Confidentiality of Personnel Files in the Private Sector

The Privacy Act of 1974 guarantees the confidentiality of federal agency personnel files. Currently, however, there is no similar protection of private sector personnel files. This comment examines the confidentiality of these personnel files and concludes that the Privacy Act should be extended to the private sector.

INTRODUCTION

In recent years, employers have collected, stored, and disclosed an enormous amount of personal data about their employees.[1] An increasing variety of uses for this information has evolved.[2] Under current law,[3] private sector employers may disclose part or all of this information without notice to, or consent of, the subject employee.

---

[1] *See* PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY app. 3 (EMPLOYMENT RECORDS) 9-21 (1977) [hereinafter cited as PPSC REPORT]. Congress created the Privacy Protection Study Commission to study the information practices of governmental and private organizations and to determine what protections are needed for individuals. The Commission has found that "the workplace has become a repository of personal information." *Id.* at 10. This report describes the numerous types of information gathered, kept, and used by employers. These include interviewer evaluations, medical records, skill tests, payroll information, personal information, insurance claims, security, performance evaluations, and promotion tables. *Id.* at 9-21. *See also* A. MILLER, THE ASSAULT ON PRIVACY 205-06 (1971) (noting a general increase in information-gathering throughout society).

[2] *See, e.g.*, Note, *Privacy of Information in Florida Public Employee Personnel Files*, 27 U. FLA. L. REV. 481 (1975). Florida public sector employers maintain information ranging from very personal to routine. *Id.* at 501. Private employers use personnel information "in deciding whether to hire, fire, place, transfer, promote, demote, train, discipline, and provide full or partial benefits." PPSC REPORT, *supra* note 1, app. 3 at 15. These uses, which are fundamental to the employment relationship, make "interorganizational exchange of information on people particularly significant." Berg & Salvate, *Record-Keeping and Corporate Employees*, in ON RECORD: FILES AND DOSSIERS IN AMERICAN LIFE 177, 186-88, 192 (S. Wheeler ed. 1969).

[3] *See* notes 7-9 and accompanying text *infra*.

Currently, three legal doctrines are most relevant to the confidentiality of personnel files. These are breach of confidential relationship,[4] defamation,[5] and the common law right of privacy.[6] However, these three doctrines fail to adequately protect the rights of private sector employees.[7] The control and use of per-

---

[4] Communication between people standing in a confidential relation to each other is privileged under statutory and common law. The law does not allow the communication to be divulged without the subject's consent. Examples of confidential relationships include the attorney-client relationship and the physician-patient relationship. However, this doctrine does not yet apply to employment relationships. Mironi, *The Confidentiality of Personnel Records: A Legal and Ethical View,* 25 LAB. L.J. 270, 279 (1974) [hereinafter cited as Mironi].

[5] The tort of defamation protects the individual's interest in his reputation. *Id.* at 283. *See, e.g.,* Tumbarella v. Kroger Co., 85 Mich. App. 482, 271 N.W.2d 284 (1978), in which the court held a supermarket chain liable for defamation because it told all its supervisors that it had fired a cashier for theft. The court held that this disclosure was too broad. Although defamation covers employees, a qualified privilege usually shields employers from liability. Mironi, *supra* note 4, at 283. Employers enjoy this privilege when they disclose personnel information in good faith to a person having a job-related interest in it, such as a prospective employer. *Id.* at 284.

[6] The concept of privacy has no clear, universally accepted definition. Comment, *Privacy and the Freedom of Information Act,* 27 ADM. L. REV. 275, 275-76 (1975). For purposes of this comment, privacy is: "not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves." Fried, *Privacy,* 77 YALE L.J. 475, 482 (1968). Fried suggests that law is important as a potential protector of individual privacy rights, since it may give individuals this control. *Id.* at 493. Another commentator describes privacy as an aspect of human dignity, asserting that the interest involved is that of an "inviolate personality." Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser,* 39 N.Y.U. L. REV. 962, 1001 (1964).

Dean Prosser described four distinct types of privacy invasions: appropriation of another's name or likeness for personal advantage, intrusion upon one's physical solitude or seclusion, public disclosure of private facts, and publicity that places a person in a false light in the public eye. W. PROSSER, HANDBOOK OF THE LAW OF TORTS § 117 (4th ed. 1971). Only the third category—public disclosure of private facts—is relevant to this comment. There are three elements to a tort action for public disclosure: Disclosure must be public (to a large group, not just to an individual), the information must be private (not matters of public record), and the matter disclosed must be one that would be offensive to a reasonable person. *Id.* These requirements seriously limit the tort's applicability to the employment situation. Mironi, *supra* note 4, at 282.

[7] For further discussion of these doctrines and their limited applicability to the problem of personnel information usage, see Mironi, *supra* note 4, at 278-87. *See also* A. MILLER, *supra* note 1, at 187-90.

sonal employee information is therefore governed by little more than the will of the individual employer,[8] and possibly society's general notions of "fair play."[9]

This comment examines the confidentiality of personnel files in the private sector, presents a framework for its protection, and proposes an extension of existing law. The first section describes the Privacy Act of 1974,[10] which protects employee privacy rights, but only in federal agencies.[11] The second section analyzes the similarities and differences between public and private sector employment relationships. The final section proposes the extension of the Privacy Act's protections to the private sector. This comment concludes that the minimal protection that societal influence affords to private sector employees is not adequate, and that these employees need greater *legal* protection.

---

[8] In its study of privacy protection within the private sector employment relationship, the Privacy Protection Study Commission found that employers have sole discretion over maintaining the confidentiality of personnel files, and that this discretion may be abused at any time with no duty owed to an individual employee. PPSC REPORT, *supra* note 1, at 269.

[9] *See* Berg & Salvate, *supra* note 2, at 196, 198-99. "The essential protection against abuses borrows heavily from whatever influence more general norms of fair play have in a democratic society." *Id.* at 198-99. The authors suggest that businessmen both know of community norms and desire to maintain good reputations. *Id.*

[10] 5 U.S.C. § 552a (1977). *See also* notes 15-33 and accompanying text *infra*.

