TORTS

INFORMATIONAL PRIVACY AND THE PRIVATE SECTOR

Fred J. Greguras*

I. INTRODUCTION

The issues of the confidentiality and the extent of data collected and maintained by businesses and other private organizations are important concerns of the general public today.¹ All organizations in both the governmental and private sectors which collect, maintain, and disseminate information regarding individuals on the basis of some form of relationship between the individual and his society should reevaluate their information practices. The relationship may be as general as the newspaper-public relationship or as specific as a taxpayer's obligation to his government. It may merely be an employer-employee or client-customer business relationship. Recent United States Supreme Court decisions and the trend of legislative developments indicate that the legal processes are responding to the public's concern.

This article will provide an overview of the types of potential liability associated with the use of personal information in the private sector.² Relevant Nebraska law is identified and analyzed and other more detailed authority regarding various areas of potential liability is discussed. Additionally, general guidelines for fair information practices are suggested which should minimize both the risk of liability and the disruption occasioned by the imposition of governmental requirements.

* B.A. 1966 University of Omaha; M.S. 1968, University of Nebraska, Omaha; J.D. 1975, University of Nebraska, Lincoln; Associate, Kutak Rock & Huie, Omaha, Nebraska; Director of Law Programs, Creighton University Institute for Business, Law, and Social Research, 1976-1977.


2. The proper course of action to be followed under specific circumstances should be determined with the aid of legal counsel.
II. SOCIETAL INTERESTS

Case law, legislation, and administrative regulations pertaining to legal liability for the use of personal information reflect a compromise among competing societal values or concerns. A consensus is achieved through trade-offs among legislators and a balancing of interests by the courts. In achieving a consensus, the following societal values are considered and weighed.

THE INDIVIDUAL’S RIGHT OF PRIVACY

In an informational context, an individual’s right of privacy involves the right to have a role in determining what personal information the recordkeeper may collect, maintain, and disseminate. This is not an absolute right, since records containing personal data are usually the product of relationships in which both individuals and organizations have an interest. Thus, if an individual wants, needs, or is required to interact with record-keeping organizations, he must reasonably expect to have to share partially control over the use of personal information. On the other hand, the record-generating organization should not make unilateral decisions concerning the content and use of its records containing personal information.

THE PUBLIC’S RIGHT TO KNOW

The creation of a right of privacy must not be an authorization to the government to conceal its operations from the public. An informed citizenry cannot exist if an absolute right of informational privacy is imposed upon governmental records. The Freedom of Information Act\(^3\) is an attempt to protect this societal interest.\(^4\)

FREEDOM OF SPEECH AND PRESS

The media serves as a forum for the exposition of ideas, for the criticism of government, and for the advocacy of new methods of accomplishing national objectives. An informed citizenry and a responsive government could not exist without such a forum. In a similar manner the first amendment\(^5\) pro-

---

5. U.S. CONST. amend. I.
vides individuals the right to expound, criticize, and advocate to ensure a healthy and accountable government. However, none of these rights are absolute; rather, the exercise of such rights imposes a responsibility upon the publisher or speaker. Advocacy may become incitement and may create a high risk of violence, and published criticism may become defamation, neither of which are protected by the first amendment.

THE EFFICIENCY AND EFFECTIVENESS OF GOVERNMENTAL AND BUSINESS ORGANIZATION OPERATIONS

In conflict with the aforementioned factors is the need to minimize disruptions of necessary governmental and business functions. For example, in the law enforcement setting, there is a need not to impose such restrictive information practices as to unduly disrupt the law enforcer's appointed function of preserving order in society. In the private sector, there is the need to balance individual privacy with the need of a business organization to make a profit. Extensive regulation of information practices can destroy or severely impair that ability; yet some regulation may be needed.

THE RESEARCH COMMUNITY'S NEED FOR DATA TO ADVANCE THE STATE OF KNOWLEDGE

The research community must have access to information in order to produce and compile a body of facts upon which government and business can make reasoned policy decisions.

---

8. See generally Miranda v. Arizona, 384 U.S. 436 (1966). The "Miranda rule" can be viewed as a control on the circumstances under which information may be given to an arresting officer, thereby effectively limiting his appointed function.

From an information importance vantage point, unfavorable reaction to the majority's ruling is best exemplified in Mr. Justice Harlan's dissent:

What the Court largely ignores is that its rules impair, if they will not eventually serve wholly to frustrate, an instrument of law enforcement that has long and quite reasonably been thought worth the price paid for it. There can be little doubt that the Court's new code would markedly decrease the number of confessions.

We do know that some crimes cannot be solved without confessions, that ample expert testimony attests to their importance in crime control, and that the Court is taking a real risk with society's welfare in imposing its new regime on the country. The social costs of crime are too great to call the new rules anything but a hazardous experimentation.

Id. at 516-17.
This differs from the general public's need to know, in that the researcher should document the validity of his facts. Thus, the researcher needs to know more with fewer restrictions on his access to the information. On the other hand, a researcher's right to access must include adequate safeguards to ensure that the information is used for proper research purposes and that the risk of a breach of confidentiality is minimized. The exception for researchers in the Department of Justice's regulations on access to criminal justice information illustrates the recognition of a need for data to advance the state of knowledge of the operation of the criminal justice system.\(^9\)

As these competing values are considered and weighed, tensions will arise as to which value will take precedence in making a decision or advocating a position. Decisions in traditional legal actions and newly adopted legislation reflect the courts' and legislators' struggle to achieve an optimal balance of these competing interests.

III. JUDICIALLY ESTABLISHED CONTROLS ON INFORMATION USE AND DISSEMINATION

**Defamation**

The tort of defamation is a significant legal control over the use of personal information.\(^{10}\) Early Nebraska case law held

---


Individuals who provide information in a Law Enforcement Assistance Administration funded study are protected by the “privilege” provision, 42 U.S.C. § 3771(a) (Supp. III 1973), which technically is applicable only to documents created on the basis of the information provided, not to the testimonial evidence of the researcher. This interpretation has not been litigated in the five years since the statute was passed. See also Richards of Rockford, Inc. v. Pacific Gas & Elec. Co., 71 F.R.D. 388, 389 (N.D. Cal. 1976).


A business organization can be defamed as can any living person. Id. at 745. The communication must tend to diminish the esteem, respect, or confidence with which the person or organization is held. See, e.g., Grant v. Reader's Digest Ass'n., 151 F.2d 733 (2d Cir. 1945). It must reflect upon a person's character or must create adverse or derogatory feelings or opinions against him. See, e.g., Burton v. Crowell Publishing Co., 82 F.2d 154 (2d Cir. 1936). When the communication is oral the tort is slander; when written it is called libel. W. PROSSER, supra note 10, § 111, at 737.

Before the advent of the mass oral communications media, the measure of damages, burden of proof, and other factors for slander (oral) and libel (written) were different on the basis of the possible scope of dissemination. See Nelson v. Rosenberg, 135 Neb. 34, 36-38, 280 N.W. 229, 230-31 (1938).
various statements to be defamatory under the circumstances considered.\textsuperscript{11} Nebraska courts have found statements to be defamatory per se which falsely assert that a person has committed an indictable criminal offense such as kidnapping,\textsuperscript{12} blackmail,\textsuperscript{13} or embezzlement.\textsuperscript{14} Statements which ridicule were also actionable per se.\textsuperscript{15} For example, a school teacher who was publicly disgraced recovered general damages without demonstrating actual harm to her reputation.\textsuperscript{16}

In general, the law is more responsive to the need to protect persons engaged in a business, trade, or profession from statements which imply improper conduct or incompetency in their occupation.\textsuperscript{17} Under the liability per se theory, there was often a fine line drawn between disparaging or derogatory, and damaging statements.\textsuperscript{18} For example, a statement made about a business’ financial difficulties was termed derogatory, but not so damaging to the business to call for the imposition of liability without a showing of special damages.\textsuperscript{19} From a practical point of view, proof of damage to the volume of business should be more easily demonstrated than injury to personal reputation.\textsuperscript{20}

The need for an uninhibited exposition of ideas may out-
weigh the individual's interest in protecting personal reputation. A true statement when communicated with proper motives is a complete defense to a defamation action. A complete defense also exists for defamatory statements made in official judicial, executive, or legislative proceedings. Moreover, liability in a defamation action may be further limited by first amendment considerations as is aptly demonstrated by cases decided by the United States Supreme Court.

