsuperscript{185}.] See \textsc{Computer-Based National Information Systems}, supra note 14, at 76.
\item[\textsuperscript{186}.] \textit{Id}.
\item[\textsuperscript{187}.] This was the origin of the Fair Information Practices Doctrine. See generally \textsc{C.J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States} (1992).
\item[\textsuperscript{188}.] See infra App. for the respective effective dates of the statutes enacted to protect personal information.
\item[\textsuperscript{189}.] 811 F.2d 90 (2d Cir.), \textit{cert. denied}, 484 U.S. 890 (1987).
\item[\textsuperscript{190}.] \textit{Id}. The property being protected was actually Salinger's privacy. Salinger would have been unsuccessful in a suit alleging that the unauthorized publication of personal information in the letters had invaded his privacy.
\end{itemize}
Statutes enacted during the subsequent twenty years largely divested the individual of any power to prevent or limit disclosure of his persona.\textsuperscript{191}

B. Development of the Constitutional Right to Informational Privacy

Initially, constitutional protection of informational privacy was founded on Fourth Amendment protection against the government's physical trespass of the individual's private property.\textsuperscript{192} In \textit{Ex Parte Jackson},\textsuperscript{193} the United States Supreme Court invalidated the government's warrantless seizure of a sealed letter which had been mailed by the claimant. The Court said:

Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be.\textsuperscript{194}

Similarly, in \textit{Boyd v. United States},\textsuperscript{195} the Supreme Court invalidated the government's search of premises and its seizure of Boyd's private papers.

\textquote[196]{[I]t is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense, but it is the invasion of his indefeasible right of personal security, personal liberty, and private property, where the right has never been forfeited by his conviction of some public offense...} 

would shock the conscience of the ordinary reader. . . . In short, the book contained information that tort law would not protect.

\textsuperscript{191.} See discussion \textit{infra} part IV.F. on regulation of the commercial interest in the persona.

\textsuperscript{192.} See generally \textit{LASSON supra} note 31; \textit{WAYNE R. LAFAVE & JEROLD H. ISRAEL, CRIMINAL PROCEDURE} 97-107 (1985).

\textsuperscript{193.} \textit{Ex Parte Jackson}, 96 U.S. 727 (1877).

\textsuperscript{194.} \textit{Id.} at 733.

\textsuperscript{195.} 116 U.S. 616 (1886). \textit{Boyd} is also important for the Supreme Court's recognition that, under certain circumstances, the protection of informational privacy under the Fourth Amendment and the privilege against self incrimination under the Fifth Amendment "run almost into each other." \textit{Id.} at 630. More recently, however, the Fifth Amendment has been restricted to the protection of testimonial evidence. See, e.g., \textit{Schmerber v. California}, 384 U.S. 757, 765 (1966). See also \textit{LAFAVE & ISRAEL, supra} note 192, at 97-99.

\textsuperscript{196.} \textit{Boyd}, 116 U.S. at 630. Justice Bradley here quoted from Lord Camden's opinion in the English case of \textit{Entick v. Carrington}, 19 Howell's State Trials 1029 (1762), where the seizure of certain books and papers under a general warrant was found to have been actionable as a trespass.
While both Jackson and Boyd involved the breach of informational privacy by physical means, Justice Bradley's opinion in Boyd implied that more than physical trespass could be protected by the Fourth Amendment. Compelled use of an individual’s private papers would fall within the spirit and meaning of the Fourth Amendment.197

Despite the opening of this door, the United States Supreme Court at first declined to extend informational privacy protection to non-physical intrusions.198 Chief Justice Taft, writing for the five-member majority in Olmstead, based the decision on the historic view of physical trespass and found that the use of a listening device to obtain evidence was not prohibited by the Fourth Amendment restraint against unreasonable search and seizure.199

Writing for the dissent, however, Justice Brandeis reiterated his views on privacy and prophetically noted how technological changes must necessarily alter the application of the Fourth Amendment.200

‘Time works changes, brings into existence new conditions and purposes...’ Ways may some day be developed by which the government, without removing papers from secret drawers can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.201

During the next several years, courts applying the Fourth Amendment continued to base constitutional protection of the right of privacy upon a finding that the government had “trespassed” into the “private” place that contained the protected information.202 The cases designated two classes of excluded areas: “private” areas, in which the individual can expect to be free from governmental intrusion and “non-private” areas, in which the individual does not have a recognized expectation of privacy.203 The designation of an area as “private” protected the personal information located there from governmental seizure. During this period, the courts recognized the following areas as

199. Id. at 464.
200. Justice Brandeis, who had co-authored the article The Right to Privacy, Warren & Brandeis, supra note 74, dissented in Olmstead. While that article was not cited, it was noted that several of its passages were included almost verbatim within the dissent. See Bloustein, supra note 142, at 976-77. See also TURKINGTON, PRIVACY CASES, supra note 145, at 67.
201. Olmstead, 277 U.S. at 473-74 (Brandeis, J., dissenting)
202. The same issue is the basis of an intrusion tort analysis. This similarity has prompted some commentators to argue that there is in reality little difference between constitutional and tort privacy claims, the injury to the individual being the same. See Turkington, Legacy, supra note 145, at 487-502. See discussion infra part IV.F.1.b. concerning the intrusion tort as a basis for protecting persona.
"private": a home,\textsuperscript{204} a reserved hotel room,\textsuperscript{205} a motor vehicle\textsuperscript{206} and one’s body.\textsuperscript{207}

The limitation of Fourth Amendment protection to privacy in “protected” areas lasted until the Court developed the “expectation of privacy” principle as a basis for restricting government’s access to individuals’ information.\textsuperscript{208} The first cases to invoke the “expectation of privacy” principle involved the circumstances under which electronic surveillance could violate the Fourth Amendment right to privacy. These cases were \textit{Berger v. New York}\textsuperscript{209} and \textit{Katz v. United States}.\textsuperscript{210} Of these, \textit{Katz} had the greater impact on constitutional protection of privacy.

In \textit{Berger}, the Court was asked to determine the constitutionality of New York’s eavesdropping statute. The Court held that electronic intrusions in the form of surveillance constituted a search; therefore, the Fourth Amendment’s probable cause requirements applied to requests-for-a-surveillance order.\textsuperscript{211} The statute failed to pass constitutional muster on a variety of grounds. First, the statute did not require a description of the communications, conversations or discussions to be seized.\textsuperscript{212} Second, the statute failed to require the proponent of an order to specify the duration of the requested surveillance.\textsuperscript{213} Finally, the proponent of a surveillance order could acquire an extension of the order without making a separate showing of probable cause.\textsuperscript{214} The Court refuted the United States’ argument that, due to the importance of electronic surveillance to law enforcement, the probable cause requirements should be relaxed for electronic-surveillance petitions.\textsuperscript{215}

In \textit{Katz}, FBI agents attached an electronic listening and recording device to the exterior of a public telephone booth. They recorded Katz’s part of the conversation. The government’s argument focused on two points: whether a public telephone booth is a protected area and whether

\textsuperscript{205} Stoner v. California, 376 U.S. 483 (1964).
\textsuperscript{206} Carroll v. United States, 267 U.S. 132 (1925).
\textsuperscript{207} Schmerber v. California, 384 U.S. 757 (1966).
\textsuperscript{208} After \textit{Olmstead}, the Supreme Court largely maintained its adherence to the necessity of a trespass as a basis for invoking privacy protection. \textit{See}, e.g., Goldman v. United States, 316 U.S. 129 (1942); On Lee v. United States, 343 U.S. 747 (1952); Silverman v. United States, 365 U.S. 505 (1961). For a complete history of this development, see generally 1 WAYNE R. LAFAVE, \textsc{SEARCH AND SEIZURE} (1978).
\textsuperscript{209} 388 U.S. 41 (1967).
\textsuperscript{210} 389 U.S. 347 (1967).
\textsuperscript{211} \textit{Berger}, 388 U.S. at 51.
\textsuperscript{212} Id. at 58-59.
\textsuperscript{213} Id. at 59.
\textsuperscript{214} Id. at 59-60.
\textsuperscript{215} Id. at 62-63.
physical penetration is necessary before a search and seizure violates the Fourth Amendment. The Court decided that the attachment of an electronic listening and recording device to a public telephone booth was an unconstitutional search and therefore an invasion of the individual’s privacy. The Supreme Court stated:

[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected . . . . [T]he reach of [the Fourth] Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure . . . .

Katz represents a particularly important step in the evolution of informational privacy interests—it established the “expectation of privacy” standard in determining whether “searches” are unconstitutionally intrusive. This standard eliminated the traditional trespass requirements of the Fourth Amendment. Although the majority’s expansive view of the Fourth Amendment’s privacy protection, Justice Harlan’s concurrence again linked the protection of the Amendment to the protection of an identifiable place, and emphasized that the Constitution does not provide generalized privacy protection.

In his dissent in Katz, however, Justice Black presented the core argument that would prevent the Constitution from providing generalized informational privacy protection concurrent with the changes achieved in technology. Justice Black felt that to interpret the intrusion complained of as being within the purview of the Constitution’s prohibitions would be to distort the Amendment and put the Court in the

217. Id. at 351-53.
218. LAFAVE & ISRAEL, supra note 192, at 97-98.
219. [T]he underpinnings of Olmstead and Goldman have been so eroded by our subsequent decisions that the “trespass” doctrine there enunciated can no longer be regarded as controlling. The Government’s activities in electronically listening to and recording the petitioner’s words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a “search and seizure” within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.

Katz, 389 U.S. at 353.
220. Referring to the majority’s statement that the Fourth Amendment “protects people, not places,” Justice Harlan argued, “[t]he question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a ‘place.’ ” Id. at 361 (Harlan, J., concurring).
position of being "a continuously functioning constitutional convention." 221

Justice Black's restrictive view was subsequently adopted by the Court in cases dealing with the individual's expectation of privacy in information resulting from the individual's dealings with third parties. 222 Since the Katz decision, the Fourth Amendment has not been construed to create any generalized right in the individual to prevent disclosure of personally identifiable information. 223 Pursuant to Katz, information could be protected from disclosure only if the individual divulged it under a reasonable expectation of privacy. Subsequently, the Court concluded that there is no expectation of privacy in information voluntarily given to a third party. 224 This view continues to have severe implications for computerized records, since most information is, in fact, given voluntarily to the original collector by the individual. 225 With few

221. Id. at 364 (Black, J., dissenting).
222. See, e.g., United States v. Miller, 425 U.S. 435 (1976) (regarding the individual's expectation of privacy in his bank records); Smith v. Maryland, 442 U.S. 735 (1979) (concerning the individual's expectation of privacy in a governmental recording of numbers dialed from a person's telephone by use of a pen register). In both cases, the Court held that there is no legitimate expectation of privacy in information which the individual has voluntarily exposed to a third party. Consequently, the information seizure by the government was not violative of the Fourth Amendment. See Miller, 425 U.S. at 442; Smith, 442 U.S. at 745. For a critical review of the Court's position, see Tracey Maclin, Constructing Fourth Amendment Principles From the Government Perspective: Whose Amendment Is It, Anyway?, 25 AM. CRIM. L. REV. 669, 682-83 (1988).

The Fourth Amendment cannot be translated into a general constitutional right to privacy . . . . [T]he protection of a person's general right to privacy—his right to be left alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual States. Katz, 389 U.S. at 350.

Justice Brennan later encouraged the states to actively promote the protection of—among other constitutional rights—individual privacy rights under the Fourth Amendment. See Brennan, supra at 502. The states have responded with a more liberal approach on these issues. See TURKINGTON, PRIVACY CASES, supra note 145, at 100; Symposium: The Emergence of State Constitutional Law, 63 TEX. L. REV. 959-1338 (1985); Developments in the Law, The Interpretation of State Constitutional Rights, 95 HARV. L. REV. 1324 (1982). See also State v. Hunt, 450 A.2d 952 (N.J. 1982).


exceptions, information collected from the individual by governments of all levels, pursuant to their regulatory and administrative functions, becomes a public record. Such records are subject to governmental disclosure through the Freedom of Information Act (FOIA). They are protected from disclosure only by the Privacy Act (PA) or by agency-specific statutory protection.

Before Griswold v. Connecticut, privacy under the Constitution was conceptualized only as a part of general protection afforded by the Fourth and Fifth Amendments. The Griswold Court based its decision on the "penumbral" right of individual citizens to control their own lives in highly personal matters. While such a protection may be central to an "ordered conception of liberty," it does not necessarily protect informational privacy. The Griswold type of privacy focuses on individual autonomy but does not deal directly with the disclosure of the individual's personal information. Since constitutional privacy independent of the Fourth Amendment focuses on autonomy, as opposed to informational privacy per se, the protection of personae must be found in a different venue. Due to the Supreme Court's reluctance to expand the penumbral privacy of the Fourth Amendment, it is impractical to place a heavy reliance on either existing constitutional doctrine or the creation of new constitutional rights to protect the privacy of electronic personae.

The Supreme Court has tended not to question the state's ability to collect personal information from and about U.S. citizens. When challenged specifically concerning the ability of the government to collect and maintain computer records, the Supreme Court, in Whalen v. Roe, turned the issue into whether the information, once collected, had been properly safeguarded so as to prevent unwarranted disclosure.

In Whalen, a New York statute required hospitals and pharmacies to send a record of all patients receiving certain doctor-prescribed drugs to a

397 So. 2d 643 (Fla. 1981); and Louisiana: State v. Reeves, 427 So.2d 403 (La. 1982). With the exception of Alaska, these states expansively interpreted the right to privacy in construing the reasonableness of the state's search and seizure provisions. Alaska's view was based upon a specific state constitutional privacy provision. 583 P.2d at 881-82.

226. See discussion infra part V.
227. See infra App.
228. 381 U.S. 479 (1965).
229. Prosser, supra note 34, at 383.
230. 381 U.S. at 484-86.
231. The distinction between informational privacy and autonomy was pointed out in Whalen v. Roe, 429 U.S. 589, 598-600 (1977). Westin, supra note 31, at 32-42.
232. Statutes and administrative regulations are two effective ways to control both commercial and government handling of information. See infra part V.D.
233. 429 U.S. at 601-02.
central computer data bank.\textsuperscript{234} The statute also prohibited the public disclosure of this information.\textsuperscript{235} The purpose of the data bank was to allow the state to monitor drug abuse resulting from multiple drug prescriptions. The opponents of the record keeping argued that the information was both personal and protected and, further, that the statute’s reporting requirement deprived them of the right to make personal decisions about their medical treatment unencumbered by government intrusion or public disclosure.\textsuperscript{236} While the Court recognized the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files...[t]he right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures...[That duty arguably has its root in the Constitution.\textsuperscript{237}

Since the system in question maintained adequate protection against unwarranted disclosure,\textsuperscript{238} the Supreme Court did not question the government's need to collect the information. This reasoning has been followed by state courts facing similar challenges.\textsuperscript{239}

Even though courts tend freely to allow disclosure of government records, they have refused disclosure requests that impact other recognized constitutional freedoms of the individual.\textsuperscript{240} While informational privacy under the Fourth Amendment has not been recognized generally, autonomy issues of privacy do seem to be constitutionally protected. In this regard, the First Amendment freedoms of speech and association are recognized sources of some protection against government acquisition and disclosure of information.\textsuperscript{241} This protection focuses more on autonomy than on informational privacy.\textsuperscript{242}

\textsuperscript{234} Id. at 593.
\textsuperscript{235} Id. at 594.
\textsuperscript{236} See also Schulman v. New York City Health & Hospitals Corp., 335 N.Y.S.2d 343 (N.Y. Sup. Ct. 1972), vacated and remanded, 341 N.Y.S.2d 242 (N.Y. App. Div.), judgment reinstated, 346 N.Y.S.2d 920 (N.Y. Sup. Ct. 1973); Roe v. Ingraham, 480 F.2d 102 (2d Cir. 1973). In these cases, the claim was made that a person’s constitutional right to privacy includes the character of his physical ailments and doctor’s prescriptions for them. Consequently, the state must show a strong need before it can require the druggist’s disclosure of that information. See Ingraham, 480 F.2d at 109; Schulman, 335 N.Y.S.2d at 348.
\textsuperscript{237} Whalen, 429 U.S. at 605.
\textsuperscript{238} This system was self-contained and maintained off line. Id. at 594.
\textsuperscript{239} See, e.g., Peninsula Counseling Center v. Rahm, 719 P.2d 926 (Wash. 1986) (where the information collected included the name and diagnosis of government funded mental health patients); Perley v. Department of Motor Vehicles, 721 P.2d 50 (Cal. 1986) (where the government collected the fingerprints of drivers licensed by the state).
\textsuperscript{241} In Buckley v. Valeo, 421 U.S. 1 (1976) (per curiam), plaintiffs argued that requiring the disclosure of names of minorities might have the chilling effect of deterring some
C. Development of Statutory Protection of Privacy on the Federal Level

Between 1966 and 1990, several federal statutes dealing with personal privacy were enacted by Congress. These statutes were the Fair Credit Reporting Act of 1970,243 the Privacy Act of 1974,244 the Family Education Rights and Privacy Act of 1974,245 the Right to Financial Privacy Act of 1978,246 the Privacy Protection Act of 1980,247 the Paperwork Reduction Act of 1980,248 the Computer Matching and Privacy Protection Act of 1988,249 and the Video Privacy Act of 1994.250 While the Freedom of Information Act of 1994251 was enacted to provide access to files held by the government, the parameters of its disclosure provisions and its exemptions from disclosure have operated to provide privacy of sorts to the individual.