[11] California adopted a similar statute, the Information Practices Act of 1977, CAL. CIV. CODE §§ 1798.1-.76 (West Cum. Supp. 1981), to regulate the practices of state agencies. *See* Note, *California's Privacy Act: Controlling Government's Use of Information?*, 32 STAN. L. REV. 1001 (1980). Many of the California Act's provisions are similar to those of the Federal Privacy Act, and some of the language is identical. *Id.* at 1004 n.6. Moreover, California's Act also does not apply to the private sector.

Several other states regulate the informational privacy practices of state agencies: Connecticut, CONN. GEN. STAT. ANN. §§ 4-190 to -197 (West Cum. Supp. 1981); Indiana, IND. CODE §§ 4-1-6-1 to -9 (Cum. Supp. 1981); Massachusetts, MASS. GEN. LAWS ANN. ch. 66A, §§ 1-3, ch. 214, § 3B (West Cum. Supp. 1981); Minnesota, MINN. STAT. ANN. §§ 15.1611-.1698 (West Cum. Supp. 1981); Ohio, OHIO REV. CODE ANN. §§ 1347.01-.99 (Page 1979 & Cum. Supp. 1980); Utah, UTAH CODE ANN. §§ 63-2-59 to -89 (1978 & Cum. Supp. 1981); Virginia VA. CODE §§ 2.1-377 to -386 (1979 & Cum. Supp. 1981). These statutes are discussed in R. SMITH & K. SNYDER, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS 14-16 (1977).

I. THE PRIVACY ACT OF 1974

Although the recognition and application of the common law right of privacy have expanded steadily,[12] this common law remedy has not been sufficient to protect the privacy rights of public and private sector employees.[13] Therefore, the most promising alternative for developing greater legal protection for these rights is a statutory right of privacy.[14] The Privacy Act of 1974[15] is a prime example of this type of protection. The Privacy Act greatly expands the common law right of privacy by codifying some basic privacy protections.[16] In doing so, the Act protects

---

[12] For an extensive discussion of the development of the privacy right, see Kailer, *The Release of Private Information Under Open Records Laws,* 55 TEXAS L. REV. 911 (1977). *See also* A. WESTIN, PRIVACY & FREEDOM 346-64 (1967).

[13] *See* notes 6-7 *supra.*

[14] A statutory right of privacy for more general reasons exists in many states. *See, e.g.,* California, CAL. CIV. CODE § 3344 (West Cum. Supp. 1981) (preventing misappropriation of a person's name or likeness); New York, N.Y. CIV. RIGHTS LAW §§ 50-51 (McKinney 1976 & Cum. Supp. 1979) (preventing unauthorized use of a person's name, portrait, or likeness). *See also* Delaware, DEL. CODE ANN. tit. 11, § 1335 (1979) (establishing a misdemeanor for violation of right of privacy); Georgia, GA. CODE ANN. § 26-3001 (1978) (rendering invasion of privacy illegal); Maine, ME. REV. STAT. ANN. tit. 17-A, § 511 (Cum. Supp. 1981) (limiting surveillance); Massachusetts, MASS. GEN. LAWS ANN. ch. 214, § 1B (West Cum. Supp. 1981) (proscribing interference with privacy); Utah, UTAH CODE ANN. § 76-9-401 (1978) (prohibiting "offenses against privacy"). *See generally* R. SMITH & K. SNYDER, *supra* note 11, at 28-30.

Four states have adopted statutes specifically relating to employment records: California, CAL. LAB. CODE § 1198.5 (West Cum. Supp. 1981); Maine, ME. REV. STAT. ANN. tit. 26, § 631 (Cum. Supp. 1981); Maryland, MD. CODE ANN. art. 100, § 95A (1979); North Carolina, N.C. GEN. STAT. § 126-22 (1981). *See* R. SMITH & K. SNYDER, *supra* note 11, at 17. For further discussion of the California, Maine, and North Carolina statutes, see note 55 *infra.*

[15] 5 U.S.C. § 552a (1977). For a general discussion of the Act's major provisions, see Comment, *Let Industry Beware: A Survey of Privacy Legislation and its Potential Impact on Business,* 11 TULSA L.J. 68 (1975). Of particular interest here are the Act's rules governing disclosure of information. The Act prohibits federal agencies from disclosing personnel record information without the present or prior written consent of the particular employee, unless one of eleven exceptions applies. For a brief description of these exceptions, see note 20 *infra.* For a discussion of why a federal statutory remedy similar to the Privacy Act would be the best alternative, see notes 66-69 and accompanying text *infra.*

[16] Comment, *Access to Information? Exemptions from Disclosure under the Freedom of Information Act and the Privacy Act of 1974,* 13 WILLAMETTE L.J. 135 (1976), discusses four basic privacy principles that are embodied in the

the confidentiality[17] of federal agency personnel files.

The Act sets forth conditions that an agency must satisfy to disclose information about an employee.[18] The major prerequisite to disclosure is obtaining the written consent of the employee.[19] Congress effectively has given the employee the "final say" about disclosure of personal data, at least when none of eleven specified exceptions applies.[20] When an exception applies,

---

Privacy Act:

> (1) Individuals should have access to information about themselves in record-keeping systems. And there should be some procedure for individuals to find out how this information is being used.
>
> (2) There should be some way for an individual to correct or amend an [inaccurate] record.
>
> (3) An individual should be able to prevent information from being improperly disclosed or used for other than authorized purposes without his or her consent, unless required by law.
>
> (4) The custodian [of] data files containing sensitive information should take reasonable precautions to be sure that the data are reliable and not misused.

Id. at 138 n.26 (citing an advertisement placed by International Business Machines, NEWSWEEK, July 8, 1974, at 48).

Congress passed the Privacy Act of 1974 "to promote governmental respect for the privacy of citizens . . ." by regulating agencies' "collection, management, use, and disclosure of personal information about individuals." S. REP. No. 93-1183, 93d Cong., 2d Sess. 1, *reprinted in* [1974] U.S. CODE CONG. & AD. NEWS 6916, 6916 [hereinafter cited as SENATE REPORT].

