Protecting Informational Privacy in the Information Society

GEORGE B. TRUBOW*

The centennial of the famous Warren and Brandeis article on privacy provides an excellent stimulus to assess the status of privacy today. The purpose of this article is to examine the contours of "informational privacy" in the context of modern information and communications technology.

The notion of "informational privacy," a development of the 1970s, was spawned by the remarkably constant improvement and growing pervasiveness of the digital computer and electronic data banks. Increasingly, personal information, that is, information that can be referenced to an identifiable individual, is the focus of government's information processing as well as the grist for private sector commerce.

First, this article will briefly review the "computer revolution's" effect on privacy and examine the nature of informational privacy. Next, we will consider whether common law or statutes adequately protect informational privacy with respect to public or private data bases. Finally, we will suggest some common law and statutory approaches that may better protect informational privacy without unduly hampering the fair and beneficial uses of this modern technology.

I. THE INFORMATION SOCIETY AND INFORMATIONAL PRIVACY

The importance of information has been appreciated throughout history; it has been revered as the key to power, and recognized as

---

* A.B., J.D., University of Michigan; Professor of Law and Director of the Center For Informatics Law, The John Marshall Law School, Chicago, Illinois. Professor Trubow teaches seminars on Information Law and Policy, and Privacy Law, and has served as general counsel to the Committee on the Right to Privacy, Executive Office of the President, during the Ford Administration. He is Editor-in-Chief of the three-volume work, Privacy Law and Practice, published by Matthew Bender in 1987, and is a member of the Council of the American Bar Association's Section on Science and Technology.

The author acknowledges and appreciates the assistance of Timothy Skinner, Research Fellow for the Center for Informatics Law, in the preparation of this article.

the foundation for rational decisions. With the development of the
digital computer, society’s processing and use of this information has
been transformed. When committed to paper and trapped within the
confines of a manual file, the utility of information is markedly
limited. But, when the information is available in an electronic data
base of virtually endless dimension, open to analysis and processing
at a rate of many millions of functions per second, and capable of
being transmitted through time and space at the speed of light, the
computer transforms the character of the information itself, let alone
the society that employs such technology.

George Orwell’s 1984 warned that “Big Brother Is Watching
You.” Orwell wrote about television cameras and microphones as the
modern devices of surveillance. The digital computer, however, of
which Orwell was ignorant, is a far more effective surveillance de-
vice—both government and the private sector can use it for precisely
this purpose. Though contemporary commentators have raised their
voices in warning, it was Warren and Brandeis who first worried
about the effects of technology upon the enjoyment of privacy.
Writing that “[r]ecent inventions and business methods” raised the
need to “secur[e] to the individual . . . the right ‘to be let alone,’”
they warned that “numerous mechanical devices threaten . . . that
‘what is whispered in the closet shall be proclaimed from the house-
tops.’” Though they cited “instantaneous photographs” as a major
culprit, they were very aware that new technology jeopardized the
dignity and personality of the individual. They lacked prescience,

3. Prior to the introduction of the digital computer, “[p]ersonal information was difficult to secure and compile, making large quantities of information concerning one individual unavailable. Computer technology, however, has made these protections part of a lost era.” Comment, Intrusions Upon Informational Seclusion in the Computer Age, 17 J. MARSHALL L. REV. 831, 836 (1984). Although the digital computer generally provides great benefits to the public, it also “facilitates [the] inspection of an individual’s personal data, and it may prolong the life of the data beyond the time when it has any real validity in describing the individual.” Note, Privacy, Computers, and the Commercial Dissemination of Personal Information, 65 TEX. L. REV. 1395, 1399 (1987).
5. Warren & Brandeis, supra note 1, at 195.
6. Id.
7. Id.
8. Id.
INFORMATIONAL PRIVACY

however, regarding the awesome capability of the digital computer of the future.

These threats have not gone unnoticed. Threats to individual privacy resulting from the development of automated federal data bases were documented in a study released by the United States Department of Health, Education and Welfare in 1973, *Records, Computers and the Rights of Citizens*. In 1977, the report of the Federal Privacy Protection Study Commission, *Personal Privacy in an Information Society*, recognized not only that we had become an information society but also that personal privacy was under siege by both the private sector as well as all levels of government. In the same year, the United States Supreme Court, in *Whalen v. Roe*, signaled its awareness of the privacy implications of information technology, stating:

"We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. 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, much of which is personal in character and potentially embarrassing or harmful if disclosed."

A. PUBLIC AND PRIVATE SECTOR USE OF PERSONAL INFORMATION

Probably, the average citizen is only vaguely aware of the ways in which new technology is being used to collect, manipulate, and

---


11. 429 U.S. 589 (1977). In *Whalen v. Roe*, patients and physicians brought an action challenging the constitutionality of a New York statute that required the creation of a "centralized computer [data base containing] the names and addresses of all persons who have obtained, pursuant to a doctor's prescription, certain drugs for which there [were] both [legitimate] and [illegal] markets. Id. at 591. The plaintiffs contended that the statute violated their right to privacy. Id. The United States Supreme Court upheld the statute as a legitimate exercise of the state's police power. Id. at 598. The Court noted that the statute provided sufficient security to protect the privacy of data subjects whose personal health information was contained in the data base. Id. at 600-02. The Court declined, however, to discuss the future impact of accumulations of personal information in computer data bases. Id. at 605-06.

