

1978

## Employee Privacy Rights: A Proposal

Martin N. Flics

Follow this and additional works at: <https://ir.lawnet.fordham.edu/flr>



Part of the [Law Commons](#)

---

### Recommended Citation

Martin N. Flics, *Employee Privacy Rights: A Proposal*, 47 Fordham L. Rev. 155 (1978).

Available at: <https://ir.lawnet.fordham.edu/flr/vol47/iss2/2>

This Article is brought to you for free and open access by FLASH: The Fordham Law Archive of Scholarship and History. It has been accepted for inclusion in Fordham Law Review by an authorized editor of FLASH: The Fordham Law Archive of Scholarship and History. For more information, please contact [tmelnick@law.fordham.edu](mailto:tmelnick@law.fordham.edu).

## COMMENT

### EMPLOYEE PRIVACY RIGHTS: A PROPOSAL

#### INTRODUCTION

The employment relationship is one of the most fundamental and common aspects of modern society. With the possible exception of marriage, no other relationship entered into by an individual pervades his life so completely.<sup>1</sup> Although a constitutional right of marital privacy has been recognized by the Supreme Court,<sup>2</sup> an employee<sup>3</sup> in the private sector<sup>4</sup> has virtually no legal challenge the recordkeeping practices of federal agencies,<sup>7</sup> represents the him. Because the employment relationship can be terminated at the will of the employer,<sup>5</sup> an employee is presently unable, without risking the loss of his job, to challenge any methods used to collect information, the type and extent of the information sought, or the subsequent uses and disseminations by the employer of information that is often highly personal.

The Privacy Act of 1974,<sup>6</sup> which granted individuals who are the subjects of records maintained by the federal government unprecedented rights to challenge the recordkeeping practices of federal agencies,<sup>7</sup> represents the

---

1. "We have become a nation of employees. We are dependent upon others for our means of livelihood, and most of our people have become completely dependent upon wages. If they lose their jobs they lose every resource, except for the relief supplied by the various forms of social security. Such dependence of the mass of the people upon others for *all* of their income is something new in the world. *For our generation, the substance of life is in another man's hands.*" F. Tannenbaum, *A Philosophy of Labor* 9 (1951) (footnote omitted), *quoted in* Blades, *Employment at Will vs. Individual Freedom: On Limiting the Abusive Exercise of Employer Power*, 67 Colum. L. Rev. 1404, 1404 (1967).

2. *Griswold v. Connecticut*, 381 U.S. 479 (1965).

3. Throughout this Comment, the term "employee," unless otherwise indicated, will refer to nonunion job applicants and workers. Unionized workers, unlike their nonunion counterparts, may be able to bargain for contractual protection against an employer's excessive collection and use of personal information and may resolve disputes through arbitration. *See* Craver, *The Inquisitorial Process in Private Employment*, 63 Cornell L. Rev. 1, 4-7 (1977); Summers, *Individual Protection Against Unjust Dismissal: Time for a Statute*, 62 Va. L. Rev. 481, 483-84 (1976). Furthermore, as of 1974, unions represented only 21.7% of American workers. U.S. Bureau of Labor Statistics, Dep't of Labor, Bull. No. 410, *Handbook of Labor Statistics* 293 (1977).

4. This Comment will focus on private sector employees because they are presently afforded the fewest protections against privacy invasions arising in the employment relationship. Federal employees are protected by the Privacy Act of 1974, 5 U.S.C. § 552a (1976), which grants certain rights and remedies to all individuals who are subjects of records maintained by federal agencies. *See* pt. II(D) *infra*. State employees have also benefited from similarly broad privacy legislation enacted in several states. *See, e.g.,* Ark. Stat. Ann. §§ 16-801 to -810 (Supp. 1975); Conn. Gen. Stat. Ann. §§ 4-190 to -197 (West Supp. 1978); Mass. Ann. Laws ch. 66A, §§ 1-3, ch. 214, § 3B (Michie/Law. Co-op 1978 & Supp. 1978); Minn. Stat. Ann. §§ 15.162-.169 (West 1977 & Supp. 1978); Ohio Rev. Code Ann. §§ 1347.01-.10, .99 (Page Supp. 1977); Utah Code Ann. §§ 63-50-1 to -10 (1978); Va. Code §§ 2.1-377 to -386 (Supp. 1978).

5. *See* note 24 *infra* and accompanying text.