[17] As used in this comment, "confidentiality" refers to the disclosure of information, while "right of privacy" focuses on the employers' collection of information. However, Fried's definition of privacy as "control," *see* note 6 *supra*, blurs this distinction, since an individual's true right of privacy may involve control over all phases of employer data usage, including collection, storage, and disclosure. Thus, this comment will use the all-inclusive phrase "right of privacy" in lieu of "confidentiality."

[18] *See* note 15 *supra*. Actually, the Privacy Act is not limited in scope to the protection of employees' rights, since it covers *any* individual who is the subject of an agency record. 5 U.S.C. § 552a(a)(4) (1977). By definition, this includes employees. Also, the Act's definition of "record" lists "employment history" as one type of information to be protected. *Id.*

[19] 5 U.S.C. § 552a(b) (1977).

[20] These exceptions include: Disclosure to agency officers and employees who "need" the information to perform their jobs, *id.* § 552a(b)(1); where required by the Freedom of Information Act, *id.* §§ 552, 552a(b)(2); for a "routine use," *id.* § 552a(b)(3), that is, one that is compatible with the purpose for which the information was gathered, *id.* § 552a(a)(7); to the Census Bureau, *id.* § 552a(b)(4); for statistical use only, *id.* § 552a(b)(5); to the National Archives, *id.* § 552a(b)(6); for law enforcement purposes, *id.* § 552a(b)(7); where circumstances affect the health or safety of the individual, *id.* § 552a(b)(8); to Con-

the Act suspends the employee consent requirement, giving the agency greater control over use of employee information.[21]

The Privacy Act provides for both criminal penalties[22] and civil remedies,[23] including damages[24] and injunctive relief.[25] The Act empowers individuals who are adversely affected by the agency's noncompliance to bring a civil suit against it in federal district court.[26] For example, in *Parks v. United States Internal Revenue Service*,[27] the circuit court allowed individual Internal Revenue Service employees to bring an action against the defendant agency for damages resulting from its unwarranted disclosure of their personnel files.[28] However, the court refused to issue an injunction in this situation because it did not fall within the Act's limited grounds for injunctive relief.[29]

---

gress, *id.* § 552a(b)(9); to the General Accounting Office, *id.* § 552a(b)(10); or pursuant to court order, *id.* § 552a(b)(11).

[21] *Id.* § 552a(b) (1977).

[22] *Id.* § 552a(i). The Act imposes criminal sanctions for willful and knowing violations of the Act, including willful disclosure of protected information by an agency officer or employee.

[23] *Id.* § 552a(g).

[24] *Id.* § 552a(g)(4). The Act allows recovery of actual damages only for intentional or willful agency violations.

[25] *Id.* § 552a(g)(2)(A), (3)(A). The court may order the agency to amend the individual's record pursuant to his request, and to release improperly withheld records to the individual.

[26] *Id.* § 552a(g)(1)(A)-(D). The Act enables an individual to bring a civil action whenever an agency refuses to amend his record, *id.* § 552a(g)(1)(A), refuses to allow the individual access to his record, *id.* § 552a(g)(1)(B), fails to maintain a record with sufficient accuracy to assure fairness, *id.* § 552a(g)(1)(C), or violates any other provision in a way that has an adverse effect on the individual. *Id.* § 552a(g)(1)(D).

[27] 618 F.2d 677 (10th Cir. 1980).

[28] After the plaintiff employees had failed to pledge to purchase government bonds, the defendant agency used its personnel files to compile a list of recalcitrants in order to subject them to a persuasive telephone campaign. *Id.* at 679. The employees claimed that they suffered psychological harm as a result of the disclosure. *Id.* at 680. The court held that damages were warranted. Since the "willful or intentional" standard set forth in 5 U.S.C. § 552a(g)(4) (1977) is really only a "medium standard," it is sufficient to show conduct slightly greater than gross negligence on the part of the employing agency to establish a violation. Parks v. IRS, 618 F.2d 677, 683 (10th Cir. 1980).

[29] The court held that the Privacy Act provides for an injunction only in two cases: To order an amendment of an individual's record, and to order an agency to produce records improperly withheld from an individual. Parks v. IRS, 618 F.2d 677, 684 (10th Cir. 1980). *See also* note 25 *supra*.

In an earlier case, *Zeller v. United States*,[30] a New York district court similarly interpreted the Privacy Act's provisions for civil remedies to allow the plaintiff to sue the defendant Interstate Commerce Commission.[31] The court held that the plaintiff stated a claim for damages resulting from the defendant's issuance of a press release about the plaintiff.[32] This court also refused to issue an injunction because of limitations on employees' rights of access to and amendment of agency records.[33]

II. An Analytical Framework for Protection in the Public and Private Sectors

Extension of the Privacy Act to private employers first requires a comparison of personnel file use in federal agencies and in the private sector. When Congress finds similarities, it should extend pertinent provisions of the Privacy Act wholesale to the private sector. Conversely, when differences appear, Congress must weigh conflicting factors before it may enact a significant and balanced law. This weighing process must consider the private sector's particular needs, interests, and concerns. Ultimately, this process must balance employers' needs and concerns[34] against the potentially damaging impact of information

---

[30] 467 F. Supp. 487 (E.D.N.Y. 1979).

[31] Following an accident involving a bus chartered by the plaintiff, a bus-tour broker, the Interstate Commerce Commission successfully sued to enjoin him from brokering without a license. *Id.* at 490-91. A Commission employee thereafter disclosed a press release about the suit to two other brokers in order to show them the adverse consequences of not being licensed. *Id.* at 492.

[32] *Id.* at 503. The plaintiff stated a claim for actual damages under the Privacy Act since the disclosure had been made without his consent and the agency had not previously published this use as a "routine" one. *Id.* The court further held that the willfulness of the disclosure was a question of fact. *Id.*

[33] *Id.* at 500-03. However, the *Zeller* court refused to grant injunctive relief for reasons different from those given in *Parks*. The court denied the plaintiff's request for access to his records for two reasons. First, the records had been compiled in reasonable anticipation of a civil action or proceeding. *See* 5 U.S.C. § 552a(d)(5) (1977). Second, the court denied the request for an injunction ordering amendment of inaccurate records, since accuracy depends upon the manner in which the agency was using the record to make decisions about the individual. Zeller v. United States, 467 F. Supp. 487, 502 (E.D.N.Y. 1979). Thus, if the press release was accurate when made, later amendment was not required. *Id.* at 502-03. The court's narrow interpretation of the Act is unduly restrictive, since it would permit the agency to maintain inaccurate information in the individual's file.