12. Id. at 605.
disseminate personal information. We are conscious of the traffic in mailing lists that cause us all to be inundated with "junk mail" of every possible kind, and most have received computer-generated "personal" letters and other solicitations demonstrating that someone has a surprising amount of information about us. But these manifestations hardly reveal the extent of the clever uses for a constantly increasing number of automated data bases that contain detailed personal information.

1. Computer "Match" Programs

The federal government has undertaken to employ technology to "match" information from a variety of separate government computer data bases. Originally begun by the Department of Health, Education and Welfare to detect welfare fraud, the practice of "matching" has spread to other agencies, such as the Selective Service System and the Internal Revenue Service. The former uses "matching" programs to identify those who have failed to register for the draft; the latter uses matches of governmental and private data bases to construct personal "lifestyle" characterizations of taxpayers according to categories of spending. Indeed, the activities of federal agencies in trading information became significant enough for Congress to pass the "Computer Matching and Privacy Protection Act of 1988" to regulate these exchanges of information. State and local governments perform similar "matching," but the states have not yet passed legislation restricting these practices.


15. See Comment, IRS Computer Data Bank Searches: An Infringement of the Fourth Amendment Search and Seizure Clause, 25 Santa Clara L. Rev. 153, 154 (1985) (The IRS now has the capacity to pull together bits of information on an individual from sources throughout the country.).

2. **Private Sector Use**

The private sector is also developing countless programs to collect and distribute personal data. The credit reports and detailed financial information maintained by business organizations will increase immeasurably with the development of the Electronic Funds Transfer Systems (EFTS). These EFTS will debit and credit bank accounts by moving electronic impulses instead of cash or checks. As a medium of exchange for point-of-sale transactions, EFTS will generate a constant supply of detailed information that describes exactly when, where, and for what someone commits financial resources. Obviously, anyone with access to that data flow could track the whereabouts of any particular data subject.

3. **The Social Security Number**

Informational privacy also has been jeopardized by congressional action and inaction that, in effect, renders the social security number (SSN) a form of national identification. Though the SSN was

---

17. Electronic Fund Transfer Systems (EFTS) are electronic data processing systems that are used to pay bills or transfer debits or credits. PRIVACY LAW AND PRACTICE § 3.01[7] (G. Trubow ed. 1990). In its 1977 Final Report, the National Commission on Electronic Fund Transfer Systems listed several potential threats to privacy resulting from the use of EFTS. NATIONAL COMMISSION ON ELECTRONIC FUND TRANSFERS, FINAL REPORT: EFT IN THE UNITED STATES 20-23 (1977). Most notable is the increase in the quantity and types of stored information concerning individuals. Id.

18. Note, Privacy, Computers, and the Commercial Dissemination of Personal Information, 65 TEX. L. REV. 1395, 1397-98 (1987) [hereinafter "Commercial Dissemination of Personal Information"] ("[E]very time a person uses an automatic bank teller, a computer collects . . . information identifying the person's location, the date and time of day, and the amount of money requested and received.").

19. Comment, Conceptualizing National Identification: Informational Privacy Rights Protected, 19 J. MARSHALL L. REV. 1007 (1986). The creation of the SSN grew out of the government's need to uniquely label individuals in order to track the social security benefits to which they were entitled. Privacy Protection Study Commission, Personal Privacy in an Information Society, 607-08 (1977). Though initially, the number was used solely for federal government social security purposes, in 1943, President Roosevelt issued an executive order encouraging federal agencies to make greater use of the number. Rotenburg, The National ID Card: An Executive Summary 7 (1990). Widespread use of the number for identification purposes did not actually occur, however, until the 1960s. Id. Since that time, the use of the SSN has expanded dramatically with the improvement of the digital computer. Id. The number is currently used for processing individual tax returns, registering U.S. securities, administering senior citizens assistance programs, and as the service number for American military personnel. Id. Congress requires every United States citizen to have a SSN. Id. In fact, the Tax Reform Act of 1986 requires children to be assigned a number at five years of age. Tax Reform Act of 1986, §§ 6109 and 6676.
originally intended to serve only as a means of accounting for contributions to the social security system, increasingly, it is being used as the device to link various public and private sector data bases and for identification purposes. Though this may afford convenient and inexpensive universal identification, it presents alarming privacy implications. Considering that the personal information in government files can be combined with information in private sector EFTS, anyone who knows an individual's SSN can amass a wealth of highly sensitive information about that individual. Congress undertook to control the use of the SSN in the Privacy Act of 1974, although the then current uses were "grandfathered," and additional uses have since been allowed. Nothing more has been done to restrict use of the number, however.

Interestingly, the Supreme Court's opinion in Whalen v. Roe contains a relevant observation: "The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures." Furthermore, Justice Brennan added in his concurring opinion that, "The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology." Because Congress chose to extend the use of the SSN beyond its originally intended purpose and requires every taxpayer and dependant to have one, it must assume the responsibility of guarding informational privacy from abuse through the use of that number.

20. Comment, Conceptualizing National Identification: Informational Privacy Rights Protected, 19 J. MARSHALL L. REV. 1007, 1008 (1986). The use of the SSN has extended far beyond its original purpose. In the District of Columbia, Hawaii, Mississippi, Nevada, and Virginia, an individual's SSN is also his or her driver's license number. Whole Earth Review, September 22, 1989, at 80. Alabama, Indiana, Missouri, New Mexico, North Dakota, Ohio, Rhode Island, South Dakota, West Virginia, and Wyoming require the SSN to be placed on the driver's license in addition to the standard driver's license number. Id. Other states display the number on the license, unless the driver objects. Id. For a discussion of proposals for a national identification number see Federal Identification Systems: Hearings on S. 1706 Before the Comm. on the Judiciary, 98th Cong., 1st Sess. (1983).