During the period from 1964 to 1971, the balance was heavily weighted in favor of protecting first amendment rights. Arguably, the net effect of these cases was to eliminate defamation actions. The focus was whether the person allegedly defamed was a public official, or public figure, or whether the subject matter of the communication was a matter of public or general concern. Society's need to know about events of general importance was deemed paramount. If the person or set of facts met one of these three criteria, recovery was allowed only if the plaintiff demonstrated that the defamatory falsehood was published "with knowledge it was false or with reckless disregard of whether it was false or not."
In the recent case of *Gertz v. Robert Welch, Inc.*\(^{28}\) the Court attempted to achieve a better balance between the competing interests. *Gertz* narrowed the scope of the qualified privilege to statements made only about a public official or public figure.\(^{29}\) Thus, the decision whether an individual is a public or private figure is now the key factor in allowing recovery. A public figure has been defined as an individual who has attained special prominence in the resolution of public questions.\(^{30}\)

To counterbalance the shift toward protection of the private individual, the Court added these safeguards to preserve first amendment rights:

1. In establishing a standard for liability when a "private figure" is involved, states must require that some degree of fault or culpability be demonstrated before liability is imposed. The degree of fault may be mere negligence on the part of the communicator but may *not* be strict liability, i.e., liability without fault.\(^{31}\)
2. Recovery of damages under the relaxed standard is limited to those actually proven.\(^{32}\)
3. Presumed and punitive damages are recoverable only if it is established that the defamatory statement was made with knowledge that it was false or with reckless disregard of whether it was false or not.\(^{33}\)

Subsequently, in *Time, Inc. v. Firestone*,\(^ {34}\) the Supreme Court held that mere use of the judicial process does not transform a private figure into a public figure.\(^ {35}\) Arguably, *Firestone* establishes a presumption against a private citizen being a public figure. At a minimum, the case provides a strong factual precedent for those claiming not to be public figures.\(^ {36}\)

---

29. *Id.* at 339-48.
30. *Id.* at 342. The court defines public figures as "[t]hose who, by reason of the notoriety of their achievements or the vigor and success with which they seek the public's attention, are properly classed as public figures . . . ." *Id.*
31. *Id.* at 347-48.
32. *Id.* at 348-50. The net effect of this case is to eliminate "per se" liability, that is, liability without a showing of special damages, unless malice is demonstrated.
33. *Id.* The difficulty in demonstrating concrete evidence of a statement's actual injury to reputation may render private plaintiffs' victory an empty one. The relaxed burden does increase the probability of avoiding a directed verdict and proceeding to a jury.
35. *Id.* at 454. See Note, 10 Creighton L. Rev. 351 (1976) for an excellent discussion of the Firestone case.
36. 424 U.S. at 455. The basis of Mrs. Firestone's allegation involved an
Although the fault issue was not litigated in *Firestone*, the opinions of the Court provide some indication of the evidential factors which are relevant in fault analysis. The source of the defamatory information, the credibility of the source, and the efforts to verify accuracy were deemed relevant.\(^{37}\) The ambiguity of the divorce decree and the unfamiliarity of a lay person with the complexity of the judicial process were factors generated by the specific circumstances.\(^{38}\) Generally, the issue was whether Time, Inc. could have taken additional action to insure investigative accuracy.\(^{39}\)

*Firestone* illustrates that while communicators and other business organizations should act responsibly under all circumstances, a greater responsibility is required when the circumstances are uncertain. Since *Gertz* dictated that some element of fault is required to impose liability,\(^{40}\) it would seem that communicators must, at a minimum, be negligent in order to incur liability. Thus, the communicator must use "reasonable care" in the collection and dissemination of information.\(^{41}\)

In the Nebraska Supreme Court's most recent defamation decision, the court did not find it necessary, in view of the facts, to establish a new standard of care when private persons are involved.\(^{42}\) It is likely that the least degree of fault, negligence, would be required since that position comports with the court's previous policy of protecting personal reputation even when the statement in question was made by mistake.\(^{43}\) The harshness of

---

37. *Id.* at 458.
38. *Id.* at 458-64.
39. *Id.* at 462-64. In *Firestone v. Time*, Inc., 305 So.2d 172 ( Fla. 1974), the Florida Supreme Court concluded that Time, Inc. was guilty of "journalistic negligence." *Id.* at 178. While the United States Supreme Court implied that this may have been the case, the Court vacated and remanded to the state court since there was a lack of a specific factual findings of fault at the trial level as required by *Gertz*.
41. To be liable for negligence an individual must fail to use reasonable care under the circumstances. This is the accepted standard. W. PROSSER, *supra* note 10, § 32, at 150.
strict liability coupled with the limited liability provided for in the Nebraska retraction statute would also seem to support a general standard of reasonableness.

If communicators attempt to act "reasonably" in all circumstances, their potential liability will be minimized as will that of their organizations. When there is any doubt as to a statement's impact, a thorough and impartial investigation of all sources should be conducted to ascertain and verify the facts and to evaluate the reliability of the sources. The communicator must balance the risk of injury of a communicated statement against the social utility of the statement. That is, the importance of the information to society and the need to release immediately the information must be balanced against the potential injury to the subject of the statement. A record of the communicator's "reasonable" efforts should be made for evidentiary purposes. As a final precaution, the communicator should procure liability insurance.

THE COMMON LAW RIGHT OF PRIVACY

The common law right of privacy may also be utilized as a basis for the imposition of liability for the use or dissemination of personal information. Simply stated, the right of privacy connotes "the right to be let alone." The common law right of privacy must be distinguished from the constitutional right of privacy. The constitutional right protects a citizen's expectations of privacy in relation to local, state, and federal government. Broadly construed, this concept encompasses the fourth amendment protection against unreasonable searches and seizures. This right has been expanded to include the marital privacy involved in deciding whether to use birth control devices and to individual decisions regarding the propriety of abortions. In contrast to the constitutional law of privacy, the common law right of privacy protects against unwarranted intrusions upon an individual by another individual or nongovernmental organization. This right has received widespread legislative and judicial acceptance.

44. NEB. REV. STAT. § 25-840.01 (Reissue 1975).
45. W. PROSSER, supra note 10, § 117, at 802.
46. Id. at 816.
50. See W. PROSSER, supra note 10, § 117, at 802-04.
51. Forty-six states protect the several interests classified under this concept. Only Rhode Island, Texas, and Wisconsin, in addition to Nebraska, do not
The law of privacy comprises "four distinct kinds of invasion of four different interests" of the individual, "which are tied together by the common name." Each represents an interference with "the right to be let alone." Of the four, there are three specific causes of action in which improper use or dissemination of personal information can create liability under the common law right of privacy:

(1) when the name or likeness of an individual is appropriated for the taker's benefit;

(2) when an individual is placed in a false light in the public's view; and

(3) when public disclosure is made of private facts concerning an individual.

In analyzing situations in which the right of privacy is an issue, the rights of free speech and press and the public's right to know present the counterbalance. The nature of our democracy tends to encourage freedom of action and expression rather than to inhibit conduct. This implies that when a person is in a public place he has consented to being observed or reported on. A photograph or an accurately written description of an event in a public place is merely a recorded observation of a scene which anyone in the public place could have viewed. Thus, it has been held that a person waives his expectations of privacy by entering the public view. Similarly, occurrences of a public nature such as issuances of marriage licenses, ambulance calls, accident reports, dispositions of court cases, and entries on law enforcement blotters can at least be factually and accurately reported without being actionable as a divulgence of personal information.

Presently, the common law right of privacy is not recognized in Nebraska. In 1955, in Brunson v. Ranks Army Store, the Nebraska Supreme Court rigidly applied stare decisis in holding that there was no common law right of privacy. The recognize a common law right of privacy. See Berthiaume v. Pratt, 365 A.2d 792, 794 (Me. 1976).

52. W. Prosser, supra note 10, § 117, at 804.
53. Id.
54. Id. at 804.
55. Id. at 812.
56. Id. at 809.
57. See Galella v. Onassis, 353 F. Supp. 196, 225 (S.D.N.Y. 1972), modified and aff'd., 487 F.2d 986 (2d Cir. 1973), for an interesting decision as to what is a public place and what a public figure consents to by being in a public place. This case involved a photographer who tried to photograph the President's widow, a public figure, everywhere she and her children went.
58. 161 Neb. 519, 73 N.W.2d 803 (1955).
59. Id. at 525, 73 N.W.2d at 806.
court reasoned that such a right should be provided by the legislature and not by judicial legislation. 60

However, it can be persuasively argued that Brunson should be overruled. 61 First, in 1966 in Myers v. Drozda, 62 the Nebraska Supreme Court decision overruled the long standing charitable immunity doctrine, 63 reflecting a trend away from the philosophy of judicial self-restraint. The court in Myers recognized stare decisis more as a guiding principle than an inflexible command. 64 Secondly, the interests protected under the common law right of privacy have in fact been protected to some extent under legal theories other than privacy, i.e., intentionally or recklessly inflicted emotional distress and defamation. 65 Thirdly, since the Brunson decision, there has been judicial recognition of a constitutionally based right of privacy in Griswold v. Connecticut. 66 Fourthly, a Nebraska case prior to Brunson 67 had recognized the right of privacy as being well established in English common law. 68 Finally, an analysis of the Brunson briefs indicates that the decision may have been the result of a weak brief 69 and argument rather than a firmly supported position that no common law right of privacy exists in Nebraska.