[34] *See* notes 36-38 and accompanying text *infra*.

abuses on employees.[35]

A. Similarities in the Public and Private Sectors

1. Employers' Need for Information

In both the federal and private employment sectors, employers have a legitimate need[36] to acquire and control information about their employees.[37] This need conflicts with employee privacy rights. To resolve the conflict, the subject employee should be able to curtail the disclosure of certain personal information. Congress adopted this compromise in the Privacy Act, and it may be the fairest and most effective means of protecting these conflicting interests.[38]

2. Disclosure

Both federal and private employers face the disclosure problems of *who* may see the information and *how much* they may see.[39] Both federal and private employers disclose personnel file information externally as well as internally. For example, federal agency employers disclose personnel information not

---

[35] *See, e.g.,* Peller v. Retail Credit Co., 359 F. Supp. 1235 (N.D. Ga. 1973), *aff'd mem.,* 505 F.2d 733 (5th Cir. 1974), in which an employee lost his job upon disclosure of adverse polygraph results by a former prospective employer. In applying for an earlier job, the plaintiff voluntarily took a polygraph test. The results were adverse and he was not hired. A different employer later hired him, but it fired him after seeing the polygraph results, which had been disclosed to the defendant company and placed in its Consumer Credit Report. Since the court rejected the plaintiff's claim under the Fair Credit Reporting Act, 15 U.S.C. §§ 1681a-t (Supp. III 1979), the plaintiff was left without a legal remedy or a job.

[36] *See* PPSC REPORT, *supra* note 1, at 225-26. A large organization needs to maintain specialized records about its employees. This need arises not only from the employer's recruitment, selection, and job placement processes, but also from its efforts to maintain "industrial relations, benefit programs, occupational medicine and safety, and compliance with various Federal and State government requirements." *Id.* at 225. Complex bookkeeping requirements and employees' skill specialization enhance the need. *Id.* at 226.

[37] *See* notes 8-9 *supra.*

[38] *See* text accompanying note 79 *infra.*

[39] This second similarity arises in part from the employers' needs for information. This comment distinguishes the term "disclosure" from "need" in that the latter gives rise to internal disclosure. Because employers have a need to acquire and control personnel information, they collect, store, and disclose it for various internal uses. *See* note 36 *supra.*

only to individuals and departments within the agency, but also to individuals and organizations outside the agency.[40] Similarly, private sector employers disclose personnel information to persons within the company[41] and to outside entities such as labor unions[42] and other companies.[43]

3. Enforcement

A further common issue facing federal and private employers concerns the enforcement of privacy rights. Pertinent questions include determining what types of enforcement actions are available, and what parties have standing to bring them.

Employees have relatively low awareness of record-keeping issues.[44] Because of this, self-initiated remedies are unlikely to provide adequate protection of employees' privacy rights.[45] In-

---

[40] External disclosure is made to other agencies and other branches of government. In justifying the broad coverage of the Privacy Act of 1974, Congress cited "the haphazard patterns of information swapping *among* government agencies, the diversity of confidentiality rules and the unevenness of their application *within and among* agencies." SENATE REPORT, *supra* note 16, at 14, *reprinted in* [1974] U.S. CODE CONG. & AD. NEWS 6916, 6929 (emphasis added).

[41] *E.g.*, disclosures within the company are made to supervisors and to employees in other departments.

[42] In the federal sector, the Privacy Act restricts labor unions' access to information about member employees. For example, in Local 2047, American Fed'n of Gov't Employees v. Defense Gen. Supply Center, 423 F. Supp. 481 (E.D. Va. 1976), *aff'd*, 573 F.2d 184 (4th Cir. 1978), the court held that the plaintiff union could not acquire certain personnel information that the defendant employer held without first obtaining written consent from the subject employees. The union had sought information about its members pursuant to a collective bargaining agreement between the union and the agency that permitted disclosure of personnel information without employee consent. 423 F. Supp. at 482. The information sought went beyond the mere identification of employees, a use that had been published as a "routine use" by the agency. It included names of employees suspected of abusing sick leave, names of employees who were continually tardy, and copies of warning letters and proposed disciplinary actions. *Id.* at 482-83 n.1. The court ruled that the Privacy Act controlled and overrode the earlier collective bargaining agreement. *Id.* at 485-86. Since the union's disclosure request fell within none of the Act's exceptions, it was denied absent prior consent. *Id.* at 486 n.11. *Accord*, Detroit Edison Co. v. NLRB, 440 U.S. 301 (1979), *discussed in* note 88 *infra*.

[43] These other companies commonly include prospective employers.

[44] Baker, *Record Privacy as a Marginal Problem: The Limits of Consciousness and Concern*, 4 COLUM. HUMAN RIGHTS L. REV. 89, 92 (1972).

[45] *Id.* at 98.

stead, employees need an external force to help safeguard their rights.[46]

4. Employees' Vulnerability

The fourth similarity between federal and private sector employers is employees' vulnerability to several possible employer information abuses.[47] First, employees realistically cannot afford to deny information to either prospective or current employers.[48] This inherent employee disadvantage raises questions about the validity of *any* employee waiver of privacy rights.[49] If waiver is

---

[46] *Id.* at 100. Baker suggests that this external force could take the form of policy requirements. These requirements would place respect for privacy in the organization's best interest, or would at least build respect into the record process itself. *Id.*

[47] One author describes the gravity of the situation:

> Employers — whether governmental or private — exercise the most continuous and direct authority over people. . . . And, increasingly, the records . . . are used not only to make personnel decisions but also to determine pension rights, health-insurance claims and coverages, antidiscrimination conflicts, . . . and a host of other major aspects of individual life now administered at the workplace.

Westin, *Privacy and Personnel Records: A Look at Employee Attitudes*, 4 CIV. LIB. REV. 28, 34 (Jan.-Feb. 1978).