21. Section 7 of the Privacy Act prohibits the federal government from denying rights, benefits, or privileges to individuals who refuse to disclose their SSN's. Wolman v. United States, 501 F. Supp. 310 (D.D.C. 1980) (Selective Service System's requirement that draft registrants supply SSN's violated Privacy Act).

22. See supra notes 20-21 and accompanying text for a discussion of the developments and uses of the SSN.


24. Id. at 607 (Brennan, J., concurring).
It is clear that new information and communication technologies pose serious threats to informational privacy in both the public and private sectors. To what extent do statutes and common law provide the individual with adequate protection in the midst of these new technologies?

II. INFORMATIONAL PRIVACY PROTECTION IN THE PUBLIC SECTOR

Three federal statutes are the principal means for protecting informational privacy in federal data banks: the Privacy Act of 1974\textsuperscript{25} (the Privacy Act), the Computer Matching and Privacy Protection Act of 1988\textsuperscript{26} (CMPPA), and the Freedom of Information Act of 1966\textsuperscript{27} (FOIA). Though FOIA opens access to federal records, it exempts from disclosure information that would constitute an unwarranted invasion of privacy.\textsuperscript{28} A recent United States Supreme Court case interpreting FOIA recognizes the impact of technology and provides significant protection for informational privacy. In \textit{United States Dep't of Justice v. Reporters Comm. for Freedom of the Press},\textsuperscript{29} the Court was called upon to decide whether the FBI's

\textsuperscript{29} 109 S.Ct. 1468 (1989). In \textit{United States Dep't of Justice v. Reporters Comm. for Freedom of the Press}, the United States Supreme Court addressed whether a compilation of criminal history information in a “rap sheet” could give rise to an unwarranted invasion of privacy under FOIA exemption 7(C) even though the bits of information contained within the data bases were derived from public sources. \textit{United States Dep't of Justice v. Reporters Comm. for Freedom of the Press}, 109 S.Ct. 1468, 1476 (1989). Exemption 7(C) allows an agency to withhold an investigatory record if its release would “constitute an unwarranted invasion of personal privacy.” 5 U.S.C. § 552(b)(7)(C). This exemption has been interpreted broadly to protect information concerning marital status, medical conditions, welfare recipient's names and benefits. Cohen v. E.P.A., 575 F. Supp. 425, 429 (D.D.C. 1983).

In discussing the applicability of exemption 7(C) in \textit{Reporters Comm. for Freedom of the Press}, the Court addressed the need to balance the privacy interest in withholding the rap sheets against the public interest in its release. \textit{United States Dep't of Justice v. Reporters Comm. for Freedom of the Press}, 109 S.Ct. 1468, 1476 (1989). The Court divided the case into several areas of focus. First, they addressed whether the data subject, Charles Medico, had any “personal privacy” interest in having his rap sheet remain undisclosed. \textit{Id}. The Court noted that there are two different kinds of interests involved when protecting privacy: the interest of the individual in “avoiding the disclosure of personal matters, and . . . the interest in
disclosure of a "rap sheet" (a compilation of criminal history information derived from public document sources) could constitute an invasion of privacy under the FOIA. The Court held that the information was properly withheld from disclosure, reasoning that "the power of compilations to affect personal privacy . . . outstrips the combined power of the bits of information contained within."30 In effect, the Court said that the whole was greater than the sum of its parts; though each individual item of information was available elsewhere in a public record, since it had all been assembled into a compilation or profile, the whole could display a great deal about an individual and thus infringe upon a privacy interest.31 The Court also

independence in making certain kinds of important decisions." Id. In this case, the Court focused on the interest in avoiding the disclosure of personal matters. Id.

The Court quickly drew a distinction between "records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country . . ." and those that are contained in a single clearinghouse such as a computer database. Id. at 1477. They supported this distinction by pointing to the myriad of federal regulations that limit the circumstances under which rap sheet information may be disclosed. Id. These statutes were seen as evidence of congressional intent that such compilations remain private. Id. The Court stated that "the power of compilations to affect personal privacy . . . outstrips the combined power of the bits of information contained within." Id. They also cited the provisions of FOIA which require that identifying information be removed from requested materials prior to disclosure as evidence that Congress did not intend the records of private citizens to be subject to disclosure. Id. at 1477-78.

Additionally, the Court cited the Privacy Act as support for the idea that a stronger privacy interest inheres in the compilation of computerized information. Id. at 1478. Though the Privacy Act exempts information subject to disclosure under FOIA, the Court stated that the Act was still evidence of congressional concern over centralized data bases. Id.

The Court praised the practice of redacting or removing identifying information from personal summaries prior to disclosure of the documents. Id. at 1479. They were well aware, however, that even if the data subject's name is removed from the compilation, by virtue of the information itself, it is still possible for the information to be linked to the data subject. Id. In these situations, the Court emphasized, nondisclosure is the best means of protecting the individual privacy interest. Id.

The Court then addressed the reporter's contention that the public had an interest in Medico because of his dealings with a corrupt congressman and the Department of Defense ("DoD"). Id. at 1482. The Court rejected these arguments, stating that the documents would reveal nothing about the "Congressman's behavior. [N]or would it tell us anything about the conduct of the Department of Defense . . . ." Id. (emphasis in original). Though the Court conceded that Medico may be of interest in a news story, it stated that disclosing his rap sheet would go beyond the intent of Congress in drafting FOIA. Id.