6. 5 U.S.C. § 552a (1976).

7. *See* pt. II(D) *infra*.

most comprehensive federal legislative treatment of the rights of subjects of the "information process." The recent report of the Privacy Protection Study Commission<sup>8</sup> (Privacy Commission) has furthered the development of this new area of privacy law by proposing far-reaching reforms designed to give the subjects of insurance, educational, and employment records similar rights to those provided by the Privacy Act.<sup>9</sup> There are, however, no existing constitutional or common law protections for invasions of an employee's privacy in the private sector,<sup>10</sup> and existing federal legislation provides only minimal benefits in this area.<sup>11</sup> In the absence of legislation, the outlook for protecting employee privacy interests is bleak.<sup>12</sup>

This Comment will argue that comprehensive privacy legislation protecting an employee's rights can be formulated without unduly infringing on an employer's legitimate interests in collecting and using information about its employees. Part I will explore the privacy issues raised in the employment context and the relevance of the legal nature of the employment relationship to those issues. Part II will survey existing privacy rights and their application to private sector employees, and will elucidate those general principles of privacy protection that might be incorporated into employee privacy legislation. Part III will consider two existing models of employee privacy rights, and Part IV will propose a legislative scheme granting rights and remedies to protect an employee's interests.

## I. THE EMPLOYMENT RELATIONSHIP

The term "privacy" encompasses a broad range of interests that can be invaded in any one of the following ways: (1) intrusions upon an individual's person, property, or private conversations; (2) inquiries into the private facts or beliefs of an individual by, for example, compulsory, overbroad, or surreptitious investigations; (3) the use of irrelevant, inaccurate, or incomplete facts in order to make decisions affecting an individual; and (4) the uncontrolled disclosure of facts about an individual to third parties.<sup>13</sup>

---

8. Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977) [hereinafter cited as *Privacy Report*]. The Privacy Commission was established pursuant to the Privacy Act of 1974 to study whether the requirements and principles of the Act should be applied to the private sector. Pub. L. No. 93-579, § 5(b)(2), 88 Stat. 1906.

9. See text accompanying pt. III(A) *infra*.

10. See pt. II(A), (B) *infra*.

11. See pt. II(C), (D) *infra*.

12. A recent survey conducted by the American Civil Liberties Union discovered that employees believe that their privacy interests are important and merit legal protection. The survey revealed strong support among employees for several privacy rights, including a right of access to their personnel records and a prohibition on the use of the lie detector. Westin, *Privacy and Personnel Records: A Look at Employee Attitudes*, 4 Civ. Lib. Rev. 28, 29 (Jan.-Feb. 1978).

13. The first, second, and fourth types of invasion are encompassed within the definition of privacy offered in Beane, *The Right to Privacy and American Law*, 31 Law & Contemp. Prob. 253, 254 (1966). The regulation of the third type of privacy invasion is one of the basic purposes of the Privacy Act of 1974. See Pub. L. No. 93-579, § 2(b)(4), 88 Stat. 1896; *Privacy Report*, *supra* note 8, at 17. The third type of invasion is particularly relevant to the relationship between an individual and an organization that maintains records about individuals that are utilized in decisionmaking, such as an employer, insurance company, or educational institution. See *id.*

The employment relationship is unique because the close and continuing relationship between an employer and employee presents many situations in which the employee's privacy may be invaded in any of the aforementioned ways. These invasions can occur during the four analytically distinct stages of the information process: (1) the initial collection of information about an individual; (2) the subsequent storage and maintenance of the information; (3) the employer's internal use of the information in making decisions concerning the individual; and (4) the employer's dissemination of the information to outside parties.

The collection of information begins when an individual applies for a job. Prior to being hired, a prospective employee will ordinarily complete an application form requesting his employment, financial, medical, and criminal histories, and he will probably be evaluated by an interviewer.<sup>14</sup> He might also be required to submit to a physical examination or take psychological, vocational, and lie detector tests.<sup>15</sup> In addition to the information provided by the applicant, the employer may also seek information about him from third parties by, for example, requesting references from a previous employer<sup>16</sup> or obtaining a report from a credit agency.<sup>17</sup> During this initial collection process, the first type of privacy invasion may occur if the applicant is subjected to collection methods that are unnecessarily intrusive. The second type of invasion will occur when he is required to divulge information concerning sexual matters or political beliefs.