The statutes have had mixed results in defending the individual's privacy.252 While each of these statutes is diagrammed in the Appendix, a brief overview of their respective purposes is provided here.

The Freedom of Information Act (FOIA) makes federal records available for inspection and copying by the public. Its ostensible policy is that citizens should be able to find out what their government is doing. FOIA has several exemptions, one being that information should not be disclosed when such action would constitute a clearly unwarranted invasion of privacy.

The Fair Credit Reporting Act (FCRA) was the first piece of federal privacy legislation designed to regulate the disclosure of information people from making contributions to minority parties. The court said that these effects were too remote to overcome the public interest served by the collection of the information. This is contrary to the Court's prior ruling in NAACP v. Alabama, 357 U.S. 449 (1958), in which the Court struck down a requirement that the NAACP disclose its membership rosters.

242. See discussion infra part IV.B. concerning the individual's interest in the persona.
244. 5 U.S.C. § 552a (1994).
252. For a view of the deficiencies, see infra App.
held by the private sector. FCRA was touted as offering three basic forms of privacy protection to the consumer. First, it limits disclosure of reports on individuals to companies with a legitimate business need for the information. Second, it requires that organizations which provide credit or investigative reports to third parties also make their records available to the subject of the report. Finally, it mandates procedures for the correction of errors in reports.

The Privacy Act (PA) was enacted to protect the confidentiality of individuals about whom a government agency held a file containing personal information. Like FCRA, it provides the individual with access to information stored about him and establishes procedures for the correction and amendment of these files. It also attempts to limit the government's ability to disclose the information to third parties.

The Privacy Protection Act (PPA) limits the procedures by which the government can gain access to the files held by newspaper agencies.

The Family Education Rights and Privacy Act (FERPA) limits the ability of schools and colleges to disclose student records to third parties. It also requires the school or college to provide the student access to such records and provides procedures for challenging the accuracy of and amending student records.

The Right to Financial Privacy Act (RFPA) gives bank customers a limited expectation of privacy in their bank records by requiring that law enforcement officials follow certain procedures before any information can be disclosed.

Despite the apparent scope of coverage of these statutes, the actual protection afforded the individual's privacy varies greatly from one to the next. The number of statutes passed, each an attempt at protecting "privacy," partially explains society's failure to design a coherent policy regarding the aspects of personal information needing protection.

IV. ASSESSMENT OF THE INTERESTS COMPETING FOR USE OF THE PERSONA

A. Overview

The computer's utility in storing, retrieving, manipulating and sharing information has shaped the conflict between four different interest groups in their respective quests for access to more in-depth

253. See infra App.
personae. These groups can be described loosely as the public, the
government, the commercial and the individual.

By focusing on the subject matter of the data, existing laws do not
offer a viable guide to balancing the use of the persona by these
competing interests. The balancing of these interests centers on three
aspects of the information collection and dissemination process: the right
to collect information, the right to control or restrict the use of previously
collected information and the right to monitor the accuracy of the
information collected about the individual. The current legal rules on
informational privacy are a multi-leveled maze of sometimes conflicting
laws that are generally ineffective from the individual's standpoint.
Despite the pervasive influence of the electronic persona over an
individual's life, the electronically stored information comprising the
persona is not under the control of the individual in any significant way.
While there have been some attempts to ensure confidentiality under
some statutes and privacy under others, the right of the individual to
prevent the collection and secondary dissemination of personal
information is virtually nonexistent. The right of the individual to
correct inaccurate information is piecemeal at best, particularly since the
individual does not have a right to know whether a private enterprise has
compiled information concerning him. If an individual wants to
discover the existence of a record about him, he must decipher one set of
rules for records generated

Currently, the balance between these competing rights lies in favor
of the party in possession of the information. This means that the
possessor of the information has the power to control the collection,
content and disclosure of personal data without the subject's knowledge
or consent. This improperly divests the subject of the data file of his right

254. In a 1984 study by the Congressional Office of Technology Assessment (OTA),
only three "values" were identified as being in conflict: commercial, private and public. See COMPUTER-BASED NATIONAL INFORMATION SYSTEMS, supra note 14, at 49.

255. See discussion infra parts IV.B.-D. concerning these interests.

256. Confidentiality deals with the ability of the individual to prevent disclosure of
information to third parties. Privacy, on the other hand, deals with the ability of the
individual to prevent collection of the information.

The statutes of some states specifically focus confidentiality on the protection of
medical records of the individual as they relate to specific medical conditions. Forty-eight
states have such confidentiality provisions. See, e.g., FLA. STAT. ANN. § 381.606 (West 1986)
tests for infectious diseases). California has the most comprehensive protection requiring
the written permission of the patient before his medical records are disclosed. CAL. CIV.
CODE § 56 (West 1985).

257. See discussion infra part IV.E.

258. See infra App.
to self-determination, in that he can no longer monitor the accuracy of the
information upon which decisions about him are being made.259

Even more confusing for the individual is the fact that the national
trend in this area has been to base protection of the persona upon the
subject matter of the record itself, or on the type of damage done to the
database, rather than to enact general personal information protection
provisions.260 The existing statutes do not necessarily consider the
information’s relation to an identifiable person as important.

This haphazard approach is at cross-purposes to society’s stated
interest in preserving the individual’s privacy. It has created a
necessarily inconsistent definition of the interests sought to be protected
and has failed to establish a workable framework for balancing the
interests of those competing for access to personal information.261 Given
technological advances, which will sharply reduce the economic barriers
to the cross-referencing and continued storage of vast amounts of
information,262 such a framework is crucial. Without this framework,
there can be no uniform and comprehensive protection of personal
information.

There are two contexts in which the four interests conflict:
collection and secondary disclosure to third parties. The disclosure is
secondary in the sense that the party receiving the information was not a
party to the transaction giving rise to its collection. These recipient
parties may or may not intend to use the data for purposes consistent
with its original collection. From the collector’s view, use of the
information is implicit in its collection and its disclosure. This may not
comport with the individual’s understanding of the information
exchange. The individual’s interest in his persona is, as compared to
public, governmental and commercial interests, the least protected by the
current information regulatory system.

An additional impediment to balancing the use of the persona is the
difference in fundamental perspectives between the four groups with an
interest in the persona. The need for the collection and disclosure of the
persona is largely driven by economic incentives of government, public
and commercial groups.263 The individual’s personal need to control the

259. See generally Rothfelder, supra note 1.
260. See infra App.
261. For a description of different standards of protection provided by federal statutes,
see infra App.
262. From 1952 to 1980, the average computer system cost dropped from $1.26 to
$0.0025 per 100,000 calculations. COMPUTER-BASED NATIONAL INFORMATION SYSTEMS, supra
note 14, at 4 fig. 2 (citing OFFICE OF TECHNOLOGY ASSESSMENT AND PRESIDENT’S
REORGANIZATION PROJECT, FEDERAL DATA PROCESSING REORGANIZATION STUDY: BASIC
REPORT OF THE SCIENCE AND TECHNOLOGY TEAM 29-30 (1978)).
263. BELL, supra note 45, at 49-119.
persona may stem more from a concern for autonomy, which is not conducive to economic evaluation.

Not all of the interests held by the four different groups are adverse. They share an interest in the accuracy of the information. In addition, they would want notice of the disclosure of information to third parties and would want the ability to limit such disclosure to a designated few. Statutes applying to both the federal government and private industry have recognized this unity of interest. Some states' statutes require the reporting agency to correct inaccurate information. In other instances, where a given statute is otherwise silent, the courts have imposed due process notice and hearing standards upon reporting agencies.

The interests diverge sharply, however, on the secondary disclosure of information. Both federal and state statutes attempt to balance these interests depending upon the type of record sought to be disclosed and its context. In addition, the nature of the rights afforded and the remedies provided differ depending upon whether the infringer is a governmental, public or commercial entity. Such a distinction is without merit because the identity of the infringer does not change the disclosure's effect on the individual.

---

264. There can be no interest in collecting or disclosing inaccurate information about the individual. Nimmer, supra note 100, at 16-26.

265. Under the Privacy Act, the following procedure is provided to contest the accuracy of information in a federal file. The individual may inspect the record and, if he finds it to be inaccurate, he may file a statement disagreeing with it. The agency has 10 days to respond. If the agency declines to change the record, the individual may request a review, at both the agency and judicial levels. 5 U.S.C. § 552a (1994). If correction is ordered, the agency is required to notify all persons who received a copy of the inaccurate record of the change. In like manner, the Fair Credit Reporting Act (FCRA) allows the individual to challenge inaccuracies found in reports about him. 15 U.S.C. § 1681 (1994).

Unlike the Privacy Act, however, there are no requirements under FCRA that the agency notify all users of record of its correction. Unfortunately, under both statutes the correction process is begun only when the subject of the file discovers that the information is incorrect, which may be after the individual has been denied some benefit. See discussion infra part IV.

266. See, e.g., Koppes v. Waterloo, 445 N.W.2d 774 (Iowa 1989) (information in the report stigmatized the individual).

267. See, e.g., In re Bagley, 513 A.2d 331, 388 (N.H. 1986) ("Today governments collect great quantities of data about their citizens, data which, when stored in computers, potentially are available to large numbers of people. The dangers presented by governmental possession and use of inaccurate information are greater than ever. The principles of due process are our most effective shield against these dangers.").

268. See infra note 454 on Freedom of Information Act.

269. See American Fed'n of State, County & Mun. Employees v. County of Cook, 555 N.E.2d 361 (1990) (requiring disclosure of computer tape as public record under Illinois law; the terms of this open records law are contrasted to FOIA). See infra App.

270. See infra App.

271. "The connection ... between informational privacy rights in constitutional law and torts is in the nature of the injury and not in the character of the actor that causes the
B. The Individual's Interest in His Persona

The individual plays a dual role to the persona. On the one hand, the individual is the subject of the information-gathering. On the other, he is a consumer of the benefits and services that depend upon his disclosure of personal information. This dual role invokes different views of ownership of the persona. As a service provider, the compiler of the persona may want to assert superior "ownership" rights in the information by virtue of the compilation itself. However, the fact that the individual potentially benefits from the compilation "service" should not render him any less an "owner" of the persona thus compiled.

The five rights the individual might assert were articulated over twenty years ago. Each assumes the individual has some modicum of control over the information and thus implies a property right. The rights were stated as follows: the person should be able to find out what files concerning him exist; when the individual provides information concerning himself, he should know how the information is to be used and how broadly the information will be disclosed; if the record holder wants to disclose the information more broadly than originally contemplated, the individual’s consent should be obtained; the individual should have access to files concerning him and the opportunity to correct inaccurate information; and files should be afforded adequate security and outmoded information updated.

Control is not the sole issue from the individual’s perspective. Concerns over the proliferation of databases and the unchecked availability of personal information move beyond issues of information control to issues of maintaining the individual’s autonomy and a free society in which personal differences can exist. Some have argued that privacy is not properly a claim, but rather "a situation of freedom about which claims may be made." Even this view acknowledges that, as a practical matter, attaining the privacy necessary for true autonomy turns on the individual’s ability to control his personal information.

---

272. In 1973, the HEW Secretary’s Advisory Committee on Automated Personal Data Systems: Records, Computers and the Rights of Citizens developed the stated consensus on the basic protection persons should be afforded in their personal information. It was called the code of Fair Information Practices. See GREENAWALT, supra note 97, at 57. See also infra App. (comparing several federal statutes' effectiveness in achieving these goals).

273. See generally Countryman, supra note 30.

274. GREENAWALT, supra note 97, at 6.

275. Id. at 7.
C. The Government’s Interest

Both state and federal governments use personal information about citizens on different levels. On one level, a government may use anonymous statistical data to assist it in making fiscal projections and allocating resources.\(276\) The value of this information does not rely on its relation to any identifiable person. Such use does not infringe upon the individual’s privacy. On another level, the information may be used by government to determine a specific individual’s qualifications to receive government benefits.\(277\) For any government, the determination of the individual’s qualification to receive benefits requires accurate and current information.\(278\) As more governments seek sources of revenue, they will face financial pressures to offer their collected files to the private market.\(279\)

This situation directly conflicts with the individual’s desire to prevent collection and limit disclosure of his persona. While the individual’s need or desire to disclose information may vary depending upon the circumstances, he might want to be able to restrict the types and amounts of personal information the government can require him to divulge. None of the existing statutes places comprehensive limits on what the government can collect.\(280\) The individual may also wish to limit the government’s post-collection uses of the information and limit the government’s ability to divulge this information to third parties. However, information which has been recorded by the government has traditionally been freely accessible as a public record.\(281\) Such status gives the individual no power to restrict its disclosure.

\(276\). SMITH, supra note 1, at xi-xiii.


\(278\). The government’s collection of information for research on trends, and the development of statistics, does not generally impact on privacy issues since the information does not need to be tied to a specific individual. Only the collection of information on a specific individual raises privacy concerns. This would include such information as would be necessary for the assessment of a specific individual’s eligibility for government benefits; qualifications for employment; criminal records; draft records; real estate transactions; marriage; birth and death records; automobile registration; and tax liability. See NIMMER, supra note 100, § 16.09.

\(279\). Approximately 40 states sell the information you provide when registering a vehicle or applying for a license. Typically this information includes your age, sex, social security number and, through deduction, your income range. Big Brother May Be Closer Than You Thought, Bus. Wk., Feb. 9, 1987, at 85.

\(280\). See infra App.