30. Id. at 1477.
31. Id. at 1476-77. "Merely because [information] can be found in the public
noted that the purpose of FOIA was to reveal information about
government operations, not the personal history of a private person.32

The Court’s approach would markedly enhance privacy if applied
to other federal data bases containing personal information that
discloses a great deal about the individual but not very much about
the government itself. The Reporters Committee decision indicates
that the Supreme Court is balancing the competing FOIA interests in
a way that protects privacy while allowing access to information that
illuminates government practices.

Although the FOIA recognizes a privacy interest, the Privacy Act
of 1974 is the principal federal law that protects personal information.
This Act regulates the information practices of federal agencies by
providing some protection for informational privacy. A major over-
sight in the creation of the Act was that its drafters did not anticipate
the computer matching programs such as were described above. This
matter was later addressed by the CMPPA, which establishes me-
chanisms and procedures to monitor matching activities. However,
even with the combined effect of these two acts, a significant problem

---

1990:521] INFORMATIONAL PRIVACY 529

record does not mean that it should receive widespread publicity if it does not involve
a matter of public concern." Id. at 1476 n. 15 (citing W. KEETON, D. DOBBS, R.
KEETON & D. OWENS, PROSSER & KEETON ON THE LAW OF TORTS § 117 (5th ed.
1984)).

It must be noted that the Ohio Supreme Court, in virtually the same situation,
held otherwise and did not find a privacy interest in such information. In State, ex
rel. Cincinnati Post v. Schweikert, 38 Ohio St. 3d 170, 527 N.E.2d 1230 (1988), a
newspaper was refused access to reports compiled by the court administrator for city
municipal courts and courts of common pleas which are used by judges in determining
whether to reduce jail sentences in assessing jail overcrowding. Id. These reports
identify the charges brought against defendants assigned to each judge; the age, sex,
and race of each defendant; and the bond amount and whether it was made. Id. at
171, 527 N.E.2d at 1231. The record also contains the defendant’s "prior convictions,
violent history, drug, alcohol, or psychiatric history . . ." and probation violation
history as well as a statement of the number of days a defendant has served in jail.
Id.

The Ohio Supreme Court determined that the state’s Public Records Law does
not exempt from disclosure compilations of information derived from public records.
Id. at 172-74, 527 N.E.2d at 1232-33. The court stated that the statute does not
require members of the public to exhaust their time, energy, and resources to gather
information that is already available in compact form. Id. at 173-74, 527 N.E.2d at
1233. In reaching this conclusion, however, the court failed to take into account the
severe privacy threats surrounding the release of such a compilation. Instead, the
court opted for a convenience approach without seriously weighing the potential
harm of the bits of information contained within the dossier.

32. United States Dep’t of Justice v. Reporters Comm. for Freedom of the
remains: no single federal agency is vested with the overall responsibility of safeguarding informational privacy with respect to federal records.

Though the CMPPA requires the creation of a data protection board within each agency that performs match programs, no provision exists for the coordination of privacy policy throughout the federal establishment. The Office of Management and Budget has nominal responsibility for the oversight of the Privacy Act, but it can provide only limited privacy protection. Therefore, Congress should establish a quasi-independent federal agency with the authority and resources to monitor and protect informational privacy.

State and local governments should provide parallel protection of their own databases. Almost every state has public record laws which replicate the federal FOIA or provide public access to certain data bases or records. If the rationale of the Reporters Committee...
case is followed in the administration of state FOIAs and if each state assigns a privacy protection role to a specific agency, then informational privacy will receive a better measure of protection in the governmental environment. This matter rests with the state courts and legislatures. A public outcry on behalf of individual privacy could surely attract attention to the need for adequate privacy protection.36

III. PRIVACY IN THE PRIVATE SECTOR

As previously discussed, the private sector maintains a myriad of personal information data bases, and more are being created every day. Probably the most pervasive collections are maintained by credit bureaus. The Fair Credit Reporting Act37 (FCRA) regulates the practices of these bureaus to some extent, but it does not significantly limit the sale or exchange of the personal information.38

The information maintained by banks and other financial institutions is protected from inquiries by the federal government through


36. For example, a group of Illinois citizens who believe the practice of telemarketing violates their right to privacy have decided not to wait for the legislature to curb such practices. This organization, “Private Citizen,” has enlisted over one thousand members in its one year existence. Parsons, Naperville Group Wants Telemarketers to Buzz Off, Chicago Tribune, March 20, 1990 § 2, at 1. The group distributes catalogs to telemarketing organizations containing the names of its members who do not want to be solicited by telemarketers. Id. In addition to this catalog, the group also notifies the telemarketers that the group will charge such organizations for the use of their time on the telephone. Id. The group’s members have been successful in receiving modest judgments from telemarketers who call them against their wishes. Id.

37. 15 U.S.C. § 1681 (1982). The purpose of the FCRA was to curb privacy abuses in the private sector. Freedman, The Right of Privacy in the Age of Computer Data and Processing, 13 Tex. Tech L. Rev. 1361, 1375 (1982). The Act requires that consumers be notified whenever a credit report is used as the basis of rejecting their request for some benefit. Id.

the Right to Financial Privacy Act of 1978. Few states have parallel laws to deal with inquiries to financial institutions from state or local government agencies, and none restrict the sale of these data bases to the private sector. Is the common law more effective in vindicating the belief of Warren and Brandeis?