The collection of information is not limited to the prehiring stage. Once employment begins, a variety of records about the employee are generated. These records may include such job-related information as performance evaluations, payroll data, various reports necessitated by government regulations, and records relating to fringe benefits, such as pension and health insurance programs.<sup>18</sup> Some employers, seeking to improve their efficiency or to ferret out employee-thieves, may observe employees through the use of closed circuit television and undercover investigators,<sup>19</sup> or conduct searches of employees' desks and lockers.<sup>20</sup> Although the collection of job-related information is generally useful and necessary, some of these methods of collection are often overly intrusive.

The information that has been collected by the employer will be maintained in some type of recordkeeping system, either manual or computerized.<sup>21</sup> The

---

14. See generally Privacy Report, *supra* note 8, at 223; S. Astor, Loss Prevention: Controls and Concepts 72-78 (1978).

15. See Privacy Report, *supra* note 8, at 223; S. Astor, *supra* note 14, at 78-79.

16. See Comment, *Qualified Privilege to Defame Employees and Credit Applicants*, 12 Harv. C.R.-C.L. L. Rev. 143, 146 (1977).

17. See Note, *Protecting Privacy in Credit Reporting*, 24 Stan. L. Rev. 550, 553 (1972) [hereinafter cited as *Protecting Privacy*].

18. Privacy Report, *supra* note 8, at 225-26.

19. S. Astor, *supra* note 14, at 20-21, 89-101.

20. See Ben Scheiber, *Tests and Questionnaires in the Labor-Management Relationship*, 20 Lab. L.J. 695, 696 (1969).

21. See A. Westin & M. Baker, *Databanks in a Free Society* 9-10 (1972). In some companies, typically smaller ones, all of the information will be located in one central file. In larger organizations, information may be decentralized among various departments, such as personnel and security. Privacy Report, *supra* note 8, at 225.

information will be available to persons within the company who will use it to make decisions affecting the employee. To the extent that any of the information used in making these decisions is inaccurate, irrelevant, or incomplete, the third type of privacy invasion will occur. The fourth type of invasion, the uncontrolled disclosure of personal facts, may also occur when individuals in the company gain access to information about an employee that they have no need to know.<sup>22</sup>

This fourth type of invasion may also result when an employer disseminates any of the information that he has gathered for internal use to outside parties such as credit agencies, subsequent employers, or government agencies. The vast quantity of personal data maintained by an employer that can be disclosed creates a danger of long-term damage to an employee who believed that he was supplying the information for a specific employer's purposes, only to discover years later that other prospective employers and credit agencies were freely granted access to the information. The employee may find that, as a result of these disclosures, he is denied credit or subsequent employment.<sup>23</sup> Without any control over the type of information gathered or its subsequent uses, the employee's interest in keeping certain facts private is protected solely by the unrestricted discretion of the employer.

The legal nature of the employment relationship has inhibited the development of an employee's right to challenge his employer's unfair and damaging practices. An employer has traditionally enjoyed an absolute right to discharge an employee for any or no reason in the absence of an agreement to retain him for a specified period of time.<sup>24</sup> This concept of "terminability at will" permits an employer to fire any employee who objects to the employer's collection and use of information about him.<sup>25</sup> As a result, an employer may

---

22. See note 262 *infra* and accompanying text.

23. See notes 78-86 *infra* and accompanying text.

24. 9 S. Williston, Contracts § 1017 (W. Jaeger ed. 1967); see, e.g., *Pearson v. Youngstown Sheet & Tube Co.*, 332 F.2d 439, 441 (7th Cir.), *cert. denied*, 379 U.S. 914 (1964); *Shaw v. S.S. Kresge Co.*, 328 N.E.2d 775, 779 (Ind. Ct. App. 1975); *Simmons v. Westinghouse Elec. Corp.*, 311 So. 2d 28, 31 (La. Ct. App. 1975); *Geary v. United States Steel Corp.*, 456 Pa. 171, 175, 319 A.2d 174, 176 (1974). Terminability at will is based upon the concept of mutuality of obligation in the law of contracts. J. Calamari & J. Perillo, *Law of Contracts* § 4-14 (2d ed. 1977). Because the employee is free to leave his job at any time, the principle of mutuality provides an employer with a similar right to terminate their relationship. *Simmons v. Westinghouse Elec. Corp.*, 311 So. 2d at 31 (citing *Pitcher v. United Oil & Gas Syndicate, Inc.*, 174 La. 66, 67, 139 So. 760, 761 (1932)).