Further support for the proposition that Brunson should be reversed can be found in Carson v. National Bank of Commerce Trust & Savings, 70 a diversity action brought in federal district court and decided under Nebraska law. In Carson, a travel agency trying to promote business used the name of a well known entertainer without his consent. 71 The federal court deferred to the principle of comity, holding that no right existed on the basis of Brunson, 72 but suggested that the Nebraska Su-

60. Id.
63. Id. at 187, 141 N.W.2d at 854.
64. Id.
65. W. PROSSER, supra note 10, § 117, at 802.
66. 381 U.S. 479, 485-86 (1965). The lack of a constitutionally based right of privacy was a point made in the appellee's argument in Brunson. See note 69 infra.
68. Id. at 761, 110 N.W. at 766-67 (dictum).
69. Compare Brief for Appellant at 20-23, with Brief for Appellee at 7-55, Brunson v. Ranks Army Store, 161 Neb. 519, 73 N.W.2d 803 (1955). However, it should be noted that Brunson was an actor, arguably, a public figure. Therefore, his chances for a recovery suffered at the outset.
72. Id. at 814.
preme Court would change its position when the proper case arose before it.73

Although since Brunson the Nebraska Supreme Court has not again faced the issue of the existence of the common law right of privacy, the court has frequently recognized the general principle that the common law is a growing body of law constantly adapting to meet changing circumstances.74 For example, in Brown v. City of Omaha,75 a sharply divided court abrogated municipal and other local governmental immunity from tort liability arising out of the ownership, use, and operation of motor vehicles.76 Thus the Brown court recognized the need to adapt the common law when necessary.77

In contrast, the establishment of a common law right of privacy has neither the financial nor the planning implications of the Myers or Brown decisions. To guard against a right of privacy claim, only a general personal liability insurance policy need be procured. An individual concerned about personal liability would be covered at the outset. Therefore, a person not currently covered could not persuasively argue that the lack of a right of privacy action was the reason for his inaction in obtaining the insurance. The individual would be unable to rely upon established standards as an excuse. Further, the social policy of providing a remedy for every substantial wrong would be supported were a claim allowed. It appears that a well briefed and argued case, involving a proper plaintiff, would move the state from the disappearing minority to the more rational majority posture.78

As was discussed above, the right of privacy tort is comprised of four distinct types of intrusion. Three of these four may be utilized to impose liability on the communicator. A discussion of these three is appropriate in understanding their impact on the collection, use, and dissemination of information.

**APPROPRIATION**

The appropriation aspect of the right of privacy tort is essentially a pirating of another's identity for commercial gain.79

---

75. 183 Neb. 430, 160 N.W.2d 805 (1968).
76. Id. at 434, 160 N.W.2d at 808.
77. Id. at 433, 160 N.W.2d at 807.
78. Only four states including Nebraska do not recognize a right of privacy in a nongovernmental setting. See note 51 supra.
This type of invasion accords a proprietary notion to one's name and likeness. Liability arises when the name, photograph, or other likeness of an individual, usually a celebrity, is used without the individual's consent in order to cultivate a business advantage for the user. The most common example is an unconsented advertising endorsement of a product. Although the aggrieved party need not be a celebrity, the allegation that a business advantage was gained is more plausible when a celebrity is involved.

The gain must be direct, not incidental. For example, a newspaper intends to profit from its sales but it is not liable for appropriation merely because a person is mentioned in or is the subject of a news article. In Zacchini v. Scripps Howard Broadcasting Co., the Supreme Court may have established a factual precedent for the meaning of the term "incidental". Zacchini performed a "human cannon ball" act which was filmed and shown in its entirety (fifteen seconds) on a television newscast. Analogizing the event to the filming and broadcasting of a copyrighted dramatical work or of a prize fight or baseball game, the Court held that the first and fourteenth amendments do not immunize the news media when balanced against the competing right of publicity and the need to earn a living. Furthermore, the Court indicated that while the states may establish a broader privilege, the federal constitution did not require it. However, the dissent pointed out that the film was routinely shown during the course of a regular newscast and noted that the majority decision could create a possible self-restraint on the media resulting from the uncertainty in applying such a general principle in concrete situations.

Business organizations should utilize release forms to minimize the possibility of liability to employees under this tort. It is generally considered a reasonable condition of em-

80. Id.
81. Id.
82. Id. at 806-07. See generally Annot., 12 A.L.R.3d 865, 923 (1969) which identifies factual situations considered as incidental use.
84. 45 U.S.L.W. 4954 (June 28, 1977).
85. Id.
86. Id. at 4957.
87. Id. at 4958.
88. Id. The unique facts of Zacchini, however, greatly reduce its precedential value.
ployment to require employees to grant the use of their "name, picture, likeness or voice" to their employer for "advertising, publicity and other trade purposes" during the duration of employment. The scope and duration of the release should be clearly articulated in lay language and communicated in a manner designed to facilitate understanding. A broadly defined range of uses such as "to promote the business of my employer in any way" provides maximum flexibility while reducing potential liability.\(^\text{90}\)

**FALSE LIGHT**

Another cause of action subsumed in the right of privacy tort can accrue when an individual is placed in a "false light" in the public view. This occurs when dispersion is cast on a person as a result of an opinion, testimonial, or other form of statement falsely attributed to that person.\(^\text{91}\) Like defamation, this right of action protects reputation. Accordingly, truth is a defense.\(^\text{92}\)

The overlap of this tort with that of defamation brings into play the public/private distinction previously discussed. In *Time, Inc. v. Hill*,\(^\text{93}\) the Supreme Court trend of giving first amendment rights more weight than individual reputation was transplanted into the "false light" right of privacy context. As a

---

90. With respect to disclosing information about himself, the recommendations of the Privacy Protection Study Commission would limit the scope of consent which can be obtained from an employee and applicant for employment, insurance, or credit. The recommendation would require such authorizations to be:

- (a) in plain language;
- (b) dated;
- (c) specific as to the individuals and institutions he is authorizing to disclose information about him who are known at the time the authorization is signed, and general as to others whose specific identity is not known at the time the authorization is signed;
- (d) specific as to the nature of the information he is authorizing to be disclosed;
- (e) specific as to the individuals or institutions to whom he is authorizing information to be disclosed;
- (f) specific as to the purpose(s) for which the information may be used by any of the parties named in (e) at the time of the disclosure; and
- (g) specific as to its expiration date which should be for a reasonable period of time not to exceed one year.

*Privacy Study Commission, Personal Privacy in an Information Society*, 252-53 (1977) [hereinafter cited as *Study Commission Report*].


The false association attributed to the aggrieved party must be objectionable to the ordinary person, not the hypersensitive individual. The conduct attributed to the individual must be beyond community norms. *Id.* at 813.

93. 385 U.S. 374 (1967).
result, the burden of proof required for recovery in a privacy action increased dramatically when the aggrieved party was a private person involved in an event of "public or general concern."

In defamation actions, the scope of this qualified privilege has been narrowed to communications concerning only public officials and public figures. Since the concept of the qualified privilege was lifted intact from the defamation action and imposed on the privacy action, it seems probable that the Court will similarly relax the standard of liability in privacy actions when the proper case arises. For example, consider a series of love letters publicly attributed to an identified married male where the letters are not to his wife. If that individual is a former president of the United States, the burden of proof required for recovery is clear and convincing evidence that the communicator had knowledge of their falsity or acted in reckless disregard of the truth. On the other hand, if the identified individual was not a public official or public figure, the lesser burden of Gertz would likely be applied but the individual would have to prove actual injury. The same protective procedures associated with the tort of defamation should be applicable to minimize the probability of liability under the "false light" tort.

PUBLIC DISCLOSURE OF A PRIVATE FACT

The third relevant type of invasion of an individual's right to privacy is the public disclosure of a private fact. To be actionable, the public disclosure of a private fact must involve a matter which would be offensive and objectionable to a reasonable person of normal sensibilities. The nature of the interest protected is personal dignity and self-respect. Courts have often required the conduct to be "outrageous" or "shocking" before recovery is allowed. A commonly recurring example is the

95. In Cantrell v. Forest City Publishing Co., 419 U.S. 245, 250-51 (1974), the most recent false light case, the Court did not find the need to decide the issue. There does not appear to be any real distinction between the two types of actions.
98. W. PROSSER, supra note 10, § 117, at 811.
100. An example of the outrageousness required is aptly illustrated in this recently reported occurrence. A man was arrested inside his house. Although he
unreasonable conduct of creditors in collection procedures.\textsuperscript{101} Another example might be published photos of intimate or deformed parts of a person's body.\textsuperscript{102} No liability arises until the private facts are made public.\textsuperscript{103}

A recent Supreme Court case upheld the position that accurately reported facts gleaned from public record or proceeding are of a public rather than private nature.\textsuperscript{104} A rape victim's father attempted to recover on the basis that the defendant had infringed his right of privacy by broadcasting to the public the fact that his daughter was a rape victim.\textsuperscript{105} The proceeding in which the offender was prosecuted and the victim identified was a public trial. The Court analyzed the case from a "public substitute" vantage point.\textsuperscript{106} The broadcast was considered a description of a public event which any citizen could have viewed if present in the public place.\textsuperscript{107}

Similarly, an individual must expect some reporting of his public activities.\textsuperscript{108} If a person publicly engages in an occupation, no liability should arise if a newspaper or broadcast reports a promotion or demotion. Those who seek publicity on a certain matter may not later claim their privacy has been invaded. Their action is equivalent to implied consent.