The invasive conduct that disturbed Warren and Brandeis was the "injurious disclosure as to private matters" and "the unauthorized circulation of portraits of private persons." These forms of conduct appear in two of the four branches of a right to privacy tort later articulated by Professor Prosser: public disclosure of private facts and appropriation of identity. Prosser's classification became the basis for the privacy torts as set forth in the Restatement (Second) of Torts.

IV. PUBLICATION OF PRIVATE FACT

Section 652D of the Restatement (Second) of Torts addresses "Publicity Given to Private Life" when the matter published is "highly offensive to a reasonable person" and "not of legitimate concern to the public." The Restatement, as well as the common law, have accepted Warren and Brandeis' belief that "[t]he truth of the matter published does not afford a defence." This concept is in direct contrast to the truth defense available in defamation law. In applying the tort, the courts have reduced its usefulness by interpreting "public concern" in broad terms; and "newsworthiness," which often is little more than curiosity, seems to meet the test. Most states

39. 12 U.S.C. § 3401 (1982). The Right to Financial Privacy Act was designed to give data subjects some control over the federal government's access to their financial records. PRIVACY LAW AND PRACTICE, § 3.03[4][a] (G. Trubow ed. 1990). Under the Act, most customer record disclosures to federal government agencies require the consent of the data subject. Id. The Act, however, applies only to federal government agencies and is, therefore, inapplicable to state and local governments and private entities. Id.
40. Warren & Brandeis, supra note 1, at 204.
41. Id. at 195.
44. Id. at § 652D(a).
45. Id. at § 652D(b).
46. Warren & Brandeis, supra note 1, at 218.
47. The test for that which constitutes a "public concern" has been defined as whether a reasonable member of the public with decent standards would determine that he or she has no concern in the matter. Virgil v. Time, 527 F.2d 1122, 1129 (9th

532 NORTHERN ILLINOIS UNIVERSITY LAW REVIEW [Vol. 10
recognize this privacy tort, though some do not.\textsuperscript{48} States that do not recognize the tort often misconstrue the Prosser formulation.

For example, in \textit{Hall v. Post},\textsuperscript{49} the Supreme Court of North Carolina refused to recognize this branch of the privacy tort. A newspaper had printed a series of articles about a former carnival worker who sought to find a daughter she had abandoned seventeen years earlier.\textsuperscript{50} The newspaper reported that the child had been adopted after the abandonment, and revealed the identity and location of the child and the adoptive mother, both of whom fled their home to avoid the public attention the articles generated.\textsuperscript{51}

The North Carolina court's opinion reflected little concern for the privacy of the adoptive mother or the child. Instead, the court focused on the first amendment ramifications of restricting the press' effort to reveal the information on the ground that it was of public interest.\textsuperscript{52}

The Supreme Court, in \textit{Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.},\textsuperscript{53} gave better insight into the nature of "public inter-
"est," at least in terms of the first amendment. The Court concluded that a credit report distributed for commercial purposes was not a matter of public interest, even though the report contained information regarding bankruptcy and net worth. Self-governance and the public's safety and welfare are the focus of "public interest," and these matters are not within the purview of commercial data bases containing personal information. This is a far better touchstone of public interest than the highly subjective "newsworthiness" standard because it places emphasis on importance to the public rather than on a particular individual's curiosity.

A. BARRIERS TO THE APPLICATION OF THE PRIVATE ACT TORT

A variety of other barriers have hampered the development of the publicity of private fact tort. First, because the tort focuses on publication, which has been equated with speech, it may run afoul of the first amendment, as illustrated by the HaP case. The root of this problem lies in the fact that the Supreme Court extended the reach [must be weighed] against the First Amendment interest in protecting this type of expression." Id. at 757.

54. Id. at 762. The information in this credit report was inaccurate. The court noted, however, that not all credit reports will receive reduced first amendment protection. Id. at 762 n.8. "[T]he report's 'content, form, and context'" determine the degree of first amendment protection that such a report is afforded. Id.

55. The Restatement (Second) of Torts provides insight into the types of matters that constitute legitimate public concern. It states:

In determining what is a matter of legitimate public interest, account must be taken of the customs and conventions of the community; and in the last analysis what is proper becomes a matter of the community mores. The line is to be drawn when the publicity ceases to be the giving of information to which the public is entitled, and becomes a morbid and sensational prying into private lives for its own sake, with which a reasonable member of the public, with decent standards, would say that he had no concern.

RESTATEMENT (SECOND) OF TORTS § 652D comment h (1977).

With respect to commercial databases, the court in Tureen v. Equifax, Inc., 571 F.2d 411 (8th Cir. 1978), made the following relevant observation:

In today's mobile society, there is a legitimate business need for consumer reports, which serve . . . important public functions . . . . In order to make informed judgments in these matters, it may be necessary for the decision maker to have information which normally would be considered private, provided the information is legitimately related to a legitimate purpose of the decision maker. In such a case, the public interest provides the defendant a shield which is similar in principle to qualified privilege in libel.

Id. at 416.

of the first amendment to defamation, a tort that is based upon the publication of false fact.57

The facts of concern in informational privacy are generally true, and the Court has not completely resolved the issue of when the first amendment will protect the publication of true facts that relate to private affairs. The Supreme Court had the opportunity to address this issue in *Cox Broadcasting Corp. v. Cohn*,58 when they considered


58. 420 U.S. 469 (1975). In *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975), a deceased rape victim's father brought a civil action against a television station alleging a private cause of action for invasion of privacy arising from a Georgia statute making it a misdemeanor to publish the name of a rape victim. *Id.* at 471-74. The name had been published in connection with news stories about the trial of the six defendants charged with raping and murdering the daughter. *Id.* The reporter assigned to cover the trial stated that he received his information by attending all but the first 30 minutes of the first morning of the trial. *Id.* at 472 n.1.