Recent commentary has criticized the terminability at will theory as an anachronistic vestige of nineteenth century notions of freedom of contract between parties of relatively equal bargaining power. See, e.g., *Blades, supra* note 1, at 1418; *Summers, supra* note 3, at 485-88; *Comment, Towards a Property Right in Employment*, 22 *Buffalo L. Rev.* 1081, 1082-84 (1973); *Note, Implied Contract Rights to Job Security*, 26 *Stan. L. Rev.* 335, 337-40 (1974). Courts have also expressed dissatisfaction over the terminability theory. In *Monge v. Beebe Rubber Co.*, 114 N.H. 130, 134, 316 A.2d 549, 551 (1974), the court found that a bad faith termination of an "at will" employee was a breach of the employment contract. As noted by the dissent, this decision constituted "broad new unprecedented law". *Id.* at 137, 316 A.2d at 553 (Grimes, J., dissenting). For further criticism in a case that narrowly upheld terminability at will, see *Geary v. United States Steel Corp.*, 456 Pa. 171, 190-94, 319 A.2d 174, 183-85 (1974) (Roberts, J., dissenting).

25. "This traditional rule . . . is what most tends to make [an employee] a docile follower of his employer's every wish." *Blades, supra* note 1, at 1405.

generally collect and use this information in virtually any way it chooses.<sup>26</sup> The employee's options are either to accept the practices, to protest them and face possible dismissal, or to leave his job voluntarily, none of which are particularly desirable. The employee will also find himself without any legal remedies because existing actions for privacy invasion have limited applicability in the employment context.<sup>27</sup> The employer, on the other hand, will probably have little difficulty in replacing the employee and may continue its practices without legal restriction.

## II. EXISTING PRIVACY RIGHTS

### A. *The Constitutional Right of Privacy*

Although the Constitution contains no specific provision which affords individuals privacy rights, several amendments have been identified as sources of such rights.<sup>28</sup> The constitutional right of privacy can be classified as protecting three general interests:<sup>29</sup> the interest in freedom from unreasonable governmental searches and surveillance;<sup>30</sup> the interest in controlling the dissemination of personal information;<sup>31</sup> and the interest in autonomy in making intimate personal decisions.<sup>32</sup> Unfortunately, these constitutional protections have no direct application to the private sector employment context because the requisite state action to trigger constitutional analysis is lacking.<sup>33</sup> Although arguments have been advanced to extend the state action concept to the private sector employer so as to bring these constitutional

---

26. See *Hollenbaugh v. Carnegie Free Library*, 436 F. Supp. 1328, 1330, 1333-34 (W.D. Pa. 1977) (discharge of "at will" employees discovered to be living together in "open adultery" held not to violate their constitutional right to privacy).

27. See pt. II(A), (B) *infra*.

28. See *Roe v. Wade*, 410 U.S. 113, 153 (1973) (fourteenth amendment's concept of personal liberty); *Katz v. United States*, 389 U.S. 347, 353 (1967) (fourth amendment); *Griswold v. Connecticut*, 381 U.S. 479, 484-85 (1965) (penumbra of the Bill of Rights); *id.* at 487 (Goldberg, J., concurring) (ninth amendment); *NAACP v. Alabama*, 357 U.S. 449, 462 (1958) (first amendment).

29. *Crain v. Krehbiel*, 443 F. Supp. 202, 207-08 (N.D. Cal. 1977); see *Whalen v. Roe*, 429 U.S. 589, 599-600 & nn.24 & 25 (1977).

30. See, e.g., *Katz v. United States*, 389 U.S. 347, 353 (1967) (eavesdropping on conversations made from enclosed telephone booth held to violate fourth amendment); *Rochin v. California*, 342 U.S. 165, 172-74 (1952) (pumping of defendant's stomach held an unlawful forced confession).

31. See, e.g., *Whalen v. Roe*, 429 U.S. 589, 599 (1977); cf. *NAACP v. Alabama*, 357 U.S. 449, 462-66 (1958) (state requirement that private organization reveal its membership list held to violate freedom of association). In *United States v. Miller*, 425 U.S. 435 (1976), the Court did not extend the right to control disclosure to permit a bank depositor to prevent his bank from complying with a subpoena. *Id.* at 440-41. Although the reach of the *Miller* decision is unclear, the Court distinguished the facts of the case from other situations in which an interest in controlling disclosure should be afforded constitutional protection. *Id.* at 444-45 nn.6 & 7.