\(281\). See discussion infra concerning the conflict between the policy of open government and the individual’s desire to keep his transactions to himself.
1. COLLECTION OF INFORMATION BY THE GOVERNMENT

Government agencies collect a great deal of information about the lives of citizens.\textsuperscript{282} The creation of a portfolio of this information could enable the government to monitor the individual's activities. As Richard F. Hixson stated:

\begin{quote}
[G]overnment... is the single biggest collector and distributor of information about citizens. This itself increases the probability that such data may be acquired and used under questionable, if not illegal... circumstances. Because bureaucracies by definition are powerful and seek to enhance their hold at every opportunity, computer technology makes it easier for our worst totalitarian tendencies to go undetected.\textsuperscript{283}
\end{quote}

Neither the government's information-collection process nor private industry's gathering process uniformly recognizes or protects individual rights.\textsuperscript{284} While the treatment of informational privacy differs in the two contexts, the individual's interest in preserving privacy does not.\textsuperscript{285}

Because so many of the services offered by the government are or have come to be considered necessities, the individual has little choice but to submit to the government's informational demands.\textsuperscript{286} In the government information-collection process, the diversity of the population necessitates the establishment of both a variety and concentration of institutional relationships with individuals.\textsuperscript{287} The substitution of records for face-to-face contact in these relationships makes the persona of paramount importance to the individual. It may not be an accurate reflection of the real person, but this image will be used to determine such fundamentals as to whether the individual gets hired, qualifies for a mortgage or social security benefits or is ostracized for pursuing a nontraditional lifestyle.

Some commentators have posited that the substantial growth in governmental record-keeping capability upsets the existing power balance between the individual and government.\textsuperscript{288} Much of an individual's freedom rests on his ability to act in relative anonymity.\textsuperscript{289}

The accumulation of information about individuals, however, increases

\textsuperscript{282} The federal government maintains on the average 18 files on each citizen, adult and child. Smith, supra note 1, at 82.

\textsuperscript{283} RICHARD F. HIXSON, PRIVACY IN A PUBLIC SOCIETY: HUMAN RIGHTS IN CONFLICT 209 (1984).

\textsuperscript{284} For a discussion on the interests competing for use of the persona, see infra part IV.A; see infra App.

\textsuperscript{285} Id.


\textsuperscript{287} See Bell, supra note 46, at 32.

\textsuperscript{288} Id. See also Westin, supra note 31, at 158-68.

\textsuperscript{289} See Bell, supra note 46, at 34.
the government's power by facilitating its ability to monitor the individual directly. Thus, growth in society's record-keeping capability poses the risk that existing power balances will be upset.\footnote{290}

\subsection*{a. Constitutional Bars to Information Collection}

The individual's primary ability to fight governmental intrusions is based on the guarantees of individual liberty provided by the Constitution. Most of the literature documenting the individual's struggle has treated the protection of personal information as a form of privacy protection.\footnote{291} The current concept of privacy protection does not explicitly guard against truthful but embarrassing or intrusive informational disclosure of an individual's persona. While privacy protection under the Constitution has been found to exist beyond Fourth Amendment intrusions, the protection afforded by the Constitution most often relates to personal autonomy and freedom, not specifically to informational privacy.\footnote{292} These are balance-of-power issues between the individual and the state. They are not founded upon the individual's loss of control over his persona. As such, the individual's interest in controlling the collection and disclosure of personal information is not coextensive with the traditional concept of privacy under the Constitution.

With exceptions in criminal prosecution or personal autonomy decisions, there are few restraints on the power of the government to collect data. The government has been restrained under the First, Fourth


291. There is some authority for the position that the protection of personal information is not an issue of privacy, but rather one of confidentiality. All of these interests can be characterized as interests in privileged access to the information. Privileged access is more a question of confidentiality than it is of privacy. "Because privacy protects intimacy, personal information that is not of the most intimate nature is not so much private as it is confidential." \textit{Privacy and Computers, supra} note 123, at 1407 (citing Gerety, \textit{supra} note 39, at 282). "Gerety contrasts the concepts of privacy and confidentiality. In his view 'specially private information includes only information that is necessary to the intimacies of our personal identities for standards of intimacy, unlike standards of confidentiality, cannot be created simply by mutual agreement.' " \textit{Id.}

292. Personal autonomy issues arise when the individual's choice of activity conflicts with the government's right to regulate the activity of its citizens. While the choices of life style and choice of association do "tell" about the specific individual, this is not exactly the same issue as the protection of informational privacy of the persona. Privacy, in the autonomy sense, has been used as the basis for recovery for such diverse intrusions as door-to-door solicitations (Saia v. New York, 334 U.S. 558 (1948); Kovacs v. Cooper, 336 U.S. 77 (1949)), and the decision on whether or not to have an abortion (Roe v. Wade, 410 U.S. 113 (1973)). In neither situation has information about the individual been disclosed. Similarly, a search of the marital bedroom invades the privacy of the family independently of any information discovered there. \textit{Greenawalt, supra} note 97, at 4.
and Fifth Amendments when its attempts to collect information have impacted the individual's right to exercise freedom of choice in birth control, abortion and marital choice matters. As a consequence of these prohibitions, the government's right to collect personal information has most often been challenged as a violation of constitutional rights.

b. Statutory Bars to Government Collection of Data

Despite several federal statutes passed during the last thirty years, the individual has little control over the collection and usage of personae. While giving lip service to protecting the individual's privacy, these statutes largely promote the interests of the groups they ostensibly regulate. Current laws tend to regulate the activities of specific record keepers rather than providing rules governing how the individual's relationship to personal information should be protected. The primary restraint on the government's ability to collect and use information is the Privacy Act of 1974. As indicated in the Appendix, this Act is a limitation only upon a system of records about natural persons held by a federal agency. The Privacy Act does not provide the individual with broad rights to discover personal information.

Another troubling aspect of the Privacy Act is its silence on the issue of revealing third-party sources of information. If the source is a part of the record, it must be revealed. However, the Privacy Act does not obligate the agency to disclose the information's source. This works adversely to the interests of accuracy in the information. The subject must be in a position to know the source of third-party information to successfully challenge it.

The Privacy Act presumes the individual's consent to use and disclose the information for "routine use" but requires that consent be

293. While there is no recognized general federal constitutional right to privacy, in 1986 it was noted that at least 10 states did provide such a right. See SMITH, supra note 116, at 2. See also PERKEY v. Department of Motor Vehicles, 721 P.2d 50, 55-56 (Cal. 1986). Not all matters of sexual choice have received constitutional protection. See, e.g., Bowers v. Hardwick, 478 U.S. 186 (1986).

294. Data collection on the part of the government was denied in NAACP v. Alabama, 357 U.S. 449 (1958). There the Court invalidated a requirement that the NAACP disclose membership rosters on First Amendment freedom of association grounds. See supra part IV.A.; infra App.

295. See infra App. According to the Office of Management and Budget (OMB), the approximately 7,000 federal data banks hold personal information files on 3.8 billion identifiable individuals. SMITH, supra note 1, at 82. Only half of these are kept to evaluate government programs and to determine the individual's eligibility for benefits. Id.

296. See discussion infra part IV.A. concerning how the competing interests have framed the discussion. See also infra App.

sought before the record is disclosed for other uses.\textsuperscript{298} Unfortunately for
the individual, the agency is not required to explain the extent of
disclosure subsumed under the heading of “routine use.” As a
consequence, the individual may not be aware of the uses to which the
government will put his information. Once such information is disclosed
to a third party, there are no requirements that the receiving agency use it
in a manner or for a purpose consistent with its original collection.

Although the Privacy Act directs each agency to establish security
and confidentiality standards for the use of the personal information files,
it does not create any mechanism for systematic review of the adequacy
of these standards. The only other notice provision is activated when the
use of the information may result in an action adverse to the individual.
Pursuant to the individual’s challenge to the information’s accuracy, the
agency is directed to collect information to the greatest extent practicable
from the individual himself.

The Paperwork Reduction Act of 1980 limits the collection of
information from individuals.\textsuperscript{299} This Act requires any agency soliciting
information from members of the public to inform the public of the
reason for which the information is being sought and whether the failure
to comply with the request will affect the individual’s eligibility for
benefits. The Act also gives the federal Office of Management and
Budget (OMB) the power to determine whether the requested
information has already been collected by a different agency; if so, the
OMB may deny the requesting agency the right to seek the information
from the individual. It will also refuse to allow an agency to collect
information if the OMB finds that the agency will not be able to use the
information if collected.

\section*{2. SECONDARY USE OF THE INFORMATION BY
GOVERNMENT}

Data matching is another area of conflict between government and
individual interests in private information.\textsuperscript{300} Because cost efficiency is
given higher priority than information accuracy, government agencies
will match and combine data files collected on an individual by several
agencies rather than create a new information file.

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{298} “Routine use” means that a record may be disclosed for a purpose which is
compatible with the purpose for which it was collected. 5 U.S.C. § 552a(a)(7) (1994). While
these routine uses are published annually in the Federal Register, the importance of this
disclosure may not be apparent to the general public.
\item \textsuperscript{299} 44 U.S.C. § 3501 (1988).
\item \textsuperscript{300} See Computer Matching and Privacy Protection Act of 1988, 102 Stat. 2507-14
\end{itemize}
\end{footnotesize}
The primary restraint on the government's secondary data collection ability is the Computer Matching and Privacy Protection Act of 1988. This statute is very broad and provides guidelines for the computerized matching of information for two basic purposes: verification of the individual's eligibility or continued eligibility for government "cash or in-kind assistance for payments under Federal benefit programs" and collecting payments or delinquent debts owed the United States. The government's eligibility to match information is conditioned upon its obtaining written consent from the individual.

Most important for the individual are the statute's requirements in the event that adverse action results from a matching. Before taking the adverse action, the government is required to make an independent verification of the facts and to extend to the individual the opportunity to contest the findings of the agency.

Governments now routinely match individuals' data files in multiple agencies to discover violators of laws. Despite the efficiency benefits of these means, some commentators characterize information matching as an unnecessary governmental fishing expedition. Their opposition is apparently based on the belief that the difficulty of combining paper personae residing in different offices provides the individual with a modicum of privacy. An efficient data-matching system foils this de facto privacy. However, courts considering this issue have not found in favor of the individual. In Jaffees v. Secretary of Health Education Welfare, the government matched an individual's social security and veteran's records and determined that the individual's benefits should be reduced. The court stated that the constitutional right to privacy did not extend to a matching of documents to determine the individual's right to continue receiving governmental benefits.

301. The statute is strengthened by the mandated creation of Data Integrity Boards for every agency participating in a matching program. The board approves matching programs requested by the agency and makes public reports concerning the matching program conducted by the agency. 5 U.S.C. § 522a.


304. 5 U.S.C. § 552a(o)(1). The agreement gives the recipient a great deal of information concerning the purpose and authority for the program; the justification for the program; a description of what records will be matched; the procedures to be used to verify information; and the procedures to be followed to notify individuals that the information will be subjected to matching. Id.


306. See Langan, supra note 122, at 146.


309. Id. at 629.
Despite the recognition which courts have given to a constitutional right of privacy in other contexts... the present thrust of the decisional law does not include within its compass the right of an individual to prevent disclosure by one governmental agency to another of matters obtained in the course of the transmitting agency's regular functions.\textsuperscript{310}

The courts have agreed with this principle in cases dealing with other government activities and benefits as well.\textsuperscript{311}

While the Computer Matching and Privacy Protection Act of 1988 outlines rules regarding disclosure of records in connection with "matching programs," it does not cover matching programs that are "non-threatening" to the economic or privacy interests of individuals whose records are matched.\textsuperscript{312} Pursuant to its authority, the Office of Management and Budget (OMB) is required to issue guidelines that would standardize the data-matching activities of different government offices. The effect of the Computer Matching Act was to partially nullify provisions of the Privacy Act.\textsuperscript{313} Likewise, the Paperwork Reduction Act of 1980 provides that the OMB may refuse to allow an agency to collect certain data if it concludes that another agency has already collected the information or that the agency proposing to collect the information cannot use it.\textsuperscript{314}

The Right to Financial Privacy Act requires the government to give the individual notice before the government can get financial records of the individual from a bank.\textsuperscript{315} The act's primary function is to restrict access to financial records in institutions in which the federal government has either a financial or regulatory interest.\textsuperscript{316}

The Family and Educational Privacy Act limits the information which schools and other institutions can disclose about individuals.\textsuperscript{317} Notably, while there have been several attempts to pass legislation concerning health records, Congress has yet to enact a privacy protection statute for personae based on health transactions.\textsuperscript{318} Thus, while there are

\begin{itemize}
  \item \textsuperscript{310} Id.
  \item \textsuperscript{312} See NIMMER, supra note 100, at 16-30.
  \item \textsuperscript{313} JOHN M. CARROLL, CONFIDENTIAL INFORMATION SOURCES: PUBLIC AND PRIVATE 47 (2d ed. 1991).
  \item \textsuperscript{314} 44 U.S.C. §§ 3501-3520 (1988). See also infra App.
  \item \textsuperscript{316} See 12 U.S.C. § 3402 (1994).
  \item \textsuperscript{317} See 20 U.S.C. § 1232g (1994).
  \item \textsuperscript{318} A bipartisan bill, the Medical Records Confidentiality Act of 1995, was proposed as S. 1360, 104th Cong., 1st Sess. (October 24, 1995).
\end{itemize}
some constitutional and statutory constraints on the government’s collection and use of personae, these limits offer only minimal protection of the individual’s right to act in seclusion.

D. The Public Interest in the Persona

American society has always viewed information as having a public value and has asserted the public interest in a free flow of information. In addition, our system of justice sets guidelines concerning the disclosure of information to opposing parties in a suit through discovery, despite the individual’s desire to maintain his silence. The public interest in freely available information is not changed simply because the request is made by a person who intends to use the information for commercial gain. The value of maintaining unrestricted access is so strong that the courts have at times imposed on governmental entities “what amounts to a joint venture with an information services provider.”

Unless the disclosure has a perceptible and direct impact on a recognized constitutional right of the individual, the public interest in open information will override the individual’s interest in privacy. The basic premise of open records is the American policy of open government. The Freedom of Information Act (FOIA) was enacted to promote this policy.

Freedom of information laws that support the public’s interest in disclosing government-held personae can conflict with individual or commercial concerns for privacy. In serving the public interest, governments collect an extraordinary amount of information about

319. Examples of this phenomenon include public support of libraries, schools and museums; a tradition of academic freedom and a system of openly scholarly publication; the guarantees of the First Amendment; and freedom of information laws.

320. See, e.g., Techniscan Corp. v. Passaic Valley Water Comm’n, 549 A.2d 1249 (N.J. 1988) (holding that a company searching public records for profit has the same right of access as any other party under the state’s right-to-know law).

321. NIMMER, supra note 100, at 16-39. This relationship is not necessarily voluntary. See, e.g., Department of Justice v. Tax Analysts, 442 U.S. 136 (1989). The Supreme Court held that a commercial publishing house was entitled to weekly access in an ongoing publication. The costs of the enterprise are apparently shared by the government and the commercial recipient. Id.

322. In Paul v. Davis, 424 U.S. 693, 713 (1976), the issue was whether the general constitutional law or more specific statutes or regulations preclude a disclosure that the government desires to make. The Supreme Court concluded that no privacy right was infringed by dissemination of a list of active shoplifters from arrest records. Collection and distribution of those records did not disclose otherwise confidential information. See also Minnesota Medical Ass’n v. State, 274 N.W.2d 84, 91-94 (Minn. 1978); State v. Harder, 641 P.2d 366 (Kan. 1982) (disclosure of abortion reimbursement records was not a violation of privacy rights of either the doctors or the patients where there was no showing that disclosure would alter the actions of the doctors).

citizens, businesses and other organizations. Much of this information has been theoretically available to the public by law for a long time, but has been protected by the effort required to retrieve it in a manual record-keeping system. Automated systems reduce the cost and time barriers to wider access to these public records, raising the issue of the extent to which this information can and should be publicly available.

The basic premise of the Freedom of Information Act (FOIA) is that federal records must be open to public scrutiny unless they fall within one or more of seven exemptions. In operation, FOIA precludes the disclosure of otherwise public information if it would infringe on the privacy of the individual. In United States Department of Justice v. Reporters Committee for Freedom of the Press, the Court held that FOIA’s mandate to avoid “unwarranted invasions of privacy” prevented the disclosure of an FBI rap sheet, which combined reports on an individual’s arrests and convictions from various state and federal law enforcement agencies. The Court stated that the determination of whether disclosure of a private document . . . is unwarranted must turn on the nature of the requested document and its relationship to the FOIA’s central purpose of exposing to public scrutiny official information that sheds light on an agency’s performance of its statutory duties, rather than upon the particular purpose for which the document is requested or the identity of the requesting party. The statutory purpose is not fostered by disclosure of information about private citizens that is accumulated in various governmental files but that reveals little or nothing about an agency’s own conduct.