In its analysis, the Court began by recognizing the:

great responsibility ... placed upon the news media to report fully and accurately the proceedings of government[;] and official records and documents open to the public are the basic data of governmental operations ... With respect to judicial proceedings in particular, the function of the press serves to guarantee the fairness of trials and to bring to bear the beneficial effects of public scrutiny upon the administration of justice ... The commission of crime, prosecutions resulting from it, and judicial proceedings arising from the prosecutions, however, are without question events of legitimate concern to the public and consequently fall within the responsibility of the press to report the operations of government. *Id.* at 491-2.

The Court noted that the Warren and Brandeis article proposed that privacy actions would be limited in the same manner as libel and slander actions if the publication was privileged: "[T]he right to privacy is not invaded by any publication made in a court of justice ... and (at least in many jurisdictions) reports of any such proceedings would in some measure be accorded a like privilege." *Id.* at 493 (citing Warren & Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 216-17 (1890)). The *Cox* Court also noted that the tentative drafts provided in the comments of the Restatement (Second) of Torts state that a person would not be liable for accessing or publishing information in public records.

The *Cox* Court emphasized this point in stating:

[E]ven the prevailing law of invasion of privacy generally recognizes that the interests in privacy fade when the information involved already appears on the public record. The conclusion is compelling when viewed in terms of the First and Fourteenth Amendments and in light of the public interest in a vigorous press ... .

By placing the information in the public domain on official court records, the State must presume to have concluded that the public interest was thereby being
whether a newspaper could be liable for violating a rape shield statute by publishing the name of a rape victim that had been found in a public record. However, the Cox Court sidestepped the first amendment question by finding that the information was not private.  59 This author suggests that the Greenmoss  60 decision provides a workable test that could be applied in determining when truthful information is of private, not public, concern.

The Cox case introduced a second obstacle to the utility of the private fact tort: whether personal information in a public record can be considered private information. Though on the facts presented in Cox the Court appropriately said no, the Reporters Committee  61 case gave a different result in the context of FOIA. In Cox, the disclosure was of a single fact obtained directly from an indictment, the public record. In Reporters Committee, the plaintiff sought disclosure of a

served. Public records by their very nature are of interest to those concerned with the administration of government, and a public benefit is performed by the reporting of the true contents of the records by the media. The freedom of the press to publish that information appears to us to be of critical importance to our type of government in which the citizenry is the final judge of the proper conduct of public business. In preserving that form of government the First and Fourteenth Amendments command nothing less than that the States may not impose sanctions on the publication of truthful information contained in official court records open to public inspection.  

Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 494-95 (1975).

59. Id. Similarly, in Florida Star v. B.J.F., 109 S. Ct. 2603 (1989), the United States Supreme Court decided whether the first amendment is violated if damages are imposed on a newspaper for printing a rape victim's name pursuant to information legally obtained. In Florida Star, a rape victim brought suit against a newspaper for publishing her name that a reporter obtained from a publicly released police report. Id. at 2605-6. The Florida rape shield statute allowed the imposition of civil damages against newspapers that revealed this information. Id. at 2605. The Court rejected the plaintiff's claim, noting that though the state's interests in protecting the privacy of sexual assault victims are significant, imposing liability is not the best means to advance those interests. Id. at 2610. The Court placed great reliance on the fact that the government itself provided the information to the media; therefore, it had the opportunity, but did not guard against its dissemination. Id. at 2611-12. The Court stated that when the government fails to police itself, it cannot punish the media for reporting truthful accounts of the information the government distributes. Id. The information dissemination, without qualification, led the recipients to believe printing it was lawful. Id. at 2612. Furthermore, the Court emphasized that the statute only punishes media, not those who distribute such information by word of mouth. Id. at 2612-13. State attempts to protect rape victims in the name of privacy requires an even-handed approach. Id. at 2613. It must apply equally to the small-time as well as the big-time disseminator. Id.


"rap sheet," a compilation of information that had been derived in turn from a series of public records. Nevertheless, in other contexts, personal information has lost its confidential nature when found in some public record.

A third problem in applying the private facts tort lies in the required scope of disclosure. A relatively widespread publication of the information is required to constitute an invasion of the privacy interest, unlike defamation wherein disclosure to one other than the data subject is sufficient. Though this requirement was not contemplated in the Warren and Brandeis formulation nor in Prosser's early explication, the courts routinely accept such a limitation. Because the "publication" of commercial data maintained in computer data bases is routinely made to a small group, often one at a time, it may not satisfy this requirement.

Another pervasive problem in applying the private fact tort is the requirement that the information disclosed be highly offensive to a reasonable person. The courts frequently deny the tort's application when the information, though private and perhaps not of public interest, is not in itself deemed harmful or offensive. Most of the information stored in commercial computer files is not offensive or embarrassing, even though it does provide a detailed description of an individual's behavior, tastes, and values.

62. See, e.g., Rycroft v. Gaddy, 281 S.C. 119, 314 S.E.2d 39 (S.C. Ct. App. 1984) (In tort actions arising out of the publication of private facts, communication to a single individual or small group of individuals is insufficient.).