32. See, e.g., *Roe v. Wade*, 410 U.S. 113, 152-56 (1973); *Griswold v. Connecticut*, 381 U.S. 479, 481-86 (1965).

33. The due process clause of the fourteenth amendment protects only against infringements of rights by the state and not against those by private parties. See, e.g., *Jackson v. Metropolitan Edison Co.*, 419 U.S. 345, 349 (1974).

protections into play,<sup>34</sup> there is no reason to believe that the vast majority of private sector employers will be directly subject to constitutional limitations in the foreseeable future.<sup>35</sup>

### B. *The Common Law Right of Privacy*

An influential law review article by Warren and Brandeis in 1890,<sup>36</sup> lamenting the indiscreet reporting of "high society" by gossip columnists,<sup>37</sup> first proposed the development of a common law right of privacy. The article reinterpreted prior common law actions for wrongful publication of private letters and intellectual property as arising not from the breach of an implied contract or from a narrow interpretation of property law, but from an independent interest in the right to an inviolate personality—the right to privacy.<sup>38</sup> New York was the first state to adopt a limited privacy right by

---

34. One established line of analysis would find the activities of large corporations to be state action because of their pervasive influence over the lives of many citizens. *See, e.g., Berle, Constitutional Limitations on Corporate Activity—Protection of Personal Rights from Invasion Through Economic Power*, 100 U. Pa. L. Rev. 933 (1952). Although the Court has never accepted this argument, it has, on occasion, found state action when a private corporation was performing governmental functions. *See Marsh v. Alabama*, 326 U.S. 501 (1946) (private corporation performing all necessary municipal functions in company-owned town). Some commentators have endorsed this "private state action" approach as a method of applying constitutional privacy law to the private sector. *See, e.g., Hermann, Privacy, the Prospective Employee, and Employment Testing: The Need To Restrict Polygraph and Personality Testing*, 47 Wash. L. Rev. 74, 140-42, 148-49 (1971); Comment, *Privacy: The Polygraph in Employment*, 30 Ark. L. Rev. 35, 44-45 (1976).

35. Although state action was found in *Holodnak v. Avco Corp.*, 514 F.2d 285 (2d Cir.), *cert. denied*, 423 U.S. 892 (1975), the case would seem to be *sui generis*. In *Holodnak*, the employer was a government contractor, and the United States owned all of the land, buildings, and equipment used by the employer, and supervised the manufacturing process. *Id.* at 289. In *Flagg Bros., Inc. v. Brooks*, 436 U.S. 149 (1978), however, the Court refused to expand the state action doctrine to a private sale of goods by a warehouseman acting under the provisions of the Uniform Commercial Code. Given the extreme facts of *Holodnak*, and the Court's failure to expand the state action doctrine in *Flagg Brothers*, the state action requirement still cannot be interpreted on the basis of any judicial authority to include the privacy-invading activities of any large private employer. In *Flagg Brothers*, the Court noted that under the public function analysis of state action, a private organization must be performing functions that have been exclusively reserved to government. *Id.* at 157-64. Using a second line of state action analysis, the Court reaffirmed the view expressed in *Jackson v. Metropolitan Edison Co.*, 419 U.S. 345, 357 (1974), that the mere acquiescence of the state in private action is not tantamount to state action. 436 U.S. at 164-66. Requiring a private party to conform to certain standards, however, would constitute state action. *Moose Lodge No. 107 v. Iris*, 407 U.S. 163 (1972). Thus, absent judicial or legislative enactment that expressly requires a party to perform some act, it is unlikely that state action will be found. *See Flagg Bros., Inc. v. Brooks*, 436 U.S. at 168-71 (Stevens, J., dissenting).

Since the direction of these decisions is to require a case-by-case determination of whether state action exists, based upon criteria that are unlikely to be met by most private employers, it is unrealistic to formulate a theory of constitutional privacy protection that would be generally applicable to the private sector.

36. Warren & Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

37. *Id.* at 196.