Consequently, even though FOIA is a statute mandating disclosure, it has been used to prevent the disclosure of personal information in a variety of different contexts.

324. See supra note 91 and accompanying text.
326. The exemptions are as follows: 1) national security material; 2) material related solely to internal personnel rules and practices; 3) documents and information exempted by other statutes; 4) information that pertains to “trade secrets and commercial or financial information”; 5) “inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency”; 6) personnel, medical and other files, “the disclosure of which would constitute a clearly unwarranted invasion of personal privacy”; and 7) records compiled pursuant to a law enforcement investigation. These records are exempt only to the extent disclosure would interfere with the enforcement proceedings or a fair trial, constitute unwarranted invasions of personal privacy, disclose the identity of a confidential source or investigatory techniques, or endanger the safety of enforcement personnel. 5 U.S.C. § 552(b) (1994).
328. Id.
329. See, e.g., Painting & Drywall Work Preservation Fund, Inc. v. Department of HUD, 936 F.2d 1300 (D.C. Cir. 1991); Reed v. NLRB, 927 F.2d 1249 (D.C. Cir. 1991) (disclosure of
The news media claim to represent a public interest in government-held personae. There are few deterrents on the news media’s desire to publish personal information about the “newsworthy.” The right to privacy urged by Warren and Brandeis would allow an individual to recover damages for widespread publication of information about him.

E. Conflict Between the Interests of the Government and the Public for Use of the Persona

In one setting, the public’s interest in use of a persona comes into conflict with the government’s interest in precluding the disclosure of the information. The government is not prohibited from selling information to third parties who intend to package the information commercially. But the government’s desire to profit commercially from the information it holds may conflict with that of a third party. In Legi-Tech v. Keiper, Legi-Tech sought access in computer format to New York state legislative developments. Legi-Tech wanted to market the information commercially. Since the state itself provided this information for a fee, it viewed Legi-Tech as a direct competitor, and it refused Legi-Tech’s request. The Second Circuit ruled that the First Amendment required the state to provide information on the active legislative process to Legi-Tech, although the state could charge Legi-Tech a fee. In effect, the public’s interest in access to “public documents” was found to be superior to the government’s interest in profiting commercially from information collected pursuant to the agency’s function.

names and addresses of employees eligible to vote in union election declared to be exempt as a clearly unwarranted invasion of personal privacy); Oliva v. United States, 756 F. Supp. 105 (E.D.N.Y. 1991) (disclosure of social security numbers and birth dates was unwarranted privacy invasion).

330. See, e.g., Sidis v. F-R Publishing Corp., 113 F.2d 806 (2d Cir. 1940). Plaintiff, William James Sidis, was a child prodigy. He lectured mathematicians on the fourth dimension at age 11 and graduated from Harvard at 16 years of age. During adolescence, however, Sidis withdrew entirely from the limelight. Several years later, the New Yorker found Sidis and published a story about his life in obscurity. Despite its terrible effect upon Sidis, the court found that there was no cause of action because the story would not be objectionable to the ordinary person.

331. Warren & Brandeis, supra note 74, at 204. See also Zimmerman, supra note 54, at 713 (arguing that what is notable about Warren and Brandeis is that they advocated the right of the individual to “recover in a court of law for the publication of accurate information about themselves, simply for the reason that such publicity was unwarranted”). See also RESTATEMENT (SECOND) OF TORTS § 652 (1977).

F. Commercial Interests in the Individual’s Persona

Institutions’ need to make decisions based on valid information and the infeasibility of direct contact with the individual have created a lucrative information market. This market drives the desire of government and business entities to disclose the information they collect in their direct dealings with individuals. A number of features of this market and the requirements of administrative efficiency combine to produce a system which by nature separates the persona from the real person and gives the data in the persona more consideration in the decision-making process than it gives the individual. This is disturbing because the current accuracy requirements on the majority of records are uneven.

Economic competition is often based on access to special marketing information, such as a customer-base composition, salary, product preferences and frequency of purchase, credit history and residential patterns. The availability of the persona has created an industry in which the secondary use of information can generate direct sales solicitations known as direct mail. The practice is so pervasive that in 1992, the Direct Marketing Association reported that 66 of the Fortune 100 and 190 of the Fortune 500 used some level of direct marketing. The mere receipt of the “junk mail” generated by this industry has never been considered to be a major problem for the individual, but the phenomenon raises two persona protection issues. First, data marketers have the ability to collect and manipulate information even when the individual has had no prior contact with them. Second, there are no requirements that the direct marketers check the accuracy of the newly created persona with the individual or refrain from transferring the persona thus created to yet another party unknown to the individual.

333. “[M]odern Americans inhabit a social environment virtually composed of formal organizations. The main source of . . . privacy controversies . . . has been the demands of formal organizations for information on the people with whom these organizations must deal.” JAMES RULE ET AL., THE POLITICS OF PRIVACY 30 (1980).

334. “For the written records of one’s life, in modern America and other developed countries, shape the treatments one receives by organizations. And the role of organizations, both private and public, is powerful indeed.” Id. at 2.

335. See infra App., at row 7.

336. RULE, supra note 60, at 208-12.

337. Culnan, supra note 28, at 346.

338. Id.

339. See generally PRIVACY PROTECTION STUDY, supra note 1.
1. TORT REGULATION OF COMMERCIAL USE OF PERSONAE

The existence of and necessity for the collection and maintenance of personal information records is now a well-documented characteristic of our late twentieth-century society. Information about the individual is being collected both by a government attempting to efficiently manage a large diverse population and by private commercial entities attempting to streamline their marketing costs by locating those individuals most likely to become customers.

As information becomes a more valuable commodity, increasing tensions are arising between those who wish to sell it through new information systems and those, like the public libraries, whose traditional role is to treat information as a public good available to all. These tensions may stem from the competition between government-collected data made available through freedom of information laws and commercial data services.

Commercially marketable information may invade privacy when computerized mailing lists compiled from third-party information sources are used without the knowledge or consent of the individual involved.

DATA once collected, even for an initially legitimate reason, may be put to new and invasive uses. Knowing that every transaction is forever stored in an electronic database can change an individual's perception of herself and her relationship to society. She knows she can never discard her past, that others will judge her on a computer record. Thus, she is apt to assume conformist behavior to maintain a "good" record, avoid "deviant" or controversial activity regardless of her true beliefs and feelings, and reduce her independent action and thought.

At common law, protection of the individual's interest was first based in tort theories of privacy. "[Although] solitude and privacy have become more essential to the individual . . . modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury." These words, written in 1890, seem to forecast the threat to this solitude posed by the modern day computer and database.

340. See supra part II. "The growth of an enterprise, for example, requires specialization and differentiation and very different kinds of control and management systems when the scales move from, say, $10 million, to $100 million to $1 billion." Bell, supra note 46, at 32.
342. Warren & Brandeis, supra note 74, at 196.
a. The Appropriation Tort

The appropriation tort, being a mix of property and privacy concepts, would be the most likely tort to protect the individual's interest in his persona. It has been used to punish the commercial and non-commercial exploitation of an individual's name and/or likeness.343 In many cases, courts would have to broaden the existing definition of likeness to apply this tort to an electronic persona. Unlike photographs, personae in the form of data-marketing profiles have not yet been determined to be likenesses. While both photographs and marketing profiles can give a clear image of the subject, the distinct media in which the "likenesses" are created pose very different issues for the application of the tort to personae in the electronic wilderness.

For the appropriation tort to be actionable, a complete and easily recognizable likeness of the individual must have been used.344 To apply this tort to redress the nonconsentual use of the electronic persona, a standard of completeness would have to be established. Different profiles of the individual, having been compiled by different parties for different purposes, may contain some but not all of the available information concerning the subject. The information in any profile may be correct, but that would not necessarily make the profile a complete "likeness" of the subject in the traditional sense.345 By the same token, inaccurate information would not be actionable under this tort, since inaccurate information could never be a "likeness" of the subject.346 The "name appropriation" aspect of the tort would not be difficult to apply in redressing abuse of the electronic persona. A great deal of information is accessible under the individual's name.347 By use of the "name," a user of the persona would be able to access any and all personal information filed "under" it. Once accessed, the information could be used to the acquirer's benefit without the consent of the subject.348

345. See supra part VI. See also GREENAWALT, supra note 97, at 47.
346. Miller, supra note 30, at 174.
348. Ward v. Superior Ct., 3 Comp. L. Serv. Rep. 206 (1972). This tort could be used by the database owner to redress nonauthorized access to electronic personae included in a database.
b. The Intrusion Tort

This tort protects against intrusion into a person's solitude or his personal affairs. Traditionally, this tort covered such physical intrusions as entering into an individual's home or hotel room. More recently, plaintiffs have been successful in using this tort to redress such electronic intrusions as wiretapping, electronic eavesdropping, physical surveillance and other sensory surveillance. To recover, a plaintiff must establish that the information was obtained by improperly intrusive means. The means of obtaining the information is considered improperly intrusive if it infringes upon areas in which the ordinary person would have a reasonable expectation of being able to exclude others. This tort prohibits in the private sphere the type of intrusion prohibited to the government by the Fourth Amendment.

While this tort can represent the civil branch of the unauthorized access cases, it does not focus on the privacy of the persona per se. Rather, it focuses on the concept of intrusion into a protected area. Unless mere intrusion is equated with access to the persona, or the intrusion is accompanied by appropriation of the information, this type of tort recovery would not ordinarily redress a violation of the individual's interest in his persona.

In at least one instance, a court has recognized the propriety of extending this tort to non-physical intrusions. In Pearson v. Dodd, Senator Dodd alleged that his privacy had been invaded by Pearson's publishing of information allegedly stolen from his files. Since Pearson had not himself perpetrated the intrusion to obtain the files, the court failed to find that the intrusion tort had been established. It did state, however, "We approve the extension of the tort of invasion of privacy to instances of intrusion, whether by physical trespass or not, into spheres from which an ordinary man...could reasonably expect the particular defendant should be excluded." This echoes the Fourth Amendment's protection of areas in which the individual has reasonable expectations of privacy. In Dodd, the intrusion was accompanied by disclosure of the information without the consent of the data subject. Thus, it did redress the violation

---

350. Rhodes v. Graham, 37 S.W.2d 46 (Ky. 1931) (eavesdropping by use of a wiretap); Brex v. Smith, 146 A. 34 (N.J. 1929) (considering the issue of looking at an individual's bank account without his consent).
351. Id.
352. Prosser, supra note 34, at 390-91.
354. Id. at 704; see also MILLER, ASSAULT, supra note 30, at 174-175.
355. 410 F.2d at 704.
of the individual’s interest in his persona.  Similarly, the intrusion tort might be used to redress unauthorized access into personal home computers by third parties via modem.

Should the intrusion tort be applied only to individuals who lack authorization to access the information? Society could conclude that the tort should be applied to the individual who has authorization to access the information but who discloses the information without the consent of the subject. Whether the end-user knows the information he received had been improperly obtained should not be relevant to liability. Such a result would be in keeping with the prevailing view on misappropriation in trade secret law. Pursuant to the Uniform Trade Secrets Act, an individual cannot defend himself against a claim of misappropriation by alleging that he properly acquired the information if he is aware that his source misappropriated the information.

c. Public Disclosure of Private Facts

Public disclosure of private facts is the species of tort advocated by Warren and Brandeis. The tort is narrowly focused and requires the plaintiff to establish that private facts were actually communicated to the public at large. The definitions of “private” and “public facts” complicate the use of this tort to redress the use of computerized personal information without consent. It would be difficult to fit disclosures of personae on the secondary market into the public disclosure tort.

The cases in this area have refused recovery for publication of any information visible in a public place. An individual’s name is not ordinarily considered to be private or personal information. Despite this perception, an individual’s name can provide access to the social security number and the individual’s entire credit history. In addition, pieces of

356. In another case, the court considered several allegedly intrusive activities by General Motors and its agents into the privacy of consumer advocate Ralph Nader. Nader v. General Motors Corp., 307 N.Y.S.2d 647 (N.Y. 1970). These included having Nader accosted by young women making illicit proposals. Id. at 650. The court decided the case on narrow grounds, finding all of the conduct to be offensive but only the telephone tap and the surveillance to be actionable as intrusion torts, since only those activities could be said to be for the purpose of gathering information of a private and confidential nature. Id. at 654.


358. Warren & Brandeis, supra note 74, at 195-197. See also Prosser, supra note 34, at 392.

359. “It is an invasion of the right [against the public disclosure of private facts] to publish in a newspaper that the plaintiff does not pay his debts.” Prosser, supra note 34, at 393 (citing Trammell v. Citizens News Co., 148 S.W.2d 708 (Ky. 1941)).

360. The dissemination of the information to an unauthorized but consistent purpose user should constitute a violation. See MILLER, ASSAULT, supra note 30, at 184-85

361. Prosser, supra note 34, at 394.

362. Rothfelder, supra note 2, at 82.
information may be public in the traditional sense if disclosed separately but become private as they are combined with one another. At what point does the compilation of public facts give so complete a view of the subject that it should be considered private?\textsuperscript{363}

The unrestricted release of combinations of name and address has resulted in unfortunate consequences. Rebecca Schaefer was murdered in her apartment by an obsessed fan. After stalking her for two years, he obtained her address from a private investigator who requested the information from the California Department of Motor Vehicles. These records were available to the public in California for a fee. The fan used the information to go to Ms. Schaefer’s home, where he shot and killed her.\textsuperscript{364}

Even if information could be labeled private as opposed to public, the compilation of “private” information and “public” information in one profile might allow the dissemination of both. The traditional defense to a claim of public disclosure of private facts is that the published matter is of general public interest.\textsuperscript{365} The key question is how to distinguish between that information which is genuinely private and that which is of public interest. Borrowing from the constitutional arena, we can discern a number of areas which have been consistently labeled private and therefore protected.\textsuperscript{366} Perhaps these areas reflect the consensus of the public as to what arenas are truly private and therefore deserving of the greatest protection and consequently the greatest penalty for disclosure. In some cases, the courts have allowed recovery for disclosure to a limited public.\textsuperscript{367} Disclosure to one person would not be compensable unless the disclosure constituted a breach of contract, trust or confidential relationship.\textsuperscript{368}

In the absence of a special agreement between the individual and the merchant, there is no relationship of trust and confidence. Thus the disclosure of information concerning the individual’s transaction with the merchant would not be tortious. Computerized information would be hardest put to fit this tort category without statutory guidance.

\textsuperscript{363} See Miller, Assault, supra note 30, at 185-87.
\textsuperscript{364} Alderman & Kennedy, supra note 18, at 325. In response to this killing, California enacted legislation to restrict the disclosure of this type of information. Congress has enacted a law, to become effective in 1997, which will limit the disclosure of driving and registration records. Id.
\textsuperscript{365} See Sidis v. F-R Publishing Corp., 113 F.2d 806 (2d Cir. 1940).
\textsuperscript{366} See supra part III.B.
\textsuperscript{367} Miller, Assault, supra note 30, at 177.
\textsuperscript{368} Prosser, supra note 34, at 393.
d. The Torts of False Light and Defamation

The torts of false light and defamation are related. Defamation compensates the subject for the disclosure of inaccurate information concerning himself. Its applicability is limited by several requirements. The subject must show both financial and reputational loss. The alleged offender must not be privileged to disclose the information. The truth of the matter disclosed is a defense to a defamation action.