Additionally, those who are involved with a public entity such as a law enforcement agency, fire department, or rescue squad should expect to suffer some loss of privacy as a result of their interaction with the public even if it is involuntary. The public's right to know justifies release of a minimal amount of

\textsuperscript{102} See Comment, Debtor v. Creditor Dilemma: When does a Creditor's Communication with a Debtor's Employee Result in an Actionable Invasion of Privacy, 10 Tulsa L.J. 231 (1974).
\textsuperscript{103} W. Prosser, supra note 10, § 117, at 810.
\textsuperscript{104} Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).
\textsuperscript{105} Id. at 474.
\textsuperscript{106} Id. at 492-93.
\textsuperscript{107} Id. at 493.
\textsuperscript{108} See note 57 and accompanying text supra.
information. The name of a suspect or offender in a criminal case could be released on this basis. The minimal amount of information expected from a report of a fire call might include date and time of fire, location, type of building, and owner. Information that could be released by a hospital pertaining to a patient brought in by a public rescue squad might include name, address, age, sex, marital status, occupation, time of admission, general description of the injury, and a summary statement of condition. In contrast, in the absence of a release, no personal information should be disseminated regarding patients who enter a hospital by private means except to acknowledge their presence and their room number. The facts of occurrences which by law are reportable to public authorities such as the police, coroner, or public health officer are generally not private facts.

The process of distinguishing private facts from public facts is hardly ever clear-cut, particularly when a public official or public figure is involved. The implications of the constitutional distinction between public and private figures are unclear. In defamation cases, the injury-causing statement must be false. In contrast, liability for disclosure of private facts occurs on the basis of true statements. Since the purpose of the first amendment is to protect self-governing type speech, true statements coincide more closely with this purpose and should be more deserving of constitutional protection.

Subjects of disclosures of private facts can be divided into these classifications for consideration of the constitutional implications:

1. private figures;
2. involuntary public figures;
3. voluntary public figures; and
4. candidates for public office and public officials.

Notably, there is a definite inverse relationship between the nature of the facts disclosed and the magnitude and manner of attaining public importance; that is, as prominence increases,
the range of facts considered private decreases. A congressman or candidate for Congress would have fewer private facts than a professional athlete since a greater variety of facts would be relevant to his performance in public office. This approach is more congruent with the self-governing notion of the first amendment.

As indicated, more disclosures can be made about events occurring in a public place than a private place. However, the confines of a public place are not always easy to distinguish from that of a private place. Further, even in a public place, events beyond the control of a person may reestablish an expectation of privacy. For example, a person driving in an automobile on a public street has waived his expectation of privacy. Suppose that person is involved in an accident, is thrown from his car, and has suffered severe and ugly injuries. A photograph or a television film showing the general scene of the accident would not be actionable. As the detail of the scene increases so too does the potential liability. To prove an actionable claim; the injured person would have to demonstrate that the personal dignity or self-respect of an ordinary person in the community would suffer as a result of the publicity.

Planning to minimize liability in the case of a public disclosure of private facts is more difficult since truth is not a defense. Business organizations in the private sector can often use release forms with employees and others to minimize potential liability. The events which generate a release of information for business purposes should be identified as precisely as possible in the form. Timing of the signing of a release is also important. For example, arguably, the facts involved in firing an employee can be inflammable. If that employee had signed a release prior to being fired, the relevant facts could be provided to a prospective employer of the individual without fear of liability. The prospective employer could also have the dismissed employee sign a general release pertaining to information relating to previous employment. Although no liability may exist

115. See Virgil v. Time, Inc., 527 F.2d 1122, 1127 (9th Cir. 1975).
116. See note 90 supra.
even in the absence of a release, sound planning practices dictate that releases be used if any doubt exists. Furthermore, if privacy legislation is imposed on the private sector, the experience gained in establishing procedures for obtaining releases will be invaluable.

When a release is not relevant or is impractical, the initial step should be to determine the accuracy of the fact(s) in question. If there is no factual substance, then the choice is clear. However, if a reasonable investigation to ascertain the truth of the matter substantiates the facts, the next step is difficult. The public/private figure distinction plays a role. It is clear that a private figure has a greater range of private facts than a public figure. The inverse relationship formula suggests that the greater the prominence of the individual, the fewer private facts there are to be protected. From a planning viewpoint, however, this formula does not provide complete operational guidance. Sound information use practices are important and should be followed, but insurance may be the only practical way to minimize liability.

IV. INFORMATIONAL PRIVACY LEGISLATION

In conjunction with common law liability, the imposition of liability in the private sector has occurred through legislation dealing with informational privacy. This legislation has been proposed and enacted in response to technological advancements made in recordkeeping capability, especially with the advent of computerized systems.118

118. Consumer concern over privacy considerations of the emerging electronic funds transfer (EFT) systems is reflected in the interim report submitted to Congress by the National Commission on EFT. The Commission expressed concern over the amount and types of information EFT could create as well as the increased ease of access.

The amount of personal financial transaction information collected under EFT could increase. Cash transactions have fewer recordkeeping activities associated with them than other types of financial transactions. Thus for each cash transaction replaced by an EFT transaction, records are created that otherwise would not exist.

The kinds of information collected about personal financial transactions could increase under EFT. Information captured in an EFT transaction could include the date, time of day, location, amount of payment, type of transaction, and recipient of payment. Because of the difficulty of providing adequate audit trial information to protect both the consumer and the institution, more descriptive information about a transaction may be required to distinguish between different kinds of transactions.

The present payment system includes both paper and electronic processing and storage of personal financial transaction information. This provides a limited amount of protection due to the difficulty and cost of
Over the past sixteen years computer systems have become an integral part of the nation's recordkeeping activities in both the public and private sectors. They normally offer greater efficiency in coping with the information flow that parallels the physical operations of government and business. Computer system speed and communication networks usually promote better informed decisions by providing more meaningful and more timely information than was previously available with traditional recordkeeping systems. Likewise, computers tend to make personal information more accessible.

Easier and uncontrolled access means a higher probability of injury to the individual. In general, the nature and the magnitude of the risks vary with the type of information available and the circumstances in which it is to be applied. The danger includes the risks that:

1. accurate, complete, and timely information will be applied in irrelevant circumstances; and
2. inaccurate, incomplete, and outdated information will be utilized in decisions affecting an individual.

Commonly cited examples of abuse include the use of incomplete criminal history records for employment purposes and inaccurate credit reports in determining whether to grant credit.

accessing such information readily. EFT will reduce this protection by increasing the ease and reducing the cost of such access.

The Commission recommended that all private sector use of information concerning a consumer's depository account, without the specific consent of the account holder, be declared unlawful except for utilization to verify or complete the EFT transaction or for information regarding the improper use of the account. Id. at 29. See also STUDY COMMISSION REPORT, supra note 90, at 101.


119. A computer is only one alternative when information systems are examined for possible change. It is not the solution in every set of circumstances.

120. The computer has served to preserve records much longer than they are relevant. Once a computer record is established it can be cheaper to continue to store the information than to purge it because of the computer time involved.

121. The Fair Credit Reporting Act, 15 U.S.C.A. §§ 1681 to 1681t (1974) is a positive approach to curbing past abuses in the credit reporting area. The recommendations of the Privacy Protection Study Commission would prevent employers from using arrest records unless required by law, and even then only if the record is less than a year old. Arrest records more than a year old could be
The thrust of successful privacy legislation is a recognition of mutual responsibility on the part of recordkeepers and individuals. Recordkeepers should only request information relevant to the purpose for which the relationship with the record subject exists (employer/employee, etc.) and use the information provided only in accordance with the disclosed purpose.\textsuperscript{122} Accordingly, the record subject need only supply relevant information as a condition of establishing the relationship and should have a means of reviewing his record to determine completeness and accuracy and proper use of the information. A third party, such as a judicial system, should rule on disputes.

The core premise of mutual responsibilities is embodied in the important "routine use" concept utilized in privacy legislation, notably the Federal Privacy Act of 1974.\textsuperscript{123} This concept provides for a reasoned balance between individual privacy and the efficiency of the operation of the recordkeeper's business system. The recordkeeper notifies the record subject of the purposes for which specific information is requested and the routine use to be made of the information including the category of users to whom it may be distributed.\textsuperscript{124} A third party scrutinizes the validity of the recordkeeper's needs and practices and the security of its operational practices.\textsuperscript{125} All uses within the set of routine uses may then occur without the consent of the subject. For example, the General Services Administration defines a routine use of its employees' payroll statistics and identification information (social security number) as distributed to the Treasury Department and local taxing authorities for the purpose of insuring compliance with federal and local tax laws.\textsuperscript{126} Some of the same information would also be routinely passed to the Social Security Administration for eligibility purposes. This pertinent information is routinely transferred without the consent of and without further notice to

\small

\textsuperscript{122} See, e.g., id. at 237.

\textsuperscript{123} 5 U.S.C. § 552a (Supp. IV 1974).

\textsuperscript{124} The effectiveness of publishing such notices in the Federal Register, as the federal government does under the Federal Privacy Act of 1974, has been criticized. Belair, \textit{Less Government Secrecy and More Personal Privacy}, Civ. Lib. Rev., May-June 1977, at 15. Belair suggests that personal notice may be the only effective method to notify citizens of the information maintained in almost 7000 government data systems and of the routine uses of such information. \textit{Id.}

\textsuperscript{125} Currently no effective extra-agency scrutiny of internal practices is required by the Federal Privacy Act of 1974.