38. *Id.* at 211-13.

statute,<sup>39</sup> and virtually every state has subsequently recognized, either judicially or by statute, a privacy right in one form or another.<sup>40</sup>

The broad contours of this common law right, reflected in the academic debate over the precise characterization of privacy interests,<sup>41</sup> preclude any exact definition of its nature and scope. There is, however, a general consensus that the common law right is divided into four distinct causes of action: (1) public disclosure of private facts; (2) placement of an individual in a false light before the public eye; (3) commercial appropriation of an individual's name or likeness; and (4) intrusion upon an individual's seclusion.<sup>42</sup>

These causes of action have provided minimal practical benefit to the employee aggrieved by his employer's unfair collection and disclosure procedures.<sup>43</sup> The action for commercial appropriation is narrow and fails to address the major privacy issues facing employees.<sup>44</sup> At first glance, the

39. 1903 N.Y. Laws ch. 132, §§ 1-2 (current version at N.Y. Civ. Rights Law §§ 50-51 (McKinney 1976)). Section 51 provides an action for damages and injunctive relief for the unconsented use of any person's name, portrait, or picture for advertising purposes without his consent. This is essentially a codification of the common law action for commercial appropriation. See notes 42, 44 *infra* and accompanying text.

40. Only Nebraska and Wisconsin have expressly rejected a privacy right. See *Brunson v. Ranks Army Store*, 161 Neb. 519, 73 N.W.2d 803 (1955); *Yoeckel v. Samonig*, 272 Wis. 430, 75 N.W.2d 925 (1956). In addition to New York, five states recognize a limited privacy right pursuant to statute. Mass. Ann. Laws ch. 214, § 3A (Michie/Law. Co-op 1974); Okla. Stat. Ann. tit. 21, §§ 839.1-.3 (West Supp. 1977); R.I. Gen. Laws § 9-1-28 (Supp. 1977); Utah Code Ann. §§ 76-9-401 to -406 (Supp. 1977); Va. Code § 18.2-216.1 (Supp. 1978). The remainder of the states have judicially adopted the broader common law right of privacy. See, e.g., *Rugg v. McCarty*, 173 Colo. 170, 476 P.2d 753 (1970); *Housh v. Peth*, 165 Ohio St. 35, 133 N.E.2d 340 (1956); *Billings v. Atkinson*, 489 S.W.2d 858 (Tex. 1973).

41. Privacy protection has been described as serving a variety of functions, including "personal autonomy," "emotional release," "self-evaluation," and "limiting and protecting communication." A. Westin, *Privacy and Freedom* 32-39 (1967). The importance of allowing an individual to conceal the intimate facts of certain private relationships, such as marriage, has also been noted. Fried, *Privacy*, 77 Yale L.J. 475, 484 (1968). Another commentator has focused on the right to control the disclosure of information about oneself. Beaney, *The Right to Privacy and American Law*, 31 Law & Contemp. Prob. 253, 254 (1966).

42. W. Prosser, *The Law of Torts* § 117, at 804-14 (4th ed. 1971). The separate nature of the four actions has been challenged. See Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. Rev. 962 (1964). Professor Bloustein attempts to unify the four torts under the concept of dignity. In all the privacy cases, "[t]he injury is to our individuality, to our dignity as individuals, and the legal remedy represents a social vindication of the human spirit thus threatened rather than a recompense for the loss suffered." *Id.* at 1003. Dean Prosser, however, has advocated the separateness of the four torts by pointing out the distinct interests that they represent. For example, the intrusion tort is akin to the tort of the intentional infliction of mental distress, whereas the tort of public disclosure of private facts protects a reputational interest. Prosser, *Privacy*, 48 Calif. L. Rev. 383, 422 (1960).

43. In some cases, an employee might be able to bring a defamation action as a result of an employer's disseminations. Employers, however, have traditionally enjoyed a qualified privilege against libel and slander suits based on their remarks in employee letters of reference. Comment, *Qualified Privilege to Defame Employees and Credit Applicants*, 12 Harv. C.R.-C.L. L. Rev. 143, 144 (1977).

44. Although it is certainly possible that an employee's name or likeness might be commer-



actions for public disclosure and false light would seem to afford some protection against an employer's communication of embarrassing or misleading information in references to outsiders or in intracompany reports.<sup>45</sup> Several barriers, however, prevent such an application of the privacy right. First of all, these actions require that publication of the privacy-invasive facts be made to a large group of people.<sup>46</sup> A disclosure to one or two employees or to a subsequent employer would not ordinarily satisfy this requirement.<sup>47</sup> Furthermore, these disclosures would have to be made without the employee's consent to give rise to the cause of action.<sup>48</sup> This requirement often precludes recovery because, even if the employee did not expressly consent to subsequent disclosures of information, he may be deemed to have consented implicitly by voluntarily supplying information to an employer, or by failing to object to the collection of information from third parties.<sup>49</sup> Also, any information developed independently by an employer, such as a performance evaluation, would not be regarded as private and thus its disclosure would not be tortious.<sup>50</sup>

---

cially appropriated by an employer, it is not any more likely to occur to an employee than to anyone else. To the extent that such an injury does occur, the existing cause of action is adequate.