[48] For a discussion of the problems posed by the employee's subservient position, see A. WESTIN, *supra* note 12, at 375. When the employer requires scientific tests either for hiring or promotion, for example, the employee's refusal to consent could cost him a potential job, raise, or promotion. *Id.* Moreover, as of December, 1981, 9,500,000 people, or 8.9% of the total United States labor force of 106,700,000, were unemployed. BUREAU OF LABOR STATISTICS, U.S. DEP'T OF LABOR, EMPLOYMENT AND EARNINGS 4 (Jan. 1982).

[49] Under the Privacy Act, 5 U.S.C. § 552a(b) (1977), when an employee consents to disclosure of information, he effectively waives his right of privacy over that specific information. "Waiver" as used in the text differs from the Privacy Act consent requirement, in that "waiver" suggests a blanket relinquishment of all of one's privacy rights under the Privacy Act.

A. MILLER, *supra* note 1, calls employee consent and waiver "placebos," *id.* at 185-87, and cautions against placing too much value on them, since they are probably given involuntarily. In a situation such as an employment relationship, where the employee is subject to the employer's authority, Professor Miller says that the supposition that the information could be given voluntarily ignores reality. *Id.* at 185-86. Instead, he suggests that a combination of many complex factors, including the surrounding circumstances and the employee's personality, could eclipse the employee's freedom to choose. *Id.*

See also A. WESTIN, *supra* note 12. In questioning the validity of waiver, Westin focuses on the inequality of bargaining positions. He suggests that con-

permissible, then a subsidiary issue is whether the employer can "require" waiver either during or after the application process.[50] These issues are common to the public and private sectors. While the Privacy Act arguably proscribes waiver of its protections,[51] it is not applicable to the private sector. Thus, the waiver questions remain unanswered.[52]

Second, private sector employees are vulnerable when they have little or no access to their own files. As a result, they cannot verify the accuracy of information maintained in their files.[53] Before the Privacy Act, federal agency employees lacked access to their files. However, the Act remedies this situation for federal employees.[54] Only three states provide similar protections for private sector employees.[55]

---

sent or waiver be reviewed carefully in each case to determine how free the employee's choice actually was. He points out that in certain special areas of American law, individuals are not allowed to waive their rights where bargaining positions are unequal. For example, "yellow dog" contracts, conditioning employment on promises not to join unions, have been outlawed. *Id.* at 375.

[50] If the employer *can* "require" waiver, then privacy protections governing the employment relationship are a farce. For ways in which an employer may "require" waiver, see note 49 *supra* and notes 98-100 *infra*.

[51] *See* notes 94-96 and accompanying text *infra*.

[52] *See* notes 92-100 and accompanying text *infra*.

[53] For a discussion of the negative effects of maintaining inaccurate, incomplete, or biased information in an individual's personnel file, see M. BAKER & A. WESTIN, DATABANKS IN A FREE SOCIETY 356-57 (1972). The authors state that personnel information is an important factor in various decisions made by both government and private organizations. *Id.* Examples of decisions possibly affected include promotions, assignments to jobs, and the provision of benefits to selected individuals. *Id.*

[54] *See* notes 102-103 and accompanying text *infra*.

[55] *See* R. SMITH & K. SNYDER, *supra* note 11, at 17. The three states are California, Maine, and North Carolina. CAL. LAB. CODE § 1198.5 (West Cum. Supp. 1981) requires private employers to permit employees to inspect all records and personnel files concerning them at reasonable times and at reasonable intervals, as determined by the Labor Commissioner, upon the employee's request. However, the statute does not apply to records used in criminal investigations nor to letters of reference. Moreover, the statute provides no defined penalties for violation.

In Maine, the employer must provide an opportunity for current or former employees to review their personnel files upon request. "File" is defined to include information concerning the employee's compensation, benefits, character, work habits, and credit, as well as formal and informal evaluations. ME. REV. STAT. ANN. tit. 26, § 631 (Cum. Supp. 1981).

In North Carolina, state and local government employment records containing information regarding the employee's name, age, dates of employment, po-

Employee vulnerability also arises because employers presently need not notify employees before using their personal information. Since the employer is not required to inform the employee about disclosure even *after* the fact, the employee often does not know that the information has been disclosed.[56] This absence of notice represents a serious affront to private sector employee privacy rights.[57]

Just as it compels agencies to grant file access to their employees, where little or none had existed previously, the Privacy Act fills a similar void in the notice area.[58] Again, no comparable safeguard protects private sector employees.[59]

B. Differences Between the Public and Private Sectors

Congress passed the Privacy Act of 1974 in part to address employee privacy problems in federal agencies.[60] However, Congress has not extended the Privacy Act provisions to the private sector, despite various efforts to do so.[61] The differences between

---

sition title, salary, and most recent promotion and demotion, are open to *any* person. All other information is confidential. N.C. GEN. STAT. § 126-22 (1981). Overall, however, the wide-open disclosure of age, salary, and job status information seems contrary to privacy rights; at best, this provides only limited protection for the employee. Another provision enables the employee to add data or request removal of inaccurate or misleading data in the file. *Id.*

[56] For a general discussion of the disclosure practices of private sector employers, see PPSC REPORT, *supra* note 1, app. 3 at 87-95. Whether they are merely "verifying" information for, or are "volunteering" it to, third parties, employers need not notify the employees of their disclosures. *Id.* at 88. The Report describes specific situations in which employers disclose information without notifying the employees. Reporting wage and salary information to the Internal Revenue Service is one example, *id.* at 90, and disclosing files to law enforcement officers is another. *Id.* at 93.

To remedy this situation, the Commission recommends "[t]hat an employer clearly inform all its applicants upon request, and all employees automatically, of the types of disclosures it may make of information in the records it maintains on them, . . . and of its procedures for involving the individual in particular disclosures." *Id.* at 96.

[57] *See* Bloustein's definition of privacy, *supra* note 6.

[58] *See* notes 107-108 and accompanying text *infra.*

[59] Even where states have provided some privacy protection for employees, as in the access requirements of California, Maine, and North Carolina, no notice requirements exist. *See* note 55 *supra.*

[60] *See* notes 12-33 and accompanying text *supra.*

[61] H.R. 1984, 94th Cong., 1st Sess. (1975). *See also* Metz, *Federal Leadership in Privacy Protection,* 61 A.B.A. J. 825 (1975) (noting that 85 privacy bills

the two sectors indicate some of the obstacles to the wholesale extension of the Privacy Act to the private sector.