The disclosure of true personae will not be actionable under this tort. There is precedent, however, allowing recovery for the negligent disclosure of untrue electronically stored information to third parties. In *Greenmoss Builders*, Dun and Bradstreet issued a false report to five subscribers stating that Greenmoss was bankrupt. This report, in addition to Dun and Bradstreet’s recalcitrance in correcting the error, wreaked havoc on Greenmoss’s reputation. In awarding compensatory and punitive damages to Greenmoss, the Supreme Court stated “permitting recovery of presumed and punitive damages in defamation cases absent a showing of ‘actual malice’ does not violate the First Amendment when the defamatory statements do not involve matters of public concern.”

False light, on the other hand, redresses publicity which places the individual in a false light in the public eye. True information which is contextually inaccurate should be compensable under this form of the tort.

---

369. The privileges are twofold: 1) newspapers are privileged to print the newsworthy, and 2) the subject has consented to the disclosure. Prosser, *supra* note 34, at 412, 419.


371. *Dun & Bradstreet v. Greenmoss Builders*, 472 U.S. 749 (1985). While other federal statutes allow the individual to correct inaccurate information in records held about him, only the Fair Credit Reporting Act and the Privacy Act deal directly with protecting the individual’s rights in these records. The other statutes are the Fair Debt Collection Practices Act, 15 U.S.C. §§ 1692-1692o (1994), which regulates the manner in which debt collectors can contact the debtor, and the Equal Credit Opportunity Act, 15 U.S.C. §§ 1691-1691f (1994), which restricts the type of information which can be collected.


373. *Martin v. Johnson Publishing Co.*, 157 N.Y.S.2d 409 (N.Y. Sup. Ct. 1956). In this case, the plaintiff’s picture was used with a story captioned: “Man Hungry. She had a good man but that wasn’t enough . . .” *Id.* at 410. Miller suggests that this tort could be expanded to the personal data file that has become inaccurate due to the age of the information or has been reported out of context. *Miller, Assault, supra* note 30, at 184-85.

374. *But see Austin v. Bankamerica Serv. Corp.*, 419 F. Supp. 730 (N.D. Ga. 1974). In that case, Austin was denied credit on two occasions by the First Atlanta Bank. As its reason the bank cited a credit report which stated that Austin was a named defendant in a lawsuit. The report failed to state that Austin was named in this suit only in his official capacity as Deputy Marshal for DeKalb County. The court found for the defendant,
The definition of “public” must also be established in this context. Ostensibly, any disclosure of false information to a third party makes the information public. The usual case brought under this tort, however, deals with likenesses that have been used in advertising campaigns or news publicity and thus discloses the false light to a multitude of people. Although the potential scope of disclosure is broad for information accessible by virtue of computer-matching programs and data transfers, the public-at-large requirement of this tort should not be relaxed. This tort provides redress for a narrow spectrum of conduct in “news” publicity. Redress for the non-news agency publication of inaccurate information might be better addressed by other methods.

2. THE RIGHT OF PUBLICITY

The right of publicity involves “the use of the attributes of a generally identifiable person to enhance the commercial value of an enterprise.” This right is triggered when recognizable aspects of a person such as name, picture or voice are used commercially without the person’s permission; it provides a celebrity with “a right to damages and other relief for the unauthorized commercial appropriation of the celebrity’s persona.” The right is independent of the common law or statutory right of privacy. While the same usage might give rise to an action under both the right to privacy and the right of publicity, the rights do not cover the same type of interests. “The right of privacy protects individual personality and feelings, the right of publicity protects the commercial value of a name or likeness.”

The difficulty with fitting electronic personae under the wing of the right to publicity is that a persona is the object of both the right to privacy and the commercial marketplace. The persona is reflective of the individual’s personality with regard to his habits and patterns of spending and attitudes. As such it would come under the protection of

Finding that the report was true. This “technically correct” view of accuracy was not followed in Pinner v. Schmidt, 805 F.2d 1258, 1262-63 (5th Cir. 1986).


376. For a discussion of solutions to the problem, see infra part V.


378. Id. at 1200-01.


381. HALPERN, supra note 379, at 491.
privacy. It is this very quality which makes the persona valuable to the secondary market user. As an object of commerce, however, the persona relates more to the right of publicity than it does to the right of privacy. In *Haelen Lab, Inc. v. Topps Chewing Gum, Inc.*, the defendant chewing-gum manufacturer obtained authorization to use a ballplayer’s photograph in connection with the sales of defendant’s gum, despite defendant’s knowledge that the ballplayer already had granted the rights to plaintiff, a rival gum maker. Defendant argued that there was no actionable wrong because the contract with plaintiff was simply a release of liability from the use of ballplayer’s photograph, which would merely have been a violation of the ballplayer’s right to privacy. Thus defendant concluded that since privacy is a personal right and hence not assignable, plaintiff’s contract with the ballplayer vested in the plaintiff no “property” right or other legal interest which defendant’s conduct invaded. In denying defendant’s position, the court stated:

We think that, in addition to and independent of that right of privacy (which in New York derives from statute), a man has a right in the publicity value of his photograph, i.e., the right to grant exclusive privilege of publishing his picture, and that such a grant may validly be made “in gross,” i.e., without an accompanying transfer of a business or of anything else. Whether it be labeled a “property right” is immaterial; for here, as often elsewhere, the tag “property” simply symbolizes the fact that courts enforce a claim which has pecuniary worth.

The commercial marketability of the celebrity’s persona and the persona of the noncelebrity differ from the usual pattern, in that the persona’s value to the secondary user does not translate into the same type of value for the subject.

The confusion of the right to publicity and the right to privacy poses great problems for the protection of personae. The two theories protect two distinct interests of the individual. The right to publicity is founded on the presumption that the individual seeks exposure of his personality, and such exposure demands compensation to the individual for use of the persona. It is an economic interest subject to appropriation in exchange for consideration. In contrast, the right to privacy is premised

---

382. See, e.g., *Haelen Lab.*, 202 F.2d at 868-69.
383. *Id.* at 867.
384. *Id.* at 868.
385. *Id.*
386. *Id.* See infra part V. (concerning the inapplicability of this theory to the electronic persona).
on the individual's right to maintain a certain degree of solitude, the invasion of which can be punished.\textsuperscript{387}

3. COPYRIGHT AS PROTECTION OF THE PERSONA

The coextensive layers of interest held in the electronic persona create different property rights under copyright for the database compiler than for the subject of the persona. The individual's electronic persona is generally one of many compiled within a database. The entire database, rather than the individual persona, is offered for sale. The focus of the compiler's property right would depend upon the nature of the product created by the compiler.\textsuperscript{388} The facts as collected from public domain sources would not be subject to copyright protection. Rather, copyright protection derives from the manner in which the data are organized.\textsuperscript{389} There is authority recognizing that individual items within the database may themselves qualify for protection if unique authorship can be attributed.\textsuperscript{390} Essentially the compiler's right under copyright is to prevent others from copying the database as organized by the compiler.\textsuperscript{391} This right is indifferent to the individual's interest in preventing disclosure of his persona.\textsuperscript{392}

Only under limited circumstances would the law of copyright allow the individual to control the use of his electronic persona. Copyright protection attaches at the moment of creation for all "original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced or otherwise communicated, either directly or with the aid of a machine or

\begin{footnotes}
\item[\textsuperscript{387}] Peter L. Felcher & Edward L. Rubin, Privacy, Publicity, and the Portrayal of Real People by the Media, 88 YALE L.J. 1577, 1593 (1979).
\item[\textsuperscript{388}] There are three primary types of database products: those deriving value from their highly creative content; those deriving value from the organization of facts as they reflect the compiler's judgment as to relevance for potential users; and those deriving value from their comprehensive coverage of relevant facts. NIMMER, supra note 100, at 15-24. The electronic persona could be a part of a database of the second or third type.
\item[\textsuperscript{391}] See Copyright Act of 1976, 17 U.S.C. § 101 et seq. (1994). If the compiler offers the database in an on-line service, however, the value of the database would be in the compiler's ability to control access to the product. NIMMER, supra note 100, at 15-24.
\item[\textsuperscript{392}] See supra part V.A.
\end{footnotes}
device." Since the electronic persona is not "fixed in any tangible medium of expression," it would be outside the protection of copyright.

Assuming that this problem could be overcome by legislation, not all indicia of identity are copyrightable. While a name in a personal-information file does identify a specific person, there is no agreement that names are per se protected by copyright. Names and likenesses do not become a "work of authorship" simply because they are embodied in a copyrightable work such as a photograph. This is different from the right to publicity in which a cause of action is triggered by the unauthorized reproduction or other use of a name or likeness. Consequently, personal identity and the indicia by which they are recognized are outside the subject matter of copyright.

4. STATUTORY REGULATION OF COMMERCIAL USE

The federal statutes enacted to regulate the commercial use of personal information are diagrammed in the Appendix.

V. THE NATURE OF THE ELECTRONIC PERSONA—THE BLURRING OF THE DISTINCTION BETWEEN PUBLIC AND PRIVATE INFORMATION

Three considerations contribute to the difficulty of categorizing the individual's interest in the electronic persona. Those factors are the inadequate conceptualization of personal information as being the private property of its subject; the electronic medium, which makes traditional notions of privacy obsolete; and the public source of much of the information making up the persona.

The persona is a compilation of facts about the individual. Many of these facts can be obtained from the records of government entities.

393. "Works of authorship" which would be protected include literary works, musical works, dramatic works, choreographic works, pictorial, graphic and sculptural works and sound recordings. This right is limited in duration to the life of the author plus 50 years for individuals and the period of 75 years from the first publication or 100 years from creation, whichever expires first, for works made for hire or by employees. 17 U.S.C. § 302(a)-(c) (1994). See also Aldon v. Spiegel, 738 F.2d 548 (2d Cir. 1984).


395. The owner of a copyrighted thing acquires through copyright no property in the name by which it is designated. Lone Ranger v. Cox, 39 F. Supp. 487, rev'd on other grounds, 124 F.2d 650 (1941).


397. Some authorities would protect personal identity as a form of unfair competition. See, e.g., Restatement (Third) of Unfair Competition § 46 (1985). A full discussion of these issues is beyond the scope of this article. By analogy, however, copyright does suggest some solutions for allowing the individual to assert a property interest in the persona. See infra part V.
These records are collected by government entities pursuant to their regulatory functions. Conventional wisdom labels such records "public information." This means that, as a reflection of the workings of government, the information is a resource freely available to any seeker. Barring special circumstances, such information would most likely be disclosed despite the individual's desire to prevent its disclosure. It is this "public source" feature of the persona which prevents easy conceptualization of the individual's persona as private property.

Ultimately at stake here is society's conception of human identity and individuality. Currently, the content and accuracy of the persona depend on information compilation decisions made by parties unknown to the individual. This divests the individual of his ability to shape his own identity and control its manipulation. If the persona is merely a commodity to be manipulated at the whim of the collector, then the individual has no control over either his public face or private identity.

A. The Electronic Persona as Property in the Electronic Wilderness

The electronic persona is stored and manipulated in the database environment. It cannot be categorized as stock or material suitable for either traditional copyright or patent protection. The several layers of interests competing for its use make the electronic persona sui generis as property. Collected and stored in both government and private databases, the electronic persona is a valuable resource or property. Each database represents a bundle of competing rights in its use. The interests of the government, the public and commercial entities continually conflict with one another as they flow through commerce. The government needs to access personal information to determine eligibility for benefits or violations of lawful regulation. The public has a right to access this information to assist it in understanding the nature and scope of governmental activity. Commercial interests include the economic interest of a data collector, compiler or user in personal information about an individual. These three interests must achieve a balance, but none should be presumed superior to the others. Ultimately, the private nature of the information should allow the subject to control disclosure of the information to third parties.

As property, the electronic persona is like any other resource and should be managed accordingly by balancing the competing interests in

398. Post, supra note 24, at 648.
399. Heneghan & Wamsley, supra note 4, at 183.
400. See supra part IV.
401. Id.
its use. This does not mean that information easily fits our commonly held notions of property. In many ways, personal information does not conform to the existing definitions of either personal or intangible property. Ascribing property rights to information has been a difficult task for the law. Information is not destroyed in the act of consumption. It exists to be consumed again or by more than one person simultaneously. In this respect, it is the "classic public good" which all can enjoy in common. Physical commodities depreciate with use and must be replaced. Information need not depreciate with use and may, in fact, appreciate as knowledge and experience accumulate. Conversely, information can depreciate with non-use over time, and obscure knowledge that is not accessed becomes valueless.

Traditionally, the persona was classified as public or private information based upon whether its possessor was a public or private entity. This system of classification should be re-evaluated if the individual is to maintain any control over the disclosure of information about him. The tension between the public and the private reflects the notion that, as individuals, our identity is largely defined by the objects to which we can control access or own. We are identified by that which we own as distinguished from that which is commonly owned. If we can exclude others' access to an object, then the object is established as our property—it is private. On the other hand, everything that is not privately owned is considered to be within the common. Such an object may be used freely without regard to concurrent claims by others. This rule of common use lasts until rules determining the power of exclusion can be established to guide use of the resource.

402. Personal property is generally divisible into two types: 1) corporeal personal property, which includes movable and tangible things; and 2) incorporeal property, which consists of such rights as stocks, shares, patents and copyrights. RAY A. BROWN, THE LAW OF PERSONAL PROPERTY 9-12 (1975).

403. The difficulty is reflected in the complicated system of patents and copyright, which has been developed to protect against the unwarranted use of information as property. Porat, supra note 12, at 21.

404. Certain types of information are clearly public goods, such as television broadcasts and libraries. The only "price" that can be exacted is one of congestion or time costs faced by the library patron, or the (negligible) effect of people moving into regions that receive better [television] reception. Other types of information are strictly private goods, in that if one person owns them, the benefit to all others is zero.

405. Id. See supra introduction to part V.

406. See Radin, supra note 54, at 957-59.

407. This has been the history of the creation of all forms of property. See ROGER A. CUNNINGHAM, ET AL., THE LAW OF PROPERTY 1-29 (1984).
Privacy has never been viewed as a right without limitation. The law consistently balances the individual’s need for informational privacy with the needs of society for the collection and disclosure of personal information concerning the individual. A new view of privacy may act to balance these opposing forces.

No rules effectively balance the competing uses of a persona in the common of the electronic wilderness. Information is to the twentieth century what real estate was to the medieval economy—a basic resource that influences transactions. Modern society is an information society. Rules must now be developed to reconcile the variety of uses to which this resource is put.

B. The Merging of Privacy and Property in the Electronic Wilderness

The blurring of the public and private aspects of the persona is exacerbated by the way in which the electronic medium handles information. Until now, privacy has been considered to be an intangible attribute of a person in the physical world. As such, it was incapable of being possessed, alienated or controlled by a third party. On the electronic frontier, however, the individual’s privacy can be reduced to a “possession” and alienated from the real person when the personal information file is disclosed to a third party. Once stored electronically, these two aspects of personal information—the privacy of the individual and the nature of the file as a commodity—become inseparable. The substantive content of the information that can be identified with a specific individual and the nature of the information as a chattel merge. Once the information is disclosed through use, sale or exchange, the individual’s privacy is compromised. Privacy therefore becomes property in the electronic milieu. This use of electronically stored personal information thus requires a joint evolution of our traditional notions of property and privacy if the individual is to have any effective control over his persona and how he is viewed in the community.

Historically, locking out the public was an effective method of maintaining control over one’s property. Contemporary computer technology has eliminated such a simple solution. The individual cannot “lock out” the government once he has divulged his persona to it. While

408. Computer technology, which dramatically facilitates the transfer of this commodity, has transformed the world into a global village in which the domain of strictly private action is steadily being eroded. See Porat, supra note 12, at 19-22.