\textsuperscript{126} The routine use notices by federal agencies have substantially increased the size of the Federal Register. During the last five months of 1975 these notices cost taxpayers over $800,000 to print.
the record subject. In the absence of the routine use concept, most governmental agencies would be unable to function since all transfers of information would be subject to the approval of the record subject.\textsuperscript{127}

Since the routine use concept must be utilized in legislation affecting the private sector, it will be considered in a more general manner. Suppose recordkeeper A has requested and received information from individual X and has informed individual X of the purpose, routine uses, and category of users. This essentially creates a three dimensional use "matrix" for classes of information obtained from groups of individuals. Suppose individual or organization B later requests information from recordkeeper A on individual X. Recordkeeper A looks to its routine use matrix; if the intended use is routine for the specifically requested information and B is among the allowable range of users for that information, A complies with the request. If not, the request is denied and B must satisfy additional conditions such as a written release by X before gaining access to the information.

Several other key distinctions should be considered before examining specific legislation. A noncomputer-based personal data system can be as lethal to individual rights as can a computer-based system. This includes paper-based and microform systems. From a recordkeeper's point of view, this means that liability can be minimized only by information practice planning for all forms of systems. Another distinction is that existing legislation pertains to, and liability exists only for, the misuse of personally identifiable information as opposed to nonpersonally identifiable information compiled for statistical and planning purposes. For example, the information contained in census survey forms is confidential but the compilation of statistics based on that information is not, since no individual is identified.\textsuperscript{128}

The final distinction to consider is the identity of the recordkeeper. This is crucial to determining the applicability of privacy laws. With two major exceptions, the current objective of

\textsuperscript{127} Under the routine use concept, public records are those which are available to any person or organization for any purpose.

\textsuperscript{128} The publication or other public use of research results is another area in which the issue is whether the information is personally identifiable. See 41 Fed. Reg. 54846 (1976) (to be codified in 28 C.F.R. section 22) (regulations controlling the confidentiality of identifiable research and statistical information collected in Law Enforcement Assistance Administration funded studies); see also STUDY COMMISSION REPORT, supra note 90, at 567 (recommendations for controlling the use of information gathered about an individual in research projects).
federal and state laws is to put the government house in order before going after the private sector. However, although not presently applicable, the existing laws and the report of the Privacy Protection Study Commission forecast future enactments in the private sector.129

In addition, it is significant to note that a constitutional right of privacy is applicable to personal information in governmental data banks even in the absence of legislation. Similarly, the common law right should protect citizens from serious misuses of information contained in private data banks. The right of privacy action coupled with the following legislative enactments should insure greater protection for the individual.

**Federal Privacy Act of 1974**

The Federal Privacy Act of 1974130 applies to the use of federal government record systems containing personally identifiable information whether computerized or in other forms.131 As a compromise measure, it controls the gathering and dissemination of personal information by federal agencies but does not control state or local governmental bodies. Moreover, it does not pertain to organizations or institutions which merely receive federal funds.132

The law operates on the routine use concept.133 Its enactment is a good initial effort to balance the societal interests previously identified.134 Violators of its provisions face criminal penalties.

---

129. Although the Privacy Protection Study Commission is not recommending legislative mandates for all private sector record systems, the inference can be made that if voluntary compliance does not occur, legislation may be recommended. *STUDY COMMISSION REPORT, supra* note 90, at 34.


131. The Act's provisions are limited to federal government agencies as defined in 5 U.S.C. § 552a(e) (Supp. IV 1974).

132. The Act is not applicable to Congress, the District of Columbia, or the federal courts. It is applicable to private contractors who operate a federal agency's record system. 5 U.S.C. § 552a(m) (Supp. IV 1974).

133. *Id.* § 552a(b)(3). *See also id.* § 552a(a)(7).

134. The Privacy Protection Study Commission investigated the application of the 1974 Act and concluded that:

1. the Privacy Act represents a large step forward, but it has not resulted in the general benefits to the public that either its legislative history or the prevailing opinion as to its accomplishments would lead one to expect;

2. agency compliance with the Act is difficult to assess because of the ambiguity of some of the Act's requirements, but, on balance, it appears to be neither deplorable nor exemplary;

3. the Act ignores or only marginally addresses some personal data
sanctions and civil liability. The Act's weakest point is its failure to establish an adequate supervisory vehicle over agency practices and procedures. The most important provision is the establishment of a Privacy Commission which is empowered to study the issues relating to informational privacy and to recommend legislative measures to deal with their resolution.

The scope of the law includes the following provisions:

(1) With only a few exceptions, a listing of federal data banks must be published annually in the Federal Register. In addition, the routine uses of such records must be specified. This aids a citizen in determining what records pertaining to him are maintained and how they are used.

(2) Only information relevant and necessary to accomplishing a governmental function may be collected. Citizens must be informed why agencies need personal information at the time it is requested. The consequences of failing to provide the requested information must be indicated.

(3) Each citizen may examine his records and request modifications on the basis of inaccuracy or incompleteness.

136. The office of Management and Budget (OMB) issued general guidelines for implementing the Act and various agencies created their own specific rules but there is no real administrative overseer of agency practices and procedures.
138. 5 U.S.C. § 552a(e)(4) (Supp. IV 1974). However, see note 124 supra.
139. Id. § 552a(e)(1).
140. Consider, for example, the form accompanying the yearly Reserve Qualification Summary questionnaire which an individual may receive from the Marine Corps Reserve. It informs the individual of the authority and principal purpose for the request, the routine uses to be made of the information, and that the provision of information is voluntary on the individual's part but the chances for promotion and active duty assignments would be hampered by noncompliance.
The recordkeeper must promptly investigate the request. Review of refusals to modify is provided and, if all remedies are unsatisfactory, the citizen may file a statement of dispute which becomes part of his records. The opportunity to individually challenge and correct one's records is the best possible check for accuracy and completeness.

(4) The reliability of personal information is also increased by the requirement imposed upon each agency to investigate the accuracy, completeness, relevancy, and timeliness of personal data each time it is utilized or when it is transferred to a party or organization which is not an agency. These requirements increase the probability of fairness in decisions concerning the record subject.

The Privacy Protection Study Commission has recommended amendments to the provisions of the 1974 Act. Many of the changes proposed are based on the lessons learned during the implementation of the initial law. The 1974 Act would be amended to minimize the variations in interpretation which have occurred because of the use of ambiguous language. If the recommendations become law, decisionmaking regarding recordkeeping practices in specific situations could be based on “reasonableness tests” instead of the more ambiguous “appropriate” and “any anticipated threats or hazards” tests now required.

An executive branch overseer without regulatory authority would aid and monitor the implementation of all federal privacy laws. It would also assist in the implementation of privacy laws pertaining to the private sector imposed by both the federal and state governments.

**FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT OF 1974**

The purpose of the Family Educational Rights and Privacy Act of 1974 is to provide greater privacy safeguards to parents and students through the application of fair information prac-

142. Id. § 552a(d)(3).
143. Id. § 552a(e)(6).
144. See STUDY COMMISSION REPORT, supra note 90, at 497.
145. Id. at 502-03.
146. Id.
147. Id. at 37.
TORT

It is applicable to public and private schools of all levels which receive federal funds. The statute derives its power from the federal government's ability to withhold funds if school districts or educational institutions do not comply with its provisions.

In general, unless the student (or parent when applicable) gives written consent, an educational institution may not release any personally identifiable information or allow access to records by any third party except within the routine use for which the record was created and in other limited circumstances. Students eighteen years and older are granted inspection, review, and amendment rights similar to those provided for in the Federal Privacy Act of 1974. Parents are provided those rights when the student has not yet reached eighteen years of age.

The Privacy Protection Study Commission has recommended amendments to the law including the following. Educational agencies and institutions would be required “to formulate, adopt and promulgate an affirmative policy” to implement the Act and to establish information practices to improve the accuracy of records. Initially, the Act was directed primarily at the security of records rather than their accuracy. The definitions of “educational agency or institution” would be expanded for many purposes to encompass organizations which provide testing or data assembly services under contract to educational agencies or institutions. Additionally, the definitions of the terms “educational records” and “student” would be expanded. Applicants for student status would have rights under the law if the recommendations are followed.

**FAIR CREDIT REPORTING ACT**

Finally, the most significant federal enactment dealing with

---

151. Id. § 1232g(a)(1)(A). State statutes dealing with educational records may create more restrictive conditions on the dissemination of information to third parties but may not impair student and parental rights. See NEB. REV. STAT. §§ 79-4,156 to -4,158 (Reissue 1978) and the text accompanying note 198 infra.
155. STUDY COMMISSION REPORT, supra note 90, at 431.
156. Id. at 432-33.
157. Id. at 434.
158. Id.
informational practices in the private sector is the Fair Credit Reporting Act. Although the primary intent of this federal law is to strike a delicate balance between the right of individual privacy and the consumer's ability to obtain credit, it is also specifically directed at the utilization of credit reports in employment and insurance-granting decisions. It is applicable to any person or organization which utilizes any means or facility of interstate commerce in preparing or furnishing the specified decisional-type information.

In general, as the right of privacy becomes more absolute, it costs financial and consumer credit institutions more to learn less about a consumer with a resulting higher magnitude of risk in the credit transaction. Some dissemination is required because of commercial need. On the other hand, only accurate, complete, relevant, and timely information should be utilized in the decision whether to grant credit or insurance, or to employ.