63. Tureen v. Equifax, Inc., 571 F.2d 411 (8th Cir. 1978). In the Tureen case, a majority of the United States Court of Appeals for the Eighth Circuit ruled that information disseminated by a credit bureau was insufficient publication to support a claim for disclosure of private fact. In dissent, however, Judge Heaney rejected this contention. Judge Heaney stated that, "The collection and retention of personal information about a particular consumer by a commercial information broker, such as Equifax makes the dissemination of that information sufficiently likely as to meet any reasonable requirement of 'publicity.' " Id. at 420. He further stated that, "[t]he dissemination of private information by a commercial credit broker to insurance companies, banks and other customers requesting such information is no less 'public' than the posting of a debt in a creditor's shop window." Id. at 421.

64. See, e.g., Ross v. Midwest Communications, Inc., 870 F.2d 271 (5th Cir. 1989) (television documentary revealing rape victim's first name and picture of her residence not embarrassing enough so as to be deemed "highly offensive" for purposes of tort involving disclosure of private facts); Thomason v. Times-Journal, Inc., 190 Ga. App. 601, 379 S.E.2d 551 (1989) (newspaper's erroneous printing of live plaintiff's obituary not so highly "offensive and objectionable to a reasonable person of ordinary sensibilities" as to give rise to liability for tort of disclosure of private facts).
Finally, even when the information is "highly offensive," the courts often deny the remedy on the grounds of the conditional privileges adopted from defamation law. Because these disclosures are regarded as speech, the courts have been quick to justify them. Consequently, the privileges, coupled with the obstacles discussed above, have virtually eliminated the disclosure of private facts tort as an adequate remedy for violations of informational privacy, even in the commercial environment.

V. Appropriation of Name, Likeness, or Personality

Most of the incursions on informational privacy in the private sector result from commercial use of data. As indicated previously, there is constant growth in the sale of personal information; the tort "appropriation of name or likeness" for a commercial purpose could provide an appropriate remedy. A compelling argument can be made that a collection of personal information sold as a dossier or profile violates the appropriation tort that had been described by Prosser as "appropriation of some element of the plaintiff's personality for commercial use." When this tort is alleged, in most instances, the appropriation has been accomplished by associating the plaintiff's personality with an advertisement for the sale of goods or services or to link him with a particular cause or viewpoint. When dossiers and profiles maintained by credit bureaus and other such

65. See, e.g., Florida Star v. B.J.F., 109 S.Ct. 2603 (1989) (disclosure of rape victim's name not compensable because publicly disclosed by the government); Zinda v. Louisiana Pacific Corp., 149 Wis. 2d 913, 440 N.W.2d 548, 553 (1989) (employer who published reasons for plaintiff's termination in company newsletter protected by conditional privilege because "[e]mployees have a legitimate interest in knowing the reasons a fellow employee was discharged.").

66. RESTATEMENT (SECOND) OF TORTS § 652C (1977). A distinction must be noted between the appropriation tort and the "right of publicity," which is a relatively new tort that is gaining ground by statute and common law. This new tort is recognized as having grown out of the appropriation tort. It was first introduced in the 1953 case of Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866 (2d Cir. 1953). Its primary purpose is to protect public figures and to provide them with a descendable and assignable right. Nimmer, The Right of Publicity, 19 LAW & CONTEMP. PROBS. 203 (1954). The publicity right differs from the appropriation right, however, to the extent that the appropriation right is a personal right that does not survive the person while the publicity right is both assignable and inheritable. Id. In the context of informational privacy, the typical private person needs protection to guard against privacy invasions only while living. Therefore, the appropriation tort should suffice because, in that context, one's privacy may be regarded as complete upon death.

agencies are sold, the subject's personality is certainly being used for a commercial purpose. Similarly, when a mailing list is sold and that list identifies potential customers or individuals likely to support or contribute to a particular cause, a part of the individual's personality, not merely his name, is being appropriated for commercial gain.

A similar argument was made in the 1975 Ohio case of *Shibley v. Time, Inc.*. In *Shibley*, the plaintiff alleged that Time Magazine's practice of selling and renting subscription lists to direct mail advertisers constituted an appropriation and exploitation of his personality. The court rejected this argument mainly because the Ohio legislature had passed a statute that expressly condoned these practices. But, in noting the hesitance to allow claims based on a desire to avoid receiving "junk mail," the Ohio court misinterpreted the plaintiff's assertion. The plaintiff did not complain that he was receiving unwanted correspondence from the purchasers of the mailing lists. Instead, he was claiming that his name was being sold without his consent, thus causing an unwanted appropriation of his personality.

Surely, the requirement of commercial use encompasses the sale of mailing lists, credit reports, or detailed records of an individual's purchasing history. In the common setting of an endorsement, for instance, the plaintiff's personality has been appropriated to manipulate others—that is, to encourage others to accept a particular product, service, or idea because of the data subject's association with it. In the present reference, the personality profile is used to permit others to manipulate the data subject. In either case, it is the individual's persona that is the subject of the use, and the appropriation tort ought to apply.

The appropriation tort avoids a conflict with the first amendment. The gravamen of this tort is not speech as typified by publication; it is the act of appropriation or use that demonstrates control over the information. Conventional wisdom, at least in the degree to which the Restatement represents convention, recognizes this distinction.

---

68. 45 Ohio App.2d 69, 341 N.E.2d 337 (1975).
69. Id.
70. Id. at 73, 341 N.E.2d at 339.
72. The Restatement (Second) of Torts recognizes the distinction between the appropriation tort and the privacy torts protecting publicity of private fact and false light. *Restatement (Second) of Torts* § 652C (1977). Though, in applying all of
Additionally, the use of the appropriation tort avoids the defense of "public interest" that applies to publications of private fact. Indeed, it is the very fact of a "public interest" that encourages the commercial appropriation.