409. Since this common resource is managed by use of a means of interstate commerce (telephone, satellite, etc.), any statute regulating this resource must be federal to ensure consistent treatment. See infra part V.D.
computer security laws will protect the persona to an extent, security will not prevent an authorized record keeper from unauthorized secondary use or disclosure. Computer technology makes the privacy of the persona alienable in the sense that it can be separated from the subject individual. Access to the persona in the database performs the function of publishing personal information in the physical world. If the record keeper is given exclusive rights to disclose the persona to any third party, then the individual’s privacy interests in that information have been alienated. In this manner, privacy and property meld in the electronic milieu.

This is contrary to the common law view of privacy as an inalienable right of the individual. At common law, privacy rights may be waived, but they cannot be sold, transferred or appropriated. By contrast, the persona and, therefore, the individual’s privacy can be sold by any holder of the file. It can be transferred to any number of parties with or without the knowledge of the subject individual. The privacy of the individual is appropriated by the act of disclosing the file. These characteristics make the electronic persona sui generis. The persona is a unique combination of privacy and property rights that requires a new view of existing doctrine if society is to successfully balance those interests which compete for its use.

On the frontier, electronic personae are merely indistinguishable parts of a larger database sold as a commodity. While the database itself may be considered property by the collector, the individual files constituting it are not recognized as the property of the data file subject. The distribution chain of these databases makes it relatively easy to lose sight of the individual’s interests in any single persona contained within it. The database can be sold or transferred to a series of database users in commerce, each user modifying or redistributing the database as he sees fit. The database can also be transferred between two agencies pursuant to the agencies’ functions. Since each user following the original collector can modify the information within it, each user claims a variety of rights to the persona as it moves along a distribution chain. Most of these rights

410. Prosser, supra note 34, at 408.
411. See discussion supra part IV.F.1.a. concerning use of the appropriation tort to protect the persona. The appropriation tort stands between personal tort and property rights concepts. RESTATEMENT (SECOND) OF TORTS § 652 cmt. a (1977); MILLER, ASSAULT, supra note 30, at 23.
412. In the following cases, the database is considered to be a good: Daniel v. Dow Jones, 520 N.Y.S.2d 334 (N.Y. 1987); Gutter v. Dow Jones, 490 N.E.2d 898 (Ohio 1986). In both instances, the plaintiff sought compensation for sustaining damages due to reliance on an inaccurate database.
are based in property concepts. The interests of these users are entirely different from those of the subjects of individual files within the database. The individual's problem is particularly acute if the persona collected by government is viewed as being within the public domain and not property of the individual. The persona is simultaneously a valuable resource for the record keeper and a reflection of the individual's identity. To date, the value as a commodity to the user has been given precedence over the value to the individual.

C. Public Source of the Persona

Information collected from a public domain source and not otherwise protected by copyright is considered to be "public" information regardless of its personally sensitive nature to a specific individual. Credit and bank records, school records, medical records and policy records all directly affect the individual's or organization's ability to function in society and, as such, have "value," but they are not uniformly protected in any manner. Having been recorded pursuant to a government's interaction with an individual, the information is considered to be "public" and therefore freely subject to disclosure by the holder to third parties. The individual's interest in nondisclosure is not recognized. In fact, the policy of government is to disclose the happening of certain transactions: birth, driving records, marriage, divorce, real estate transfers, employment and death. These "public records," although highly personal, are often freely available to any inquirer. The individual's desire for privacy, in the form of nondisclosure, yields to the government's right to publish this information.

The exchange of personal information records from the public to the commercial arena is based on the understanding that the information from which the database is compiled is not protected from secondary use by virtue of law. The government makes no contract of confidentiality with the individual. Neither does its disclosure of public records breach any trust with the individual. Individuals cannot ordinarily claim that the government has a confidential relationship with them. The government is therefore not prohibited from disclosing most of its information under the freedom of information laws. Since such information is an unowned resource, it can become a chattel to the user.

413. See discussion supra parts IV.A.-C.
414. See infra App.
415. See discussion supra part IV.D. concerning the tension between the public's interest in the publication or disclosure of the information and the individual's right to prevent disclosure.
who collects and compiles it. Its nature as a chattel is determined primarily by the identity of this collector, so that the collector is free to collect, compile, store and disclose any factual information it legally acquires.

The individual's interest is impacted by the exchange of these data in several ways. A collector may make and keep a record about the individual in order to maintain a relationship with the individual. The collector may keep this record to document its own actions to a regulating institution, so that the regulating entity can monitor the activities of not only the collector but also the activities of the individual.

Since in the public domain this information is an unowned resource, the parties to its exchange have the right to agree between themselves what type and how much information concerning individuals they may acquire. Their decision to collect the information is not necessarily limited by the lack of a present need for the information. In addition, the holder of the information is not ordinarily restricted in his ability to decide to whom and when the information may be disseminated.

In any event, the concerns of the person behind the persona are not taken into consideration. There are several reasons for this omission. While the electronic persona may hold highly personal information, the individual can not be said to "possess" it since he did not compile the particular persona at issue, nor does he have an ownership interest in the database which houses it. In the absence of these obvious ownership attributes, the assumption has been that the individual can restrict neither the collection nor the disclosure of the persona to anyone. Such information is essentially free. Any limitations placed on parties' ability to collect or trade information in the market are tied only to specific statutes.

The public source of the basic data comprising the electronic persona need not be determinative of the persona's status as "public" information. There is authority for the proposition that availability from


418. Banks maintain a number of records on transactions between themselves and the federal government pursuant to federal nondiscriminatory policies in credit and mortgage applications. See, e.g., Equal Credit Opportunity Act, 15 U.S.C. §§ 1691-1691f (1994).

419. Graham, supra note 290, at 1397-1402.

420. Id.

421. See, e.g., Equal Credit Opportunity Act, 15 U.S.C. §§ 1691-1691f (1994) (restricts the collection of information which could be used to discriminate against the individual on the basis of race, religion, sex or marital status in the granting of credit).
one public source does not make a compilation of that information public. This means that while the data may be public and available for disclosure at various source collection points, a compilation of that data can be protected from disclosure. In *D.O.J. v. Reporter's Committee for Freedom of the Press*, the United States Supreme Court refused to require the government to disclose an FBI compilation of an individual’s rap sheets from several jurisdictions across the country.422 The Court determined that while the record of each infraction was a public record in the jurisdiction in which it occurred and would have been freely disclosed there, release of the compilation constituted an “unwarranted invasion of individual privacy.”423 The Court based its decision on the fact that, although single entries reflecting each agency’s interaction with the individual were public, once compiled with similar information from several jurisdictions, the data became more a persona of the individual than a reflection of the information-collection activities of government. Disclosure of such information was not within the parameters of a proper FOIA request, and therefore the exemption from disclosure was properly invoked.

*Reporters Committee* established that the persona’s public record roots do not necessarily render the persona itself a public record. Consequently, compilations of facts can be protected by the property rights derived from the privacy claims of the individual about whom the persona is collected. *Reporters Committee* also implies that merely being recorded by a public institution does not necessarily mean that such information is of “general knowledge” and therefore immune to the individual’s privacy claims.

The law of copyright and trade secrets also supports the notion that the compilation of data ostensibly residing in the public domain can give rise to a variety of enforceable property rights in information.424

D. Scope of the Property Right

Full protection for individuals in their persons and property is a principle as old as the common law, but from time to time we must define anew the exact nature and extent of such protection.425

424. See discussion supra part IV.F.3. (concerning copyright as protection of commercial interests in the persona). See also PAUL GOLSTEIN, COPYRIGHT 85-98 (1989); UNIFORM TRADE SECRETS ACT, supra note 357, at 434-36.
One hundred and six years ago, Warren and Brandeis found themselves in the position of describing a new sphere of protection for individuals in the face of modern technological advancement. The growing use of computerized databases to store and disseminate personal information puts us in much the same position in 1996. Computer technology has created several problems for individuals seeking to maintain a small degree of solitude in the electronic wilderness. In that wilderness, the individual's privacy, in persona form, is being manipulated by various users. As the persona passes through the successive hands of the collector and user, its identifiability to a specific individual is not recognized in any sphere. Consequently, the electronic persona is largely unprotected from public, commercial and governmental collection and disclosure in the secondary market. This imbalance is enforced by the existing information-regulation structure.

Current problems of protecting the individual's privacy are myriad. The malleable nature of the persona makes its conceptualization as a definitive piece of property difficult. Since each persona was compiled by a different collector or user for that entity's own purposes, a single individual may have many different personae with varying characteristics. There is no consistent mechanism requiring the individual's consent prior to disclosure. Currently, as a matter of law, an individual in possession of information has the right to disclose it. Since the interests of the information collector or user are not coextensive with those of the individual, neither the collector nor even the user can give a valid consent for disclosure on behalf of the individual. No rules currently establish a consistent pattern in the respective duties of persona users and information collectors to the subject of the personal information file. Access to the persona is not limited to those with a legitimate need for the information. Moreover, there are few effective sanctions against unauthorized users. There are even fewer incentives to encourage the policing of access by the "possessor" of the electronic persona. 426

In addition to these problems, the individual does not have a guaranteed right to discover the existence of records collected about him, and the informational accuracy of these records is not generally mandated by law. 427 There is no clear view of the nature of the harm which will trigger a claim for breach of informational privacy. Assuming that the individual is harmed by the nonconsensual disclosure of his persona, there has been no determination as to whether a cause of action must be premised upon a finding of tangible loss. Likewise, there is no determination as to whether merely a finding of a nonconsensual

426. See Westin, supra note 31, at 158-63.
427. See infra App. (detailing the number of statutes requiring contextual accuracy).
disclosure of personal information will be sufficient to support a cause of action. Finally, there is no consistent pattern establishing the penalties that will be imposed for a violation of the individual's rights.

The resolution of the problem of regulating the myriad interests in the persona should begin with reference to the law of property, since property concepts have long been used to balance competing interests in valuable resources. The prime example of such use of property law was the creation of the many estates in land in common-law England. In the agrarian economy of medieval Europe, the primary object of the economy was real property. Property rights were created by the state to establish a balance for orderly use of a common resource. To fully utilize this resource, a complex set of rules surrounding its ownership developed. The basic concept of these rules was the common but specifically delineated usage of privately held property. This was demonstrated by the creation of a variety of rights of possession, or "ownership," which could be recognized in one parcel of real estate.428

By way of analogy, each of the four interest groups—the individual, the commercial, the public and the government—could have a property interest in the individual's persona. How can these interests be balanced as the persona is transferred from collectors to successive users? The resolution of the problem hinges on a determination of which party has the strongest rights to the property as it passes through a succession of hands. Such a resolution should establish the respective responsibilities of the parties along the electronic distribution path and must necessarily rank the need for the use of the electronic persona in determining the appropriateness of its further disclosure.

The persona should be viewed as property, the ultimate "ownership" or "fee simple" of which resides in the individual. The rights of any other entity (i.e., any group, class, association or government) that might obtain, access, make use of or disclose the persona would be subordinate to those of the individual. As with other forms of property, the individual's right to restrict the use of his persona by others would vary depending upon the reason for the use.429

428. For example, a parcel of property may be owned in fee simple by X, with a life estate in Y, a lease of five years in Z, and a sublease in AA and rights to farm in BB and mineral extraction rights in CC. The same phenomenon is recognized in personal property as bailment. We term the person in whom the various rights in a thing normally and customarily reside the "owner" thereof, and one of the attributes of his ownership is the power to confer upon others one or more of his various interests in it while retaining others. BROWN, supra note 402, at 7.

429. See discussion infra part V. (concerning ranking of these uses); Trubow, supra note 8, at 821-22 (discussing the changing nature of the relationship between the interest in disclosure and the interest in maintaining the privacy of the information "depending on the role of the party seeking disclosure or privacy").
The recognition of a property right in the individual about whom the persona is collected does not detract from the interest any collector or compiler of databases may have in the same persona. It does mean, however, that any information-collector's interest would be "subject" to that of the individual in some important respects. A basic premise of the law creating this property right should be that the identity of the holder or the information (government or private) industry would not determine the nature and extent of protection provided the individual. This is consistent with the current balancing of interests required both constitutionally and by existing regulatory statutes.

The property analogy is not without its difficulties for the electronic persona. Historically, the protection of any property was based on the presumption that the object to be protected had a consistent configuration regardless of the holder's identity. In contrast, the electronic persona is characterized by its mutability. Created and continually manipulated by parties other than the individual, the electronic persona may be the compilation of any variety of pieces of personal information. The key to recognizing a property interest in the electronic persona must be based in the identifiability of the persona to a specific individual. Once that link has been established, the persona "belongs" to the individual about whom it "speaks" without regard to the source or content of the specific pieces of information constituting it. Thus the electronic persona could be defined as a collection of at least three pieces of personal information concerning the individual (or those for whom he is responsible) that identifies the individual(s): for example, name, social security number, selective service number, fingerprint, etc.

The common-law view was that an owner could never be deprived of his ownership rights without either consent or compensation.430 This theory is the basis of the current protection of identity as persona under the intellectual property doctrines of the right to publicity, misappropriation and copyright.431 Each of these doctrines is premised on the protection of various indicia of a specific person's identity from its commercial exploitation or use by a third party.432

Applying this view to a holder's use of the persona would suggest that any holder of the persona must bargain with the "owner-subject" for the right to use the information.433 The bargaining would involve

430. See discussion supra part III.A.
431. See discussion supra part V.B.
432. NIMMER & NIMMER, supra note 4, at 1-22 to 1-24.
negotiations for the price or use of persona. While there are often elements of financial gain in the use of the electronic persona by a holder, a profit motive is not always the primary incentive for its use. Governments, insurance companies, hospitals and schools all use the persona in the course of their respective operations but do not directly or consistently make a profit from this use. Thus, requiring payment for the use of the persona would not be appropriate in many circumstances, though the holder's ability to use the persona could still be regulated. The law does not require compensation for the appropriation of all valuable property. Ideas can be very valuable, but their use need not be compensated under the copyright law.\textsuperscript{434} The historic treatment of information from public sources has precluded the need to pay for such information's use per se.

On the other hand, the failure to require payment for use of the persona does not negate the need to recognize a protectable property right in the subject individual. If information is the driving force of the economy, then its use must be regulated for the benefit of all society and a valid consent must be procured for its use. A pre-disclosure consent requirement does not necessitate compensation for the persona's use. The focus of any uniform persona-protection statute should be on the electronic persona which is specific to an individual. The privacy sought on this new terrain of the electronic wilderness would give an individual a legally recognized power to manage the distribution of his persona. The privacy would have two aspects. First, it would allow the individual to regulate the extent to which any third party could obtain, access, make use of or disclose a persona concerning him or those for whom he is personally responsible.\textsuperscript{435} Secondly, this privacy would empower the individual to monitor and correct the accuracy of a persona compiled concerning him or those for whom he is personally responsible.

For the individual to exercise this power, he must be able to control the information-collector's disclosure of the persona to third parties. A statute creating an agency relationship between the information holder and the individual for the purposes of regulating the secondary use of the persona would be an effective method of securing this power to the individual. The holder's duty as agent would be to use the information consistently with the purposes for which it was collected from the

\textsuperscript{434} Ideas are considered to be in the public domain and uncopyrightable. See 17 U.S.C. § 102(b) (1994). See also Nimmer & Nimmer, supra note 4, at § 16.01. This concept applies here, since a great deal of the information from which the persona is collected comes from "public" or free sources.

\textsuperscript{435} The term "individual" would be broadly defined to include natural persons, groups, classes, associations or government.
individual and to refrain from disclosing or allowing access to the information to a third party without the individual's consent. The privilege of the holder to use and disclose the persona would carry a double warranty: a warranty of authority to disclose and a warranty of accuracy.