Under the Act, consumers have the right to learn the "nature and substance" of information maintained by a consumer reporting agency. The consumer currently does not have a right of access to his file, only to a summary of its contents. The source of most of the information may be ascertained. Specific recipients of reports based on the consumer's file such as financial institutions, insurers, and prospective employers, must be identified. The reporting agency may not charge for providing this service to the record subject when it has supplied a report which has adversely affected the individual, i.e., denial of credit or insurance, refusal of employment.

Many reports dealing with the financial situation of an individual and upon which decisions are based are covered. To determine whether a specific transfer of information is covered

160. Id. § 1681. Currently the Act is not applicable to commercial credit transactions. The Privacy Study Commission would expand its coverage to include some commercial credit transactions. STUDY COMMISSION REPORT, supra note 90, 88-100.
162. Id. § 1681(b).
163. Id. § 1681g(a)(1).
164. Id. § 1681g(a)(2).
165. For employment purposes, such recipients must be identified within the two-year period preceding the request, and for other purposes, the identification must occur only for the six-month period preceding the request. Id. § 1681g(3).
166. Id. § 1681j.
167. Id. § 1681a(f). See also Geltzer, Fair Credit Reporting Act: Survey and Checklist, 94 BANKING L.J. 223, 228 (1977) [hereinafter cited as Survey].
by the Act, the nature and sources of the information collected and the purpose for which it is to be used must be examined. 168 An organization may be a consumer reporting agency regardless of the official name of the entity. 169 For example, a business which regularly provides information on its former employees to prospective employers of those employees may be acting as a consumer reporting agency. 170 However, a consumer report does not include a report containing information based solely on transactions or experiences between the subject consumer and the person or organization making the report. Thus, the Act does not apply if the report made to a subsequent employer covers only transactions between the subject and his previous employer. 171

Consumer reports may only be made in conjunction with a currently contemplated credit, employment, or insurance transaction. The purpose must exist at the time the request for the information is made. 172 This limits blanket releases when no business purpose exists.

Users of credit reports who deny individual rights on the basis of a report must identify the reporting agency and the nature of the information which caused the adverse decision. 173 If an organization uses credit reports in its decisionmaking processes, then this provision likely has implications for its operations.

Although a reporting agency is not required to inform a consumer of this right, each individual may challenge the contents of his file. 174 If the dispute cannot be resolved, the consumer has the right to have his version of the contested facts included in future credit reports. 175

Specific items of information deemed obsolete and irrelevant may not be included in any report. 176 Dissemination of reports is limited to general categories of users. 177 Limited safeguards are also imposed on the preparation and use of inves-

169. Id. § 1681a(f).
170. Id. § 1681a(d)(2),(f).
171. Id. § 1681a(d)(2).
172. Id. § 1681b. See Survey, supra note 167, at 235, for decisions regarding what is and is not a permissible purpose.
174. Id. § 1681l.
175. Id. § 1681l(b).
176. Id. § 1681c.
177. Id. § 1681b(3).
tigative consumer reports.\textsuperscript{178}

The Privacy Protection Study Commission is recommending various amendments to the Act, which include the following:\textsuperscript{179}

(1) a means of external governmental examination of controversies concerning information used and collected by credit grantors and insurers would be established;\textsuperscript{180}

(2) credit grantors, employers, and insurers would be required to take "reasonable care" in selecting and using credit bureaus, independent authorization services, and other support organizations to assure that the information practices of such organizations comply with the Commission's recommendations;\textsuperscript{181}

(3) the individual would have the right to see and copy all information a credit grantor has used to make an adverse credit decision about him. A more comprehensible manner of communicating information about adverse decisions would also be required;\textsuperscript{182}

(4) the consumer would have the right to see and copy information maintained in credit bureaus or independent authorization services;\textsuperscript{183}

(5) an affirmative duty would be imposed on credit grantors to correct inaccurate information reported to a credit bureau or independent authorization service;\textsuperscript{184} and

(6) more disclosure would have to be made to the individual concerning the types and sources of information to be collected about him as an applicant for credit, insurance, or employment including: the techniques to be used in gathering such data, the manner in which the data will be used, and to whom specific elements of information will be disclosed. Organizations would have to establish formal information practices and identify them for applicants.\textsuperscript{185}

\textsuperscript{178} Id. § 1681d. Contrast the definition of consumer report"; id. § 1681a(d) with that of "investigative consumer report" in id. § 1681a(e). The investigative report is generally less factual and thus is potentially more dangerous to individual rights.

\textsuperscript{179} See generally Study Commission Report, supra note 90, at 74, 188, 235, which, respectively, are the recommendations for the consumer-credit grantor, insurance, and employment grantor relationships. The Federal Trade Commission recently began an investigation of computerized credit bureaus to determine if the information they retain on consumers is accurate.

\textsuperscript{180} Study Commission Report, supra note 90, at 74, 188.

\textsuperscript{181} Id. at 75.

\textsuperscript{182} Id. at 77-78. In the insurance context, see id. at 200, 204.

\textsuperscript{183} Id. at 81.

\textsuperscript{184} Id. at 82, 83.

\textsuperscript{185} See, e.g., id. at 76, 85.
Consumer advocates have argued that detailed regulations are needed to accomplish the Fair Credit Reporting Act's intent. Consumer credit reporting agencies respond, on the other hand, that greater rights would substantially diminish an individual’s ability to obtain credit because of higher operational costs and increased transactional risks. The comprehensive recommendations of the Commission would certainly increase the fairness of decisions made about the individual in the credit, employment, and insurance contexts if they are enacted into law. On the other hand, their encompassing nature will probably lead to some dilution of the amendments. However, those recommendations which are enacted will be positive steps toward better information practices.

**State Statutes**

Along with federal attempts to legislate information practices, states have also acted to protect individual privacy. State laws provide various types of protection for the confidentiality of records. Most states recognize the confidentiality of communications under the doctor-patient privilege. Several states have statutes relating to school records and credit reporting which complement the federal acts. Others have laws protecting the confidentiality of criminal history records and tax return information. Only a few state legislatures have enacted comprehensive acts dealing with state and local governmental data banks and informational practices.

Nebraska currently has no comprehensive act. L.B. 326, introduced in the 1975 Unicameral, was a well-timed but poorly researched and drafted bill. Its scope covered every automated personnel data system conceived, including those of the private sector. The uncertainties inherent in its ambiguities posed

---


187. COMPILATION, supra note 186, at 10.

188. Id. at 28-30. At least 14 states have enacted some version of a fair credit reporting act and at least another 22 have had legislation introduced. Id.

189. Id. at 10, 23-25.

190. Id. at 27.

191. Arkansas, California, Connecticut, Indiana, Massachusetts, Minnesota, Ohio, Utah, and Virginia. Id. at 31-32.


193. Id. § 1(7).
grave doubts for both state and local government as well as for business organization operations. Its complexity and vagueness lead to a greater lack of understanding than is common to legislation of this type. L.B. 326 died in the Miscellaneous Subjects Committee.¹⁹⁴

The bill did, however, serve as an impetus to the enactment of a law which limits the release of personal information on state employees.¹⁹⁵ This legislation simultaneously indicated that public records were not affected and articulated a broad definition of public records.¹⁹⁶ Administrative agencies and the judicial system were delegated the responsibility of sorting out public information from private information maintained in state record systems.¹⁹⁷

Additionally, the Unicameral has enacted protective legislation concerning the use of records of educational institutions and systems. Public school pupils and their parents or guardians are authorized access to those school files or records relating to the subject pupil.¹⁹⁸ The law also provides that all full-time employees as well as administrators and teachers in public school systems may have access to their personnel records.¹⁹⁹ An affirmative duty is imposed upon boards of education to establish and publish information policy and practices regarding student and personnel records.²⁰⁰

None of the Nebraska provisions have any apparent conflict with the Family Educational Rights and Privacy Act and should be considered supplementary to the federal provision. However, unlike the federal act, the Nebraska provisions have no applicability to the private educational institutions or systems.²⁰¹

Other Nebraska laws and regulations apply only to records held in public depositories as opposed to those record systems maintained by the private sector.²⁰² There is no indication that

¹⁹⁴. For a complete analysis of the bill, see F. Greguras, L.B. 326: Personal Data Systems and the Right of Privacy (May, 1975) (unpublished memorandum to the Legislative Council of the State of Nebraska.)
¹⁹⁶. Id. § 81-1117.04.
¹⁹⁷. See id. §§ 84-712, .03.
¹⁹⁸. Id. § 79-4,157.
¹⁹⁹. Id. § 79-4,156.
²⁰⁰. Id. § 79-4,158.
²⁰¹. The term “public school” is used or implied in each statute.
²⁰². Id. § 43-206.04(2) (Reissue 1974) (juvenile court and investigative and probation officers' records); L.B. 384, 85th Legis., 1st Sess. (1977) (bank records and law enforcement agencies); Neb. Dept. of Revenue, Policy No. 29: Confidential Information, Safeguards and Disclosure (1976) (policy based on
any present state senator will make informational privacy a personal cause. Thus, the probability of broader privacy legislation being enacted at the state level is very slight. Nebraskans desiring to review records maintained on them by the state government can, arguably, compel disclosure on the basis of Nebraska's public record review laws since the personal information to be reviewed could be construed as being public with respect to the subject of the information.203

The fundamental lesson to be learned from the experience of state legislative activity is to proceed deliberately, incrementally, and, most importantly, rationally. Privacy is a volatile issue. It can be used to build a political image without concern for practicality. For example, an ill-conceived state law dealing with the confidentiality of criminal history records lasted three days in Oregon.204 Its measures were so stringent that a wife was unable to ascertain if her husband had been arrested. The Minnesota privacy law has been amended several times to shape it into workable form.205 The Minnesota Legislature initially failed to appropriate any funds for implementation.