1. Employers' Cost of Compliance

The first difference between the public and private sectors is the cost of employer compliance with privacy regulations. The cost of compliance for federal agency employers is not an issue, since the government is regulating itself.[62] In contrast, private sector employers have justifiable concerns about the potentially substantial cost of compliance.[63] The Privacy Protection Study Commission has found that requiring an employer to change its manner of maintaining and using records "can increase its cost of operation."[64] The employer would likely pass on the increased costs to consumers or reduce production or services.[65]

This concern about compliance costs, shared by state and local governments,[66] underscores the need for federal legislation[67] to regulate the information practices of private sector employers, especially those who operate in more than one state. A preemptory federal act would preclude the imposition of conflicting requirements on private sector organizations,[68] thereby minimizing compliance costs.[69]

---

were introduced in 36 state legislatures during the first half of 1975); Comment, *supra* note 15.

[62] Nevertheless, taxpayers pay the federal agencies' cost of compliance. By analogy, consumers would have to pay for compliance in the private sector.

[63] *See* Kovach, *A Retrospective Look at the Privacy and Freedom of Information Acts*, 27 LAB. L.J. 548, 557 (1976). *See also* Comment, *supra* note 15, at 80-81 (citing projected compliance costs calculated in Goldstein & Nolan, *Personal Privacy Versus the Corporate Computer*, HARV. BUS. REV., Mar.-Apr. 1975, at 62). Based on five model data systems, including personnel and credit, Goldstein and Nolan estimate that initial conversion costs would range from $142,000 to $1,416,000 and that annual privacy costs would range from $40,000 to $20,453,000 per system. Comment, *supra* note 15, at 81. For example, extension of the Act would have an impact on routine business transactions, the convenience of customers, and the price of commodities. *Id.* at 76 n.47.

[64] PPSC REPORT, *supra* note 1, at 27.

[65] *Id.*

[66] *See* Kovach, *supra* note 63, at 557.

[67] *See* Comment, *supra* note 15, at 81-82. The commentator asserts that national coherence is needed in privacy legislation, and that the alternative of numerous state acts would place unreasonable burdens on multistate corporations. *Id.*

[68] *Id.*

[69] A preemptory federal act also would preclude industries in unregulated

2. Capacity for Excessive Surveillance

The second difference between federal agencies and private sector employers concerns overzealous surveillance and information-gathering practices. These practices provided an impetus for passage of the Privacy Act.[70] Congress passed the Act largely as a response to misuse of information about private citizens during the Nixon Administration.[71] The problem of overzealous surveillance and information-gathering is not as great among private sector employers since they generally do not possess the substantial resources and authority that federal agencies do.[72] Hence, a major reason for the enactment of the Privacy Act of 1974 is simply not as pressing in the private sector. However, abuses may and do still occur.[73]

III. Extending the Privacy Act of 1974

Congress created the Privacy Protection Study Commission[74] to study the feasibility of extending the Privacy Act to the private sector.[75] In 1975, Representatives Barry Goldwater, Jr. and Edward Koch unsuccessfully proposed such an extension.[76]

---

states from gaining unfair competitive advantages. *See id.* at 83.

[70] Senate Report, *supra* note 16.

[71] *See* Kovach, *supra* note 63, at 557.

[72] However, the effect of overzealous surveillance and information-gathering in the private sector is equally damaging to the individual. *See* PPSC Report, *supra* note 1, app. 3 at 14, which briefly describes the manner in which employers maintain security records.

[73] *See* Craver, *The Inquisitorial Process in Private Employment,* 63 Cornell L. Rev. 1 (1977). After citing the problems of internal employee crime and increased on-the-job alcohol and drug use, Professor Craver states that

> [i]n response to these problems, employers have significantly expanded utilization of such security techniques as employee interrogation, lie detector tests, searches of workers and their effects, and electronic surveillance of in-plant activities. These efforts have inevitably encroached upon the privacy of employees, who find themselves increasingly subject to Orwellian regimens in their places of employment.

Id. at 2.

[74] Pub. L. 93-579, § 5, 88 Stat. 1897.

[75] Pub. L. 93-579, § 5(b), 88 Stat. 1897.

[76] H.R. 1984, 94th Cong., 1st Sess. § 2(b) (1975). For an analysis of the unsuccessful bill, see Comment, *supra* note 15, at 76-81. The main provision of interest was § 2(b), No. 9: "There should be a clearly prescribed procedure for an individual to prevent personal information collected for one purpose from

When Congress created the Privacy Protection Study Commission, the business community became very apprehensive, primarily about the cost of the Act's possible extension.[77] Therefore, to be successful, any proposals for extension must "strike the necessary balance between protecting the legitimate concerns of individuals and the equally legitimate concerns of business in protecting their right to profitably remain in operation."[78] This balance should guide the extension of the Privacy Act of 1974 to the private sector—or, at least, in applying some of its basic principles[79] when appropriate.[80]

The wide range of persons and entities able to obtain information collected by federal agency employers[81] prompted Congress to limit unauthorized disclosure in the Privacy Act.[82] The Act protects a federal agency employee's privacy rights in part by requiring his written consent before his employer discloses information about him.[83] The Act exempts the employer from this requirement when one of eleven statutory exceptions applies,[84]

---

being used for another purpose without his consent." However, the bill apparently was too broad. It tried to do more than protect privacy, by also proposing to strengthen the individual's position in dealing with large organizations. Comment, *supra* note 15, at 77. The commentator asserts that this proposed broad approach would create several problems. *Id.* at 78-79. One would be the difficulty of developing adequate definitions for terms such as "organizations" and "proper purpose." Compliance would also pose a problem. *Id.* at 78.