Under the warranty of authority to disclose, the holder would be required to determine from the individual the extent to which secondary disclosure of the electronic persona is acceptable before the holder could disclose the information to a third party. This duty would be imposed upon the holder at the time he acquires the electronic persona. Any breach of the duty through "improper disclosure or access" should result in the higher of either statutory damages or actual damages. Attorneys fees should be provided, and criminal penalties similar to those provided by FCRA should penalize willful disclosures. Anyone in the distribution trail of the persona would automatically become subject to this duty, whether or not he had dealt directly with the individual. A secondary holder would be deemed a collector, and would be required to obtain a grant of authority from the subject of the records before either further disseminating the persona or creating a new persona by adding new information. The warranty of authority to disclose would not be transferable.

Concurrent with the warranty of authority to disclose would be a warranty of accuracy. This warranty would run to any collector or user of the information who disclosed the information to a subsequent user. It would warrant that the persona as compiled was accurate as of a specific date. Such a requirement would give the holder an incentive to make sure the persona was accurate and give the individual an added opportunity to challenge the accuracy of information before any damage is done by its disclosure. In essence, the proposed law would give the individual a right to informed consent in the disclosure of his persona.

When a user in the secondary market acquired an individual's electronic persona, he would be required to notify the individual that information had been collected concerning him and to obtain his permission to disclose the information. The holder would also have to send a copy of the information he intended to disclose to the individual,

436. At common law, a breach of the warranty of authority would subject the unauthorized agent to liability on a contract entered into purportedly on behalf of the principal. See Albert S. Abel, Some Spadework on the Implied Warranty of Authority, 48 W. Va. L. Rev. 96, 110 (1942).

identifying the source of the information. The individual would then be
given a reasonable amount of time to respond. If the individual
 disagreed with the accuracy of the information or declined to have the
information reported, then the agent would have the duty to act
accordingly. An individual’s failure to respond within the allotted time
would allow the agency to disclose the information.

These duties and disclosure provisions would not apply to
information not readily identifiable to a specific person, or to information
collected pursuant to criminal or other governmental investigations of a
specific individual.

A limited license to use the information for like purposes should be
recognized in government matching programs. Since notice to the
individual concerning the match must be sent to the individual before
any adverse action is taken, no additional burden has been placed on the
government. This means that the reasons for the disclosure are a
necessary part of the inquiry as to whether the files can be disclosed
pursuant to the collector’s warranty of authority to disclose.

In addition to the warranties of authority to disclose and of
accuracy for holders of the persona, those who give information pursuant
to confidential investigations would be required to warrant the truth of
their observations or statements. If the information given were later
found to have been false, then the confidentiality of their identity would
cease and they would be subject to damages to the individual. The
individual should have ready access to any information, including
medical records, which are collected about him.438

The proposed statute should make the accounting provisions of the
Privacy Act applicable to all statutes that govern the collection or
disclosure of personal information. This would give the individual an
opportunity to discover the existence of records concerning him and
whether they had been disclosed to third parties. The addition of an
annual review opportunity for individuals would enable the individual
to properly assess the extent of his exposure.

Finally, the proposed statute would require all organizations
maintaining files containing personal information about individuals to
rank their personnel with respect to their ability to access the personal
information files about others. The ranking should be based upon the
sensitivity of the information to the individual and the need of the
personnel to access the information in their duties for the organization.
The information holder should develop required procedures for accessing
the electronic persona which are proportionate to the nature and

438. Unlike the FCRA, the Privacy Act does allow the individual to request
potential impact of the data's disclosure upon the individual. There is precedent for such a result.439

VI. CONCLUSION

Technology has changed the manner in which the individual's identity is forged. Determining the source of the individual's identity is at the core of this controversy: Should the law continue to make a "market-created persona" the predominant force in rendering decisions about the individual, or should the law protect personal information based on the presumption that the individual's identity resides in his own capacity to act and correct misperceptions?

Since the persona is identifiable to a specific individual, the electronic persona is "owned" by that person despite its configuration. It is this very identifiability which makes it property. Following this premise, an individual needs certain legal powers over the use of his electronic persona. The suggested provisions could provide a modicum of solitude to the individual as he seeks shade in the land of perpetual sunlight—the electronic wilderness.

---

439. Personae should not be based upon the fact that criminal charges were at one time filed against an individual, but later dropped. See Brown v. Jones, 473 F. Supp. 439 (N.D. Tex. 1979); see also In re Bagley, 513 A.2d 331, 340 (N.H. 1986) (discussing the need to notify persons who have criminal records or charges filed, stored and later used without their knowledge). These cases take the position that preliminary matters which are potentially embarrassing cannot be disclosed (i.e., arrest without conviction or the filing of a lawsuit without finding of liability). Wisconsin v. Constantineau, 400 U.S. 433 (1971) (the individual should be afforded an opportunity for a hearing before highly derogatory information is generally disclosed). See also NIMMER, supra note 100, at 16-26.
# VII. APPENDIX: COMPARISON OF FEDERAL STATUTES REGULATING INFORMATIONAL PRIVACY

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Purpose[^442]</strong></td>
<td>Prohibits warrantless searches by government where individual has reasonable expectation of privacy.</td>
<td>Amend FOIA to: 1) give individual right to request access to records about him[^442] 2) prevent agency disclosure of personal information to third parties without subject’s consent.</td>
</tr>
<tr>
<td><strong>3. Discovery Right[^448]</strong></td>
<td>Discovery rights as provided by the rules of discovery, or Freedom of Information Act (FOIA).</td>
<td>No. Only publishes character of the record system and category of individuals covered[^449].</td>
</tr>
<tr>
<td><strong>4. Collection Restrictions[^450]</strong></td>
<td>Probable cause required for search or warrant procured. Collection violates other constitutional rights[^451].</td>
<td>Information must 1) be relevant to the agency’s use[^452] and 2) must inform the individual whether collection is mandatory or voluntary[^453].</td>
</tr>
<tr>
<td><strong>6. Right to Access[^455]</strong></td>
<td>&quot;Search&quot; of area within individual’s &quot;expectation of privacy.&quot;</td>
<td>Individual believes he is included within the character of the record, and category of individuals in a system of records, and makes an inquiry[^457].</td>
</tr>
<tr>
<td><strong>7. Accuracy Dispute Resolution[^458]</strong></td>
<td>N/A</td>
<td>Yes. Opportunity for agency review[^459].</td>
</tr>
<tr>
<td><strong>8. Penalty for Breach[^460]</strong></td>
<td>Suppression of the information collected, or § 1983 damages under certain circumstances.</td>
<td>If individual suffers &quot;adverse effect,&quot;[^461] actual damages and attorneys fees. For willful acts, actual damages and attorneys fees[^462]. Fraudulent requests are misdemeanors—fine of $5000.</td>
</tr>
<tr>
<td><strong>9. User Friendliness[^463]</strong></td>
<td>Supreme Court reluctant to expand protection to breaches using new technology.</td>
<td>Twelve exemptions to confidentiality[^564]. Washington location viewing only. No requirement to identify third-party sources. No agency monitors record-keeper’s compliance with PA.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Amends PA to limit the collection of information from individuals. (^{465}) Provides guidelines for matching data about the same individual between agencies. (^{466})</td>
<td>Limits collection of information from individuals, and saves government money. Relates to information collection requested of government agencies. (^{467})</td>
<td>Establishes procedures allowing police to obtain information from newspapers. (^{468})</td>
</tr>
<tr>
<td>Records of governmental agencies. The match need not be with a federal agency.</td>
<td>Records held by individuals needed for government administrative functions. (^{469})</td>
<td>Records and information held by newspapers.</td>
</tr>
<tr>
<td>Yes, if termination of an individual's benefits is contemplated pursuant to the match. (^{470})</td>
<td>The act does not create a private right of action. (^{471})</td>
<td>No.</td>
</tr>
<tr>
<td>Formal agreement between matching agencies required. (^{472}) Matching programs limited to 18-month duration unless renewed. (^{473})</td>
<td>Must inform public of reason for need of information. Need OMB approval to collect if no other agency has the information. (^{474})</td>
<td>Yes. Guidelines provided by which documentary evidence can be obtained. (^{475})</td>
</tr>
<tr>
<td>Agency publishes notice prior to conducting or revising the matching program. (^{476}) Any agency wanting to match must establish Data Integrity Board. (^{477})</td>
<td>Agencies may share information as long as the exchange is not inconsistent with law. (^{478})</td>
<td>N/A</td>
</tr>
<tr>
<td>Data subject informed that termination of federal benefits will result because of adverse information found in match. (^{479})</td>
<td></td>
<td>No. See row 3 above.</td>
</tr>
<tr>
<td>Agency must independently check accuracy of information before taking adverse action. (^{480})</td>
<td></td>
<td>No.</td>
</tr>
<tr>
<td>Same as PA penalties. (^{481})</td>
<td>If information is released contrary to law, penalties apply to both releaser and collector. (^{482})</td>
<td>Yes, against government which has waived sovereign immunity, and officer acting under color of office. (^{483}) Statutory damages and attorneys fees. (^{484})</td>
</tr>
<tr>
<td>Individual might find accuracy-challenging procedure to be cumbersome.</td>
<td>See row 3 above. PRA cannot be used as exclusionary rule. (^{485})</td>
<td>Jurisdiction resides in federal district court. (^{486})</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>1. Regulates manner that government gains access to bank records about individuals.</td>
<td>Amends the Privacy Act and limits disclosure of student records to third parties.</td>
<td>Limits the disclosure of &quot;consumer reports&quot; or &quot;investigative consumer reports&quot; to third parties (i.e., &quot;users&quot;) by &quot;consumer reporting agencies.&quot; (CRAs).</td>
</tr>
<tr>
<td>2. Records of an individual’s banking transactions maintained by the bank.</td>
<td>Records maintained by any educational institution receiving federal funds.</td>
<td>Records held by consumer reporting agencies.</td>
</tr>
<tr>
<td>3. Individual given advance notice by governmental agency and opportunity to challenge the disclosure, except no notice to individual if disclosure is limited.</td>
<td>Yes.</td>
<td>None for consumer reports. Yes, if CRA compiles investigative consumer report, but only if information is sought to determine insurability or eligibility for government benefit.</td>
</tr>
<tr>
<td>4. Procedures for disclosure must be followed before government obtains records.</td>
<td>N/A</td>
<td>None in the absence of a specific agreement between the individual and the original collector of the information.</td>
</tr>
<tr>
<td>5. The bank can notify the government about existing files.</td>
<td>Consent generally required before disclosure made to a third party.</td>
<td>Use limited to legitimate business use, but few checks on veracity of requests.</td>
</tr>
<tr>
<td>6. Notice to individual that government request was made, or individual’s subsequent discovery of disclosure within three years of alleged violation.</td>
<td>Notice to individual that disclosure is requested, or discovery by student or parent of nonconsensual disclosure.</td>
<td>Upon denial of benefit.</td>
</tr>
<tr>
<td>7. N/A</td>
<td>Yes.</td>
<td>Yes, but disputed information is reported along with individual’s statement to contrary.</td>
</tr>
<tr>
<td>8. Injunctive relief, costs, and fees; damages of $100, or actual damages plus fees if successful; and punitive for willful violation.</td>
<td>Denial of federal funding to the institution, but no individual cause of action.</td>
<td>Yes. Actual damages plus attorneys fees for negligent violations, and punitive for willful violations. False pretense obtaining of credit report is punishable.</td>
</tr>
<tr>
<td>9. Only the records of the individual's account are covered.</td>
<td>Coverage ceases when the student graduates. Limited remedy provisions (see Row 8 above).</td>
<td>More than one CRA may hold a file, and there is no requirement that corrections to one file be sent to others. Notice not required until after benefit denied.</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Prevents &quot;videotape service provider&quot; from disclosing personally identifiable information concerning individual's tape selection to third parties.(^{511})</td>
<td>Promotes open government by disclosing information relating to the workings of government.(^{512})</td>
<td>Creates a property right in personal information (persona) related to a specific individual (subject) by any identifier.</td>
</tr>
<tr>
<td>Records held by videotape service providers in a business affecting interstate commerce.</td>
<td>Government office and/or agency records.</td>
<td>Any personal information record held, collected, or accessed by any party other than the subject.</td>
</tr>
<tr>
<td>Can disclose individual's name and address with individual's prior permission,(^{513}) or a customer list which doesn't reveal the subject matter of any video rented.(^{514})</td>
<td>Yes, if record relates to functioning of government agency.</td>
<td>Yes. Restrictions imposed by warranty of authority and warranty of accuracy.</td>
</tr>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>Yes. Accounting provisions of the PA apply. Notice given to subject before persona disclosed to third party. Annual review of persona by subject.</td>
</tr>
<tr>
<td>Disclosure can be made to the individual,(^{515}) or pursuant to a warrant or court order.(^{516})</td>
<td>Disclosure prohibited if it fits one of seven exemptions.(^{517})</td>
<td>Yes. Holder must have subject's consent before allowing disclosure of persona to third person.</td>
</tr>
<tr>
<td>Yes. Information may be disclosed to the subject upon request.(^{518})</td>
<td>Provides procedures for disclosure of information.</td>
<td>Yes. Greater of statutory damages or actual damages, and attorneys fees. Criminal penalties like FCRA for willful violations and false pretenses.</td>
</tr>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>Yes. Accounting provisions of the PA apply.</td>
</tr>
<tr>
<td>Action must be brought within two years of discovery of breach. Actual damages, punitives plus attorneys fees, and other equitable relief. Liquidated damages require at least $2,500.</td>
<td>Action can be brought to enforce disclosure.(^{519})</td>
<td>Yes. Each holder must verify accuracy of record with subject.</td>
</tr>
<tr>
<td>Punitive damages and attorneys fees are available (see row 8 above).(^{520})</td>
<td>Only records indexed in a particular manner need be disclosed.(^{521})</td>
<td>Burden of disclosing existence of persona resides with person in possession of the information.</td>
</tr>
</tbody>
</table>
In 1973, the House Education and Welfare Secretary formed a committee to evaluate the then-perceived challenges to personal information privacy posed by computers. The committee, named the Advisory Committee on Automated Data Systems, issued a report entitled "Personal Data Systems: Records, Computers and the Rights of Citizens." *Automated Personal Data Systems*, supra note 36. This report listed five factors generally believed to be necessary to protect the individual's interest in personal information collected about him. Those factors were: (1) the individual should be able to find out what files concerning him exist; (2) when the individual provides information concerning himself, he should know how the information is to be used and how broadly the information should be disclosed; (3) if the record holder wants to disclose the information more broadly than originally contemplated, consent of the subject of the record should be obtained; (4) the individual should have access to files concerning him and the opportunity to correct inaccurate information; and (5) files should be afforded adequate security and outmoded information should be updated. *Greenawalt*, supra note 97, at 57. This Appendix compares these stated goals with the provisions of nine federal privacy statutes passed by Congress during the past 30 years, and with the Fourth Amendment to the U.S. Constitution. Finally, these existing provisions are compared to a proposed uniform personal information protection statute. This statute, the "Uniform Electronic Persona Protection Act," is one attempt to create an electronic environment in which each of the five aforementioned factors can be achieved.

To the five goals I have added: Row 1, "Purpose," describing the purposes of the enactments; and Row 2, "Records Covered," describing the types of records covered. The five goals of the 1973 study are included in Rows 3 to 7 respectively, as follows: Row 3, "Discovery Right"; Row 4, "Collection Restrictions"; Row 5, "Restrictions on Secondary Use"; Row 6, "Right to Access"; and Row 7, "Accuracy Dispute Resolution." Additional rows include: Row 8, "Penalty for Breach" of the individual's privacy by the collector; and Row 9, "User Friendliness," which describes the relative ease with which the individual is provided the benefit of persona integrity.

The names of the statutes evaluated appear at the head of each column. The final column compares the provision of the proposed Uniform Electronic Persona Protection Act to the existing constitutional and statutory provisions. One other provision impacts computer-based records. This statute is the Omnibus Crime Control and Safe Streets Act of 1968 (OCCA), 18 U.S.C. §§ 2510-2520 (1994) (as amended by the Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 101 Stat. 1848 (1986)). It does not deal with computer-stored records per se; rather, it focuses on the protection of the transmission of such data electronically.