The individual's personality, as it is described by the behavior and values evidenced in the commercial environment, is clearly the subject of the dossier. The dissemination of this information directly affects the way the individual is perceived and received by other members of the community. Every time a credit report or other personal-information dossier is sold, the individual's control over his persona is diminished. Though the individual is probably unaware when a compilation has been created, or is being sold,73 this happens constantly with very few restrictions.74 Is there "harm" to the individual in these commercial practices?

For a long time, "Madison Avenue" has been analyzing the public so as to predict the behavior of target segments. Whether to promote products or gather votes on a candidate or issue, clearly the goal is to learn how to affect the behavior of others—to manipulate consumers or voters. "Target marketing" seeks constantly to narrow and particularize the groups of people who are the aim of political or commercial attention. It has been suggested that this compilation and the privacy torts, the Restatement emphasizes the importance of protecting personal feelings, it distinguishes the appropriation tort because the interest protected there is in the nature of a property right. Id. at comment a. Therefore, unlike the torts of publicity given to private fact and false light, there is no widespread publicity requirement. Id. at § 652C. The only notable restriction on recovery under the appropriation tort is incidental use. Id. at comment d. The relevant portion of comment d states as follows:

No one has the right to object merely because his name or his appearance is brought before the public, since neither is in any way a private matter and both are open to public observation. It is only when the publicity is given for the purpose of appropriating to the defendant's benefit the commercial or other values associated with the name or the likeness that the right of privacy is invaded.

Id. (emphasis added).

It is important to note that incidental use as defined in comment d of section 652C differs from the limitation on matters deemed to be of a "legitimate public interest" in section 652F. Section 652F provides a privilege to publish matters of public interest. Id. at § 652F.

73. Linowes, Must Personal Privacy Die in the Computer Age?, 65 A.B.A. J. 1181, 1183-4 (1979) (discussing the fact that individuals are generally unaware that such information is used in decision-making).

74. RUBIN, THE COMPUTER AND PERSONAL PRIVACY 64 (1988) ("The sad fact of the matter is that the regular practice of credit reporting bureaus is to sell reports to anyone that claims a legitimate need for the information.").
dissemination of personal information could lead to a compulsion to avoid taking risks, thus creating a conformist, robotic public seeking to avoid exposure to the risks inherent in functioning in society.\textsuperscript{75} Without the need to subscribe to such a theory it is, nevertheless, reasonable to fear the privacy risks and to guard individuals from commercial trafficking in their personalities without their knowledge or notice of the purposes at hand.

To provide some ability to monitor these transactions, the FCRA\textsuperscript{76} should be amended to require notice to the individual when information about him has been supplied to another. Currently, the FCRA requires that notice be given to the data subject only when the credit report is used adversely in connection with credit, employment, or insurance decisions.\textsuperscript{77} Amending the Act will give data subjects a greater degree of control over information about themselves. The importance of control was recognized by Warren and Brandeis: "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."\textsuperscript{78} The need for some measure of control is even more important when personal information may be used covertly to manipulate the data subject.

In addition to amending FCRA, to the extent that the commercial use of dossiers and mailing lists is permitted, it seems fair that those who sell this information should be required to contribute some portion of the proceeds (perhaps twenty percent) to the social security accounts of the data subjects involved. It is interesting to note that the private sector understands the value of invading privacy since the market easily fixes prices for credit reports and mailing lists. To require compensation for routine invasions of privacy seems entirely appropriate.

VI. SUMMARY OF PRIVACY PROTECTION PROPOSALS

Now that we have wandered through a discussion, diagnosing ills and considering cures, a summary of what has been proposed seems in order.

\textsuperscript{75} Note, \textit{Commercial Dissemination of Personal Information, supra} note 18, at 1396.
\textsuperscript{77} \textit{Id.} at § 1681m(a).
\textsuperscript{78} Warren & Brandeis, \textit{supra} note 1, at 198. This notion of control was also emphasized in Allen Westin's treatise. \textit{A. Westin, Privacy and Freedom} 159, 169-210 (1970).
1. Federal and state governments should designate a single agency with the authority and resources to monitor and enforce informational privacy policies. A concern for privacy is the natural enemy of a government bureaucrat who pursues agency objectives with costs and efficiency in mind. Technological benefits can be enjoyed without destroying informational privacy, but an official with clout must be charged with that responsibility.

2. Congress should act to protect the social security number, especially from its use as an identifier that links information in diverse commercial record systems without the knowledge or consent of the individual. Regulating matches by federal agencies through the CMPPA is simply not enough.

3. The courts must be urged to consider the rationale suggested in *Whalen v. Roe* and articulated in the Reporters Committee case. Unless we recognize how technology can be used to invade privacy and thereafter constrain any invasion, little privacy will survive the "computer revolution."

4. Litigants should arm themselves with the appropriation tort as a viable and persuasive common law response to violations of informational privacy in the commercial environment.

5. The FCRA should be amended to: (a) provide notice to individuals whenever their dossier has been supplied, and (b) to require that a portion (we suggest twenty-percent) of gross revenues from such transactions be deposited in the subject's social security account.

6. Citizens, arise! A major reason more has not been done to protect informational privacy is because a constituency is not mobilized. Professional and civic organizations, political activists, consumer groups, and concerned citizens should all join a hue and cry to protect informational privacy.

Implementation of any part of the package will bring a significant improvement to informational privacy protection. Perhaps it is too much to hope that all is accomplished, but who is to say?