[77] The cost of complying with the Act's provisions regarding record-keeping would probably be substantial. *See* notes 63-69 and accompanying text *supra.*

[78] Comment, *supra* note 15, at 83. For a discussion of the weaknesses of H.R. 1984, see note 76 *supra.*

[79] *See* note 16 *supra.*

[80] *See, e.g.,* text accompanying notes 34-38, 53-59 *supra. But see* PPSC REPORT, *supra* note 1, app. 3 at 32-34. The Commission makes many specific recommendations relating to employment records, but proposes that employers adopt most of them voluntarily. *Id.* Although some employers (such as International Business Machines, note 16 *supra*) have heeded the Commission's call, *see* Belair, *Employee Rights to Privacy,* PROCEEDINGS OF NEW YORK UNIVERSITY THIRTY-THIRD ANNUAL NATIONAL CONFERENCE ON LABOR 3, 12 (R. Adelman ed. 1981), many have not. This is inequitable for employees of the latter organizations. Moreover, even if employers do adopt the Commission's recommendations, voluntary adoption will not effectively protect employees' privacy rights, since there will be no enforcement from outside of the companies.

[81] *See* note 40 and accompanying text *supra.*

[82] *See* note 20 and accompanying text *supra.*

[83] 5 U.S.C. § 552a(b) (1977).

[84] *See* notes 20-21 and accompanying text *supra.*

thereby striking a balance.[85]

Although no similar limitation on disclosure currently governs the private sector, the United States Supreme Court has laid the groundwork for future extension of the consent requirement to the private sector.[86] Since analogous disclosure problems confront the private sector employer and employee, and since they have comparable rights and needs, Congress should extend a similar consent requirement with attendant exceptions to the private sector.

A further disclosure issue that confronts both federal and private employers is the possible scope of the privacy protection to be afforded to employees. For example, a statute could restrict the disclosure of information involving a broad range of subjects, such as lie detector tests, medical records, phone and social security numbers, and unsubstantiated opinions about the employee.[87] A more narrow regulation would protect only the most sensitive items, such as the employee's psychological records or information about his sex life, against indiscriminate employer

---

[85] *See* text accompanying notes 63-69, 79-82 *supra*.

[86] The Court articulated a principle similar to the consent requirement of the Privacy Act in a private sector dispute in Detroit Edison Co. v. NLRB, 440 U.S. 301 (1979). However, the Court applied it in a different manner. The Court held that the plaintiff organization *was not required* to disclose information regarding its psychological aptitude testing program without first obtaining written consent from the individual employees, even though the request had been made by the employees' union for use in collective bargaining. *Id.* at 317. The information consisted of actual question-and-answer sheets and of test scores linked with employees' names. The Court ruled by implication that the privacy rights of the employees outweighed any possible impairment of the union's function as bargaining representative. *Id.*

While this decision appears to protect private sector employees' privacy rights, the Court actually left the question open. The Court did not say that the employer *must* withhold information where unauthorized; rather, it merely implied that the employer *may* do so if it wishes. *Id.* at 317-20. This is in direct contrast to the Privacy Act, which *requires* prior consent. 5 U.S.C. § 552a(b) (1977).

[87] *See* PPSC REPORT, *supra* note 1, app. 3 at 87-95. The Commission defines "directory information" as that which identifies the existence of an employment relationship (including the dates of hire, and termination, if applicable), the title or position held by the employee, and wage and salary data, although these latter are disclosed less often than the other types of directory information. *Id.* at 87. The Commission implicitly suggests that any privacy statute should exempt directory information from its requirement of prior authorization, since many employers either disclose or verify much of this information to third parties automatically. *Id.* at 87-88.

disclosure.

Although the Privacy Act does not delineate precise categories of protected information, it does provide general protection for federal agency employees. The employer may disclose personnel file information[88] only when needed, and then only in types and amounts tailored closely to the need.[89] Given the vaguely defined boundaries of the Act's protections, its effective scope depends wholly on its actual implementation and enforcement.

Additionally, both federal and private sector employees are vulnerable to information abuses by their employers.[90] The Privacy Act does not directly address the waiver issue,[91] but its avowed purposes and intent implicitly prohibit waiver.[92] The Act expresses this prohibition indirectly, since it "establishes certain minimum information-gathering standards for all agencies to protect the privacy and due process rights of the individual and to assure that surrender of personal information is made with informed consent or with some guarantees of the uses and confidentiality of the information."[93] Thus, this implicit prohibi-

---

[88] The Privacy Act protects all information that is identifiable with an individual and is maintained in an agency record. This includes, in part, information regarding the individual's educational, medical, criminal, and employment history, and his financial transactions. 5 U.S.C. § 552a(a)(4) (1977).

[89] Only those parties listed among the exceptions to the Privacy Act, *see* note 20 *supra*, may receive personnel information without prior employee consent. The Congressional Statement of Purpose evidences the policy of closely tailored disclosure. Privacy Act of 1974, Pub. L. 93-579, § 2(b)(4), 88 Stat. 1897 (codified at 5 U.S.C. § 552a (1977)). The Statement provides in part that the Act safeguards personal privacy by requiring agencies to collect and disclose information only for "necessary and lawful" purposes. *Id.* Also, the information used must be accurate for all intended uses. *Id. See also* Mossman, *A New Dimension of Privacy*, 61 A.B.A. J. 829 (1975). Mossman indicates that several major privacy studies have agreed on basic principles, which include limiting third party disclosure to those who show a "need to know." *Id.* at 831.

[90] *See* notes 47-49 and accompanying text *supra*.

[91] *See* notes 49-52 and accompanying text *supra*.

[92] Congress designed the Privacy Act to protect individual privacy rights against abuses in the information practices of federal agencies. *See* Pub. L. 93-579 § 2(b), 88 Stat. 1897 (codified at 5 U.S.C. § 552a (1977)).

[93] SENATE REPORT, *supra* note 16, at 2, *reprinted in* [1974] U.S. CODE CONG. & AD. NEWS 6916, 6917. Given these minimum standards and employee disadvantage inherent in the employment relationship, *see* notes 48-49 and accompanying text *supra*, the Congressional objective of protecting privacy rights would be poorly served if employees were allowed to waive the Act's safeguards.

tion protects the employee's right to control employer use of personal information.[94]

No similar controls exist in the private sector. A privacy statute should permit waiver, if at all, only if it results from true employee choice, and not from subtle or direct employer coercion.[95] Because of the nature of the employment relationship, the line drawn between free choice and subtle coercion is necessarily fine.[96] This fine line makes it difficult to determine in each case whether the employee waived his rights voluntarily.[97] Therefore, future legislation should impose strict limitations

---

[94] *Cf.* Fried's definition of privacy, *supra* note 6.