After analyzing state information practices, the Privacy Protection Study Commission "emphatically does not recommend wholesale application by the Federal government of the Privacy Act of 1974 to state and local government record keeping. The commission believes that the states' creative work in devising privacy protections for the individual in his relationships with state government should continue."206

The Commission does recommend that privacy protection for the individual be required at the state and local level as a condition of federal assistance, such as the Federal Educational Rights and Privacy Act.207 Other areas noted by the Commission for this approach include public assistance and social serv-

203. NEB. REV. STAT. §§ 81-1117.04, 84-712, .01, .03 (Reissue 1976).
204. COMPUTERWORLD, Oct. 1, 1975, at 1-2; See COMPUTER L. & TAX REV., June, 1975, at 3, for a discussion of a Pennsylvania bill which would cause chaos if enacted. See also COMPUTER L. & TAX REV., June, 1976, at 1, for an evaluation of the New Jersey and Wisconsin bills which would go further than their sponsors ever imagined in regulating conduct.
206. STUDY COMMISSION REPORT, supra note 90, at 490.
207. Id. at 492.
ices, research and statistical activities, and the confidentiality and use of federal tax returns.\textsuperscript{208} The measures required would be a baseline which states could increase in intensity but could not dilute.\textsuperscript{209}

Essentially, the Commission would not change the current division of regulatory responsibility for information practices. "The recommended measures create no new authority [for a state] to regulate the record keeping of organizations that are not now subject to state regulation, nor do they deprive a state of regulatory authority it now has."\textsuperscript{210}

V. CONCLUSION

Except for the Fair Credit Reporting and Family Education Rights and Privacy Acts, neither federal nor state laws generally apply to the private sector's data bases containing personal information.\textsuperscript{211} However, in establishing information practices for handling the personal information of employees, clients, and customers, the private sector should carefully scrutinize the report of the Privacy Protection Study Commission and closely monitor legislative developments since government's self-imposed information practices are likely a prototype of what could ultimately apply to private concerns.\textsuperscript{212} The cost and procedural

\textsuperscript{208} Id.

\textsuperscript{209} For example, the Family Educational Rights and Privacy Act contains a research exception, 20 U.S.C. § 1232g(b)(1)(F) (Supp. V 1975). Qualified researchers can obtain access to educational records without the consent of the subject under this exception. However, since negation of the researchers' right would increase, not impair, the rights of students and their parents or guardians, a state statute need not grant such a right.

\textsuperscript{210} STUDY COMMISSION REPORT, supra note 90, at 492.

\textsuperscript{211} It can be strongly argued that the omnibus regulation of the private sector requires uniform national legislation rather than regulation by diverse and possibly conflicting state laws. Multiple and divergent laws could create an unreasonable burden on business organizations operating in interstate commerce. See, e.g., Pike v. Bruce Church, Inc., 397 U.S. 137 (1970); Bibb v. Navajo Freight Lines, 359 U.S. 520 (1959); Southern Pac. v. Arizona, 325 U.S. 761 (1945). This issue is a factual one which would have to be decided on a case-by-case basis with the particular statute and specific industry regulated being the key elements.

\textsuperscript{212} Following the submission of the Privacy Protection Study Commission Report, more than a dozen bills were introduced in Congress to aid in implementing its recommendations.

H.R. 1984, 94th Cong., 1st Sess., 121 CONG. REC. 1216 (1975), was the most publicized federal bill proposed for the private sector prior to the Commission's report. Its power is based on the commerce clause. Since it is an omnibus bill and not specific for one industry, it will likely be abandoned in view of the Commission's recommendations.

One important recommendation of the Commission was that the legal restrictions on the collection and use of the social security number by the
difficulties of implementation and continuing operations also can serve as predictors for the future. The legislative recommendations of the Privacy Protection Study Commission primarily affect the federal government. However, legislative proposals have been made for the banking and medical care industries as well as more detailed statutory recommendations for the credit granting, investigative reporting, and insurance industries. A number of proven information practices were recommended for other records systems, including personnel record systems, but the Commission did not recommend that they be implemented by legislation.

A single omnibus law which applies uniformly to all businesses will not be enacted. Rather, the Commission has submitted recommendations with a general theme but which are federal government, as imposed by the Privacy Act of 1974, should not apply to private organizations. Study Commission Report, supra note 90, at 615.

The Commission finds that restrictions on the collection and use of the SSN to inhibit exchange beyond those already contained in law would be costly and cumbersome in the short run, ineffectual in the long run, and would also distract public attention from the need to formulate general policies on record exchanges.

Id. at 614.

213. For an in depth analysis of the cost issue, see R. Goldstein, The Cost of Privacy (1975). Costs in implementing the Privacy Act of 1974 are substantially less than estimated. Start up costs and the initial nine months of operating expenses amounted to about $66 million. Office of Management and Budget's (OMB) 1974 estimates indicated that the annual cost through the first five years would be about $200 to $300 million with an additional one-time start up cost of $100 million. See OMB, Costs of Implementing the Privacy Act of 1974 (March, 1977) (unpublished report).

214. For the Commission's analysis of the alternatives for implementation of its recommendations and its choices, see Study Commission Report, supra note 90, at 33-37.

215. The Commission stated:

In the Private sector, the Commission specifies voluntary compliance when the present need for the recommended change is not acute enough to justify mandatory legislation, or if the organizations in an industry have shown themselves willing to cooperate voluntarily . . .

The Commission also relies mainly on voluntary compliance in the area of employment and personnel . . . In this area, the Commission prefers to rely mainly on voluntary compliance because of the complexity of the relationship between employer and employee, and the difficulty of classifying all the various records different employers maintain about their employees and the way they use these records in employment decision making. For the Commission to recommend otherwise would be to recommend uniformity where variation is not only widespread but inherent in the employee-employer relationship as our society now knows it.

Most of the Commission's recommendations, however, do specify mandatory measures. This is partly because the Commission believes that in most cases voluntary compliance would be too uneven to be dependable; but more importantly, many of the issues the Commission's recommendations address are legal ones and require legal remedies.

Id. at 34.

216. See note 212 supra.
specific to types or classes of organizational recordkeepers. Any legislation enacted will thus be somewhat piecemeal but will be more practically oriented since it will apply to a specific type of business. Specific industries would be required to meet standards of confidentiality and protection particular to the nature of the information they collect, maintain, and utilize.

The burden of initiating action to see or copy one's records or to correct inaccurate information, a right the Commission found common to most forms of recordkeeping, will be on the record subject. This will minimize the cost to the private sector since no duty of notification is imposed. If an individual asks a recordkeeper whether its records contain information on him, the custodian will have a duty to determine if records do exist, but the recordkeeper need not notify the individual otherwise.

A synthesis of federal and state laws, proposed legislation, and Privacy Study Commission recommendations provides the following glimpse at the probable core provisions of enacted private sector laws. Steps taken now by private industry toward phasing in these administrative principles will minimize economic and operational impact later.

(1) Personal information collected from individuals should be relevant to the purpose for which it is obtained. The degree of supervision to be established over these standards is unclear.

217. The Commission concluded that "an effective privacy protection policy must have three concurrent objectives," which are:

- to create a proper balance between what an individual is expected to divulge to a record-keeping organization and what he seeks in return (to minimize intrusiveness);
- to open up record-keeping operations in ways that will minimize the extent to which recorded information about an individual is itself a source of unfairness in any decision about him made on the basis of it (to maximize fairness); and
- to create and define obligations with respect to the uses and disclosures that will be made of recorded information about an individual (to create legitimate, enforceable expectations of confidentiality).

218. See, e.g., STUDY COMMISSION REPORT, supra note 90, at 81, but this right may also be conditioned upon an adverse decision being made about the individual. Id. at 77-78, 109.

219. Id.


221. If the information will not be used, why pay for the cost of collecting and storing it?

222. The Commission deliberately gave Congress and the President a large degree of flexibility in determining the overseer's authority. STUDY COMMISSION
(2) Individuals should be informed of the reasons for requesting elements of information, the techniques to be employed in collecting it, the manner in which it may be used internally, and the conditions under which it may be disclosed to third parties outside the recordkeeping organization.

(3) Information should be disseminated outside the collecting organization only with the written consent of the record subject, or upon the occurrence of a specific event, or under a more scrutinized routine use concept.\(^{223}\)

(4) Individuals should be able to see, copy, and correct personal information currently stored on them.\(^{224}\) The law will allow recordkeepers to charge this cost to the record subject unless an adverse decision affecting the status of the subject is involved.\(^{225}\) The record subject will have the right to file a position statement concerning disputed information.\(^{226}\)

REPORT, supra note 90, at 36-37. It did not recommend that broad authority be delegated to the entity. Id. at 37. Specifically, the Commission recommended:

That the President and the Congress establish an independent entity within the Federal government charged with the responsibility of performing the following functions:

(a) To monitor and evaluate the implementation of any statutes and regulations enacted pursuant to the recommendations of the Privacy Protection Study Commission, and have the authority to formally participate in any Federal administrative proceeding or process where the action being considered by another agency would have a material effect on the protection of personal privacy, either as the result of direct government action or as a result of government regulation of others.