The OCCA prohibits the interception of wire or oral communications without a court order. There are three exemptions to this prohibition: 1) interception by a switchboard operator or other communications company employee monitoring mechanical or service quality; 2) interception by a Federal Communications Commission employee; and 3) interception by a party to the conversation, or a person who has the consent of a party to the conversation. Also prohibited is the manufacture, distribution, possession or advertising of devices primarily useful for the surreptitious interception of wire or oral communications. The ECPA expanded the protections of the OCCA to include any type of electronic communication including computer data transmission. *Id.*

The Fourth Amendment reads as follows:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.
442. This row sets forth the purpose for which the statute was enacted. The purposes are not always the protection of privacy, although each statute does have the effect of protecting informational privacy by virtue of its operation.

443. See 5 U.S.C. § 552a(d)(1) (1994). The agency is also required to give the individual a copy of the record if the individual wishes. The information must be given in a form comprehensible to the individual. \textit{Id.}

444. This row describes the type of records covered by the enactment.

445. See 5 U.S.C. § 552a(a)(4) (1994). “Record” has been interpreted to mean any tangible information which reveals something about the individual. See, e.g., Albright v. United States, 631 F.2d 915 (D.C. Cir. 1980) (videotape of an argument between a supervisor and an employee held to be a record). However, in American Fed’n of Gov’t Employees v. NASA, 482 F. Supp. 281, 283 (S.D. Tex. 1980), the court found that employee sign-in sheets were not “information that is substantively, i.e., in and of itself, reflective of some quality or characteristic of an individual.” The court apparently did not feel that a consistent pattern of late sign-ins would be indicative of the individual’s work habits.

446. 5 U.S.C. § 552a(a)(2) (1994) defines the individual as “a citizen of the United States or an alien lawfully admitted for permanent residence.” This is different from the definition of individual in FOIA. Thus, under the Privacy Act corporations and other business entities do not have the right to seek information about them.

447. The individual cannot have access to the record nor prevent its disclosure unless the record is a “record” under the Act, and is part of a “system of records” as defined by 5 U.S.C. § 552a(b) (1994). A system of records includes any group of records under agency control that is indexed and can be retrieved by use of an individual’s name or other identifier. 5 U.S.C. § 552a(a)(5) (1994). This definition has been interpreted restrictively. See, e.g., Smiertka v. United States Dep’t of Treasury, 447 F. Supp. 221 (D.D.C. 1978) (holding that a supervisor’s informal memorandum concerning a discharged employee’s performance was not within the agency’s system of records). This means that an individual can be denied access to records in which he is named if the record is not indexed under his name. \textit{Id.} at 228.

448. Notice to individuals concerning the existence of records about them is of primary concern when dealing with collecting agencies or an agency which participates in data matching. Notice also becomes crucial in determining the accuracy of the records maintained about the individual.

449. 5 U.S.C. § 552a(e)(4) (1994). Notice to each individual was not thought to be necessary “since most persons know many of the files of which they are the subjects.” \textit{Greenawalt, supra} note 97, at 53.

450. This row sets out the ability of the individual to prevent the collection of personal information by the collector. It is easier to protect privacy if the individual can actually prevent the collection of information concerning him. Such protection, as demonstrated by the appendix, is limited.

451. When the collection of personal information would infringe upon other recognized constitutional freedoms, the collection has been barred. For example, in NAACP v. Alabama, 357 U.S. 449, 466 (1958), the Supreme Court invalidated a requirement that the NAACP disclose its membership roster on First Amendment free association and other grounds.

452. Pursuant to 5 U.S.C. § 552a(e)(1) (1994), the information must be such “as is relevant and necessary to accomplish a purpose of the agency required . . . by statute or by executive order.” In addition, 5 U.S.C. § 552a(e)(5) (1994) requires the agency to maintain “such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness” in decisions about the individual made based upon the information.


454. This row shows whether the individual can prevent the original collector from disclosing the information to third parties. This will not be an issue under each statute.
455. The Privacy Act does not define "routine use" or restrict the uses of the information upon its transfer. Nor does the Privacy Act require the requesting agency to establish its need for the information.

456. This row considers the circumstances under which the individual can access a record concerning him. The circumstances vary widely.

457. 5 U.S.C. § 552a(f) (1994). The agency is to respond to requests by individuals wanting to learn if they are the subject of records once the agency has satisfied itself that the inquiry is a genuine one. Id.

458. The key to the individual's ability to protect himself is the ability to correct inaccurate information which has been recorded. This row identifies those statutes which provide a mechanism for correction.


460. Some statutes provide damages to the individual if information about him is improperly disclosed.


463. This row compares the ease with which the individual can operate within the statute to protect his interests.

464. The twelve exemptions are disclosure 1) to officers and employees of the agency needing the records for the performance of their duties; 2) required under FOIA; 3) for routine uses under 5 U.S.C. § 552a(a)(7), and described under 5 U.S.C. § 552a(e)(4)(D) of the PA; 4) to the Census Bureau; 5) for bona fide statistical research using nonidentifiable information; 6) to National Archives and Record Administration of a record having historical value; 7) to an instrumentality of government for civil or criminal law enforcement activity; 8) for health, safety or preservation of the individual; 9) to either house of Congress or committee to the extent of matter within its jurisdiction; 10) to the comptroller general in the course of the performance of his duties; 11) pursuant to a court order; and 12) to a consumer reporting agency pursuant to 31 U.S.C. § 3711(f) (1994). 5 U.S.C. § 552a(b)(1)-(12) (1994).


466. CMPPA is used by agencies to determine the individual's eligibility to receive federal benefits or to discover fraud. The match is done by the use of such personal identifiers as name and social security number. This statute conflicts with the Privacy Act which requires that information only be used for the purposes for which it was originally collected.


469. PRA forbids an agency from collecting information or subjecting any person to penalty for failing to provide information pursuant to an information request which lacks an OMB control number. 44 U.S.C. § 3512 (1988).

470. 5 U.S.C. § 552a(p)(3) (1994). The notice to the individual must state the findings of the match and advise the individual of the procedures he must follow to contest the re-
sults of the match. 5 U.S.C. § 552a(p)(3)(B) (1994). No adverse action may be taken unless and until the adverse information has been verified by the agency as being accurate. 5 U.S.C. § 552a(p)(1)(A) (1994).

471. PRA is concerned with the cost and efficiency of government paperwork and was not intended to create rights in persons having an interest in such information. Pierce v. Apple Valley, Inc., 597 F. Supp. 1480 (D. Ohio 1984).

472. 5 U.S.C. § 552a(o)(1)(A)-(D) (1994) requires that the matching agreement specify the legal authority for the match and the purpose and justification for it, describe the records that will be searched, and specify the procedures for verifying the accuracy of the information used in the match.


476. 5 U.S.C. § 552a(o)(1)(D) (1994). Notice must be given in the Federal Register at least 30 days before the match is conducted. 5 U.S.C. § 552a(e)(12) (1994). No matching program can last for more than 18 months unless a renewal is granted by the agency's data integrity board pursuant to 5 U.S.C. § 552a(o)(2)(C) (1994).


487. Students' records include information concerning both students' and parents' finances, confidential letters of recommendation, and students' educational records, including records of students in primary, secondary, and post-secondary educational programs. 20 U.S.C. § 1232g(a)(1) (1994).

488. Pursuant to 15 U.S.C. § 1681a(d) (1994), a consumer report is any written, oral, or other communication of any information by a consumer reporting agency [CRA] bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (1) credit or insurance...purposes, or (2) employment purposes, or (3) other purposes authorized under [15 U.S.C. § 1681b (1994)] (i.e., in response to a valid court order).

The section includes the following exemptions from coverage:

(A) any report containing information solely as to transactions or experiences between the consumer and the person making the report; (B) any authorization or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device; or (C) any report in which a person who has been requested by a third party to make a specific
extension of credit directly or indirectly to a consumer conveys his decision with respect to such request . . .

489. Investigative consumer reports are reports "in which information on a consumer's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on . . . ." 15 U.S.C. § 1681a(e) (1994). Reports which contain information on the consumer's credit worthiness, credit standing or credit capacity are not considered to be investigative consumer reports. Id.

490. A consumer reporting agency (CRA) is any person which, for monetary fees, dues, or on a cooperative basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.


491. 12 U.S.C. § 3413(g) (1994) does not require notice to the individual if the only disclosure is the individual's name, address, account number and type of account.

492. While the individual has a right to see his consumer report upon demand, he ordinarily will not discover the existence of any adverse information in his report until he has already been denied a benefit by a user of the report. See 15 U.S.C. § 1681m(a) (1994). Upon denial of the benefit, the user must notify the consumer against whom the adverse action was taken of the name and address of the CRA making the report. Id.

493. If an investigative report is requested, the user must inform the consumer of the request and of the consumer's right to request disclosure of the nature and scope of the investigation. 15 U.S.C. § 1681d(a)(1) (1994). Once notified, the consumer may request such information as the purpose of the disclosure, the nature and scope of the investigation, the sources of the information, and the identities of any of the credit report's recipients. 15 U.S.C. § 1681d(b) (1994). Note, however, that the notice requirements are only triggered when the individual's initial eligibility is being considered. See, e.g., Cochran v. Metropolitan Life Ins., 472 F. Supp. 827 (N.D. Ga. 1979) (holding that the use of a credit report to determine the validity of a disability claim was not an application for insurance and therefore did not trigger the FCRA's notice requirements).

494. See 12 U.S.C. § 3402 (1994). The federal request for disclosure will be complied with if the request reasonably describes the records sought and either the customer authorizes disclosure or disclosure is in response to a valid subpoena or search warrant. Id. If the request is pursuant to a legitimate law enforcement inquiry, the bank can supply the records upon written request of the law enforcement agency. Id. Pursuant to 12 U.S.C. § 3408(2) (1994), the head of the agency is required to develop regulations for the disclosure procedure.

495. If a creditor merely furnishes information based solely on its own experience with the consumer, the information is not a "consumer report" and the agency is not a consumer reporting agency. See, e.g., Alvarez Melendez v. Citibank, 705 F. Supp. 67 (D.P.R. 1988); DiGianni v. Stern's, 26 F.3d 346 (2d Cir.), cert. denied, 115 S. Ct. 252 (1994). Consequently, in the absence of an agreement concerning the reporting of the consumer's credit history with the creditor to a CRA, the provider is free to report the information to the CRA. See also 15 U.S.C. § 1681a(f) (1994) (defining CRAs).

496. 12 U.S.C. § 3403(c) (1994). See also 12 U.S.C. § 3413 (1994), which allows regulatory agencies—such as the FDIC, Federal Reserve Bank, IRS, SEC, or state banking and securities departments—to examine financial records.

497. Consent must be given by either the parent, or the student if he is 18 years of age or older. The consent must specify the records to be released and the reason for the dis-
closure. "Directory information" may be disclosed if the student and or parents are given notice as to the nature of the information to be disclosed in the directory and they have had a reasonable time to object to the publication. 20 U.S.C. § 1232g(a)(5)(A), (B) (1994). Directory information includes the student’s name, address, birth place, date of birth, telephone, participation in sports, attendance records, degrees and awards received. No consent is required if the information is to be disclosed to the administrator of another educational institution to which the student is transferring or to state or local authorities in connection with an application for financial aid. No consent is required if the request is made by an organization conducting studies to develop, validate or administer predictive tests, administer student aid programs, and improve instruction. 20 U.S.C. § 1232g(b)(1)(F) (1994). Such information must not be disclosed so as to allow for the personal identification of any student. If the educational institution is compelled by court order to release the information, the institution must give the student notice of its intent to comply with the order. 20 U.S.C. § 1232g(b)(2)(A), (B) (1994).

498. Consumer reports may be disclosed pursuant to an order of a court having jurisdiction, or pursuant to the individual’s consent or to a third person who the CRA has reason to believe intends to use the information for the extension of credit, employment, insurance eligibility, licensure or other government benefit determination, or any other legitimate business need. 15 U.S.C. § 1681b (1994). Pursuant to 15 U.S.C. § 1681e (1994), the CRA is required to maintain reasonable procedures to avoid violations of the FCRA. This means that the CRA must follow reasonable procedures to assure maximum possible accuracy of the information and that users must identify themselves and certify that they are using the information for proper purposes. 15 U.S.C. § 1681e (1994). There is no requirement, however, that a CRA disclose medical information in the consumer’s report to the consumer or that the sources of information be identified without a court order. 15 U.S.C. § 1681g (1994).


501. If the consumer disputes information in the report, the CRA must reinvestigate the matter and correct inaccurate information. If the consumer is not satisfied, he may file a short statement explaining the matter. The individual’s statement must be disclosed whenever the record is accessed by a third party. 15 U.S.C. § 1681i (1994).

Until recently, accuracy and truth were not coextensive terms under FCRA. In Austin v. Bank Americard, 419 F. Supp. 730 (N.D. Ga. 1974), plaintiff challenged the reporting of his being named in a lawsuit and the subsequent denial of a credit card as being based on inaccurate information. Mr. Austin was the sheriff and had been named in his official capacity only. The court upheld the company’s decision, saying that requiring contextual accuracy would impose too heavy a burden upon CRAs beyond the intended scope of the FCRA. Id. at 732-33.


505. See Tarka v. Franklin, 891 F.2d 102 (5th Cir. 1989), cert. denied, 494 U.S. 1080 (1990). The secretary of education has the power to terminate the institution’s funding. 20 U.S.C. § 1232g(f) (1994).

506. 15 U.S.C. § 1681o (1994) provides actual damages, reasonable attorneys fees and court costs in successful actions. There is no minimum amount in controversy for these actions. 15 U.S.C. § 1681p (1994). Recovery is available not only for improper disclosure of information, but also for negligence in maintaining adequate procedures to assure maximum accuracy of the report. See, e.g., Koropoulos v. Credit Bureau, Inc., 734 F.2d 37 (D.C. Cir. 1984); FTC BUREAU OF CONSUMER PROTECTION MANUAL, COMPLIANCE WITH THE FAIR CREDIT REPORTING ACT 26-27 (2d rev. ed. 1979); 5 CCH CONSUMER CREDIT GUIDE P 11,305 at pp. 59,808-09. Notice however that the FCRA has been interpreted to preempt state privacy, defamation and negligence actions. 15 U.S.C. § 1681h(e) (1994). However, if
it is established that the CRA provided false information maliciously, or with willful intent to injure the individual, then the common law actions are preserved. Thorton v. Equifax, Inc., 619 F.2d 700 (8th Cir.), cert. denied, 449 U.S. 835 (1980).


508. Any person who knowingly and willfully obtains a credit report under false pretenses is subject to a fine of not more than $5,000, or may be imprisoned for not more than one year or both. 15 U.S.C. §§ 1681q (1994). The criminal liability has been found to be the basis for a civil suit against an individual who obtains or releases the report under false pretenses. See, e.g., Hansen v. Morgan, 582 F.2d 1214 (9th Cir. 1978) (a political candidate who obtained a credit report with the intent to use it to discredit an opponent found guilty, both criminally and civilly).

509. See, e.g., Clayton Brokerage Co. v. Clement, 87 F.R.D. 569 (D. Md. 1980) (individual had no standing to challenge bank’s disclosure to the government of bank’s business records which were not records of the individual’s account).


514. 18 U.S.C. § 2710(b)(2)(D)(ii) (1994). "[H]owever, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer." Id.


521. The agency is generally not required to disclose information not indexed under the requester’s name or to compile or analyze information on behalf of the requester. See In re Guernier, 566 N.Y.S.2d 406 (N.Y. App. Div. 1991); E.J. Simmons v. Deans, 120 B.R. 831 (E.D.N.C. 1990).