[95] It is well established that a waiver of a constitutional right is not valid unless made voluntarily, knowingly, and intelligently. *See, e.g.,* Brady v. United States, 397 U.S. 742 (1970) (may not waive right not to plead guilty); Pfeifer v. United States Bureau of Prisons, 615 F.2d 873 (9th Cir. 1980) (may not waive right to counsel under due process clause), *cert. denied,* 447 U.S. 908 (1981); Murray v. Wainwright, 450 F.2d 465 (5th Cir. 1971) (may not waive right to speedy trial). Even though the United States Constitution does not expressly guarantee the right of privacy, in numerous cases the Supreme Court has found implicit privacy protection in various amendments to the Constitution. *See, e.g.,* Roe v. Wade, 410 U.S. 113, 153 (1973) (14th amendment); Stanley v. Georgia, 394 U.S. 557, 564-65 (1969) (1st amendment); Griswold v. Connecticut, 381 U.S. 479, 484-86 (1965) (1st, 3rd, 4th, & 5th amendments).

But see Thomas v. Veterans Administration, 467 F. Supp. 458 (D. Conn. 1979), in which the court allowed the defendant access to the Drug Enforcement Agency's files on the plaintiff, based on his waiver. The court held that the plaintiff had the burden of proving that the Veterans Administration's investigative techniques had coerced him into signing the waiver. *Id.* at 463. In *dicta,* the Court noted that the plaintiff was a college graduate with numerous years of administrative experience. *Id.* Therefore, the record did not support his allegation that he had signed involuntarily. *Id.*

[96] *See* Comment, *Regulation of Polygraph Testing in the Employment Context: Suggested Statutory Control on Test Use and Examiner Competence,* 15 U.C. DAVIS L. REV. 113 (1981). The commentator asserts that the employer's request for an individual to take a polygraph test actually coerces him into doing so. *Id.* at 119. He explains that because the current or prospective employee may think that acquiescence is mandatory to retain or obtain the job, *id.,* he might perceive the request as a demand. *Id.* By analogy, the same observation may be made regarding employee waiver of privacy rights.

[97] *See id.* One way to make this determination, for the similar problem of employee polygraph consent, would be to give the employer the burden of proving that the employee's consent was voluntary. *Id.* at 124. Because this burden would be costly, time-consuming, and difficult to carry, it effectively would limit, if not eliminate, subtle coercion by the employer. *Id.* By analogy, the same method may be applied to employee waiver of privacy rights.

upon employee ability to waive privacy rights.[98]

Employees are also vulnerable to employer information abuses when they lack access to their own files.[99] The Privacy Act aids federal agency employees since it provides for access to and amendment of records maintained by agencies about individuals.[100] The Act supports these provisions by establishing civil remedies for their breach.[101] Since private sector employees have comparable problems and since only three states provide similar protections,[102] Congress should extend these Privacy Act enforcement provisions to the private sector.[103]

Additionally, employees are vulnerable because employers need not notify them either before or after using their personal information.[104] Again, the Privacy Act protects federal employees, since it requires federal agencies to account for all disclosures,[105] and to release this accounting to an employee upon request.[106] Because no similar safeguard protects private sector employees,[107] they need some minimal statutory regulation requiring notification.

CONCLUSION

There is a recognized and ever-increasing need to protect the confidentiality of personnel files in the public and private employment sectors.[108] Congress took a partial step by passing the Privacy Act of 1974, which protects privacy rights of federal agency employees. Differences do exist between federal agency and private employer settings, both in employer compliance

---

[98] If voluntary waiver were permissible, but job applicants and employees preferred not to waive their rights, then they would retain only the option of seeking employment elsewhere. Given the high nationwide unemployment rate, *see* note 48 *supra*, this "solution" to the problems posed by permissible waiver is naive at best, providing only minimal comfort to the many employees who would be left without any real choice.

[99] *See* notes 53-55 and accompanying text *supra*.

[100] 5 U.S.C. § 552a(d) (1977).

[101] *Id.* § 552a(g).

[102] *See* note 55 *supra*.

[103] *But see* Note, *The Privacy Act of 1974: An Overview and Critique*, 1976 WASH. U.L.Q. 667, 692-95 (1977) (criticizing the Act's enforcement provisions).

[104] *See* notes 56-57 and accompanying text *supra*.

[105] 5 U.S.C. § 552a(c)(1) (1977).

[106] *Id.* § 552a(c)(3).

[107] *See* note 59 *supra*.

[108] *See* text accompanying notes 1-9 *supra*.

costs and in the capacity for overzealous employer investigations. However, many compelling similarities between the two settings outweigh these differences, including employer need for personnel information, disclosure, and employee vulnerability.

These similarities warrant extension of the Privacy Act's protections to the private sector. Specifically, a federal statute should mandate individual employee access to personnel files and employee opportunity to amend inaccurate information. Moreover, the statute should impose an employee disclosure consent requirement upon private employers, but exempt routine[109] and certain other uses[110] from this requirement.

To balance the employer's need to acquire and use personnel information against the employee's right of privacy, the statute should require that employers tailor all information uses closely to the actual needs of the party requesting the information. Finally, private sector employers should account for all disclosures, thus guaranteeing some minimal notice to employees.

All persons, regardless of their employer's public or private status, are entitled to protection of their privacy rights. Given the very nature of the privacy right, its protection should not depend upon being employed by a "federal agency." The Privacy Act of 1974 was merely a partial step in this direction. Employees in the private sector are entitled to the same protection.

Perry Ross Fredgant

---

[109] The Privacy Act defines "routine use" as the disclosure of a record "for a purpose which is compatible with the purpose for which it was collected." 5 U.S.C. § 552a(a)(7) (1977).

[110] The other uses should be similar to those enumerated as exceptions in the Privacy Act, *id.* § 552a(b). *See* note 20 *supra.*