(b) To continue to research, study, and investigate areas of privacy concern, and in particular, pursuant to the Commission’s recommendations, if directed by Congress, to supplement other governmental mechanisms through which citizens could question the propriety of information collected and used by various segments of the public and private sector.

(c) To issue interpretative rules that must be followed by Federal agencies in implementing the Privacy Act of 1974 or revisions of this Act as suggested by this Commission. These rules may deal with procedural matters as well as the determination of what information must be available to individuals or the public at large, but in no instance shall it direct or suggest that information about an individual be withheld from individuals.

(d) To advise the President and the Congress, government agencies, and, upon request, States, regarding the privacy implications of proposed Federal or State statutes or regulations.

Id.

223. A scrutinized routine use concept would require justification by the recordkeeper. This is necessary to insure that routine uses are not established in a casual manner. See note 125 supra. It is improbable that such justification will have to be provided by any organization in the private sector in the immediate future. See note 222 supra.

224. This right may be triggered by having an adverse decision made about the individual. See note 218 supra.

225. See, e.g., STUDY COMMISSION REPORT, supra note 90, at 81.

226. Id. at 204-05.
Reasonable measures must exist to assure the accuracy, completeness, and timeliness of personal information maintained by a recordkeeper.

Organizations which maintain personal information in computer-readable form must implement reasonable precautions to assure a high degree of reliability of the information and to prevent its misuse. This includes administrative (procedural and physical) and technical safeguards.

Open-ended authorizations allowing unlimited access to personal records will be replaced by authorizations allowing access for a specific, limited time and for a limited purpose.\(^{227}\)

Violators of the law will be subject to criminal and civil penalties. The strength of these requirements will also depend on the power delegated to the supervisory vehicle.\(^{228}\) If a strong privacy board is ever created, then recordkeepers in the private sector should be ready to justify their positions on the following issues:

1. whether a personal data system should continue in existence or if a proposed system should be established;
2. whether particular personal data elements should be collected for or retained in the system (relevancy);
3. whether information in a system should be utilized for a particular purpose within the set of defined purposes; and
4. whether specified information should be transferred or disclosed to certain users among the organizationally-defined set of users.

Legislation affecting the private sector will have major technical and procedural implications for organizations which store such information on computer-based systems.\(^{229}\) One immediate impact would be to change the current entity utilized in security precautions, the data file, to a lower level. Currently, computer software protections generally either apply to all of the records in a file or none of them. In the future these precautions will have to become more flexible to allow data managers to limit access to various segments or “sub-records” of the overall record of an individual. This will be necessary if the efficiencies achieved in the trend toward multipurpose information bases is to continue.

\(^{227}\) Id., at 196-97.
\(^{228}\) See note 218 supra.
For example, a single record in a computer data file of personnel can contain information pertinent to wages or salary, job performance, personal background, skills, and the like. When the record subject is to be paid, the individual preparing the payroll needs access only to the subject's name, wage or salary information, and perhaps the subject's address. No other information is relevant to this transaction. Thus, there will have to be computer software controls available to limit access in such situations.

However, technical and procedural security precautions alone cannot be equated with the concept of privacy. While information may be secure from unauthorized access by third parties, it may be inaccurate, incomplete, or out of date. There may be no means of determining to whom such information is disseminated or how it is to be used.

The total systems approach must be utilized in developing procedures. Automated and manual information practices should complement each other. For example, the information in forms which individuals complete as a condition of establishing a relationship can only be analyzed by a person for relevance to the organization's purpose and operation. Technical and procedural precautions can preserve the confidentiality of the information deemed relevant to the relationship but have no bearing on the determination of relevancy. Routing and audit data can be elements of the subject's automated record. Routing and audit data include the source of the elements of personal data, the routine uses and users, and an ongoing record of the use of the elements of personal information. The use information can be generated through a computer software routine. This will facilitate correcting inaccurate data which has been previously transferred and will provide the record subject and other auditors with an accounting of the uses of the data. A programming routine can also identify individuals on a scheduled basis whose records or elements of their records should be manually verified to insure timeliness and accuracy. A similar approach can minimize the use of incomplete information.

Much frustration will be avoided if private organizations become familiar with pending federal and state legislation and

---

230. *Id.* at 80.
231. "[I]nformation policy has not kept pace with information technology." *Id.* at 79. "Privacy may be a social issue, but its most significant technical implication will be . . . the simple requirement to develop systems, techniques and procedures for keeping information about people accurate, timely and complete." *Id.* at 82.
the report of the Privacy Protection Study Commission. Currently existing record systems, automated and nonautomated, should be reevaluated for relevancy to the organization's purpose, as should the elements and scope of subjects of those records. If record systems, elements, or individual records are not needed, they should be eliminated. A formal information practices policy should be established and promulgated.

232. A recent study of five major corporations by Purdue University's Privacy Research Center, as reported in COMPUTERWORLD, Oct. 10, 1977, at 1, indicated that most employees did not know how data in their personnel files is used. None of the corporations had written procedures for the release and handling of personal information but all indicated they had an informal policy that allowed only job-related uses of the information. All companies had designated a point of responsibility for privacy matters.

The Privacy Protection Study Commission proposed a set of information practices for personnel record systems. With a few exceptions, compliance would be voluntary at this point. See note 215 supra. First, it was recommended:

That an employer periodically and systematically examine its employment and personnel record-keeping practices, including a review of:

(a) the number and types of records it maintains on individual employees, former employees, and applicants;
(b) the items of information contained in each type of employment record it maintains;
(c) the uses made of the items of information in each type of record;
(d) the uses made of such records within the employing organization;
(e) the disclosures made of such records to parties outside the employing organization; and
(f) the extent to which individual employees, former employees, and applicants are both aware and systematically informed of the uses and disclosures that are made of information in the records kept about them.

STUDY COMMISSION REPORT, supra note 90, at 235.

Secondly, the elements of an information practices policy were identified. The Commission recommended:

That an employer articulate, communicate, and implement fair information practice policies for employment records which should include:

(a) limiting the collection of information on individual employees, former employees, and applicants to that which is relevant to specific decisions;
(b) informing employees, applicants, and former employees who maintain a continuing relationship with the employer of the uses to be made of such information;
(c) informing employees as to the types of records that are being maintained on them;
(d) adopting reasonable procedures to assure the accuracy, timeliness, and completeness of information collected, maintained, used, or disclosed about individual employees, former employees, and applicants;
(e) permitting individual employees, former employees, and applicants to see, copy, correct, or amend the records maintained about them;
(f) limiting the internal use of records maintained on individual employees, former employees, and applicants;
(g) limiting external disclosures of information in records kept on individual employees, former employees, and applicants, including disclosures made without the employee's authorization in response to specific inquiries or requests to verify information about him; and
Specific responsibilities should be assigned for implementing and managing information practices. Manual and automated procedures should be integrated. Preparation through incremental operational implementation of these administrative and technical principles will distribute the developmental cost of privacy over several years and will minimize business system disruption.

(h) providing for regular review of compliance with articulated fair information practice policies.

*Id.* at 237-38.

Lastly, with respect to the conditions for disclosure to third parties, the Commission recommended:

That each employer be considered to owe a duty of confidentiality to any individual employee, former employee, or applicant about whom it collects information; and that, therefore, no employer or consumer-reporting agency (as defined by the Fair Credit Reporting Act) which collects information about an applicant or employee on behalf of an employer should disclose, or be required to disclose, in individually identifiable form, any information about any individual applicant, employee, or former employee, without the explicit authorization of such individual, unless the disclosure would be:

(a) in response to a request to provide or verify information designated by the employer as directory information, which should not include more than:
   (i) the fact of past or present employment;
   (ii) dates of employment;
   (iii) title or position;
   (iv) wage or salary; and
   (v) location of job site;

(b) an individual's dates of attendance at work and home address in response to a request by a properly identified law enforcement authority;

(c) a voluntary disclosure to protect the legal interests of the employer when the employer believes the actions of the applicant, employee, or former employee violate the conditions of employment or otherwise threaten physical injury to the property of the employer or to the person of the employer or any of his employees;

(d) to a law enforcement authority when the employer reasonably believes that an applicant, employee, or former employee has been engaged in illegal activities;

(e) pursuant to a Federal, State, or local compulsory reporting statute or regulation;

(f) to a collective-bargaining unit pursuant to a collective-bargaining contract:

(g) to an agent or contractor of the employer, provided:
   (i) that only such information is disclosed as is necessary for such agent or contractor to perform its function for the employer;
   (ii) that the agent or contractor is prohibited from redisclosing the information; and
   (iii) that the individual is notified that such disclosure may be made and can find out if in fact it has been made;

(h) to a physician for the purpose of informing the individual of a medical problem of which he may not be aware; and

(i) in response to a lawfully issued administrative summons or judicial order, including a search warrant or subpoena.

*Id.* at 272-73.