45. The elements of the public disclosure cause of action are: (1) publicity; (2) disclosure of facts that are private, rather than public; and (3) the facts so publicized would be objectionable to a reasonable man. W. Prosser, *supra* note 42, § 117, at 809-12. An action for false light requires: (1) publicity; (2) a false portrayal; and (3) a portrayal objectionable to a reasonable man. It might consist of falsely attributing statements to a person or juxtaposing one's picture with an article when there is, in fact, no connection. *Id.* § 117, at 812-13.

46. *Santiesteban v. Goodyear Tire & Rubber Co.*, 306 F.2d 9, 11 (5th Cir. 1962); W. Prosser, *supra* note 42, § 117, at 810, 814. This publication requirement reflects the fact that privacy actions evolved largely from concerns with the publicity given by the mass media. *See* A. Westin & M. Baker, *supra* note 21, at 19.

47. *See* W. Prosser, *supra* note 42, § 117, at 810. *But see* *Beaumont v. Brown*, 401 Mich. 80, 257 N.W.2d 522 (1977). In *Beaumont*, the Michigan Supreme Court permitted an action for the public disclosure of private facts based on an employer's dissemination of information to the plaintiff's Army reserve officer. The employer had written a letter to the reserve officer stating that the employee had manipulated his reserve duty and submitted false health reports. The court found sufficient publication because the information was not contained in a personal letter and thus would be made known throughout the Army reserve office. *Id.* at 102, 257 N.W.2d at 530. The court also stated that the facts in the letter about the plaintiff's health were "not necessary" and that the information about military status could have been conveyed without "pejorative overtones." *Id.* at 97-98, 257 N.W.2d at 528. For the present, *Beaumont* represents a departure from the traditional analysis of the public disclosure of private facts. The court's reliance on the fact that the employer was under no duty to provide the health information and did not have to convey the information in such a negative tone is a novel approach. *Id.* at 97-98, 257 N.W.2d at 528. The same can be said for the analysis of the publication requirement.

48. *See generally* W. Prosser, *supra* note 42, § 18, at 101-03.

49. *See* *Bloomfield v. Retail Credit Co.*, 14 Ill. App. 3d 158, 173-74, 302 N.E.2d 88, 100 (1973) (implied consent to disclosure of credit report to employers because plaintiff had supplied their names as credit references); *In re Bates*, 555 S.W.2d 420, 430 (Tex. 1977) (conversation with an individual is implied consent to disclosure of the contents of the discussion to third parties).

50. "Information about the plaintiff which was already known to others could hardly be regarded as private to the plaintiff." *Nader v. General Motors Corp.*, 25 N.Y.2d 560, 569, 255 N.E.2d 765, 770, 307 N.Y.S.2d 647, 654 (1970).

The fourth privacy action, intrusion upon an individual's seclusion, is not concerned with the content or disclosure of the information, but rather with the injury inflicted by the method used to obtain it.<sup>51</sup> Wiretapping, physical intrusions into a person's residence, and other frequently overzealous means of surveillance are examples of intrusive activities that have formed the basis for liability under this cause of action.<sup>52</sup> In the employment relationship, employers use similarly intrusive activities such as lie detectors, overbroad and irrelevant application forms, closed circuit television surveillance, and pretext interviews in which an investigator conceals his identity and purpose in order to obtain information about an employee from others.<sup>53</sup>

Nevertheless, an intrusion action brought by an employee stands little chance of success. Express consent, which will bar any claim asserted by the employee, is usually obtained prior to the use of many of these methods of collecting information.<sup>54</sup> Recovery is difficult even when methods are used in which consent is not normally obtained. The collection of information from third parties is not considered an intrusion upon anything private because the facts are already known to the third parties.<sup>55</sup> In addition, one court has held that the use of closed circuit surveillance devices, ostensibly for the purpose of evaluating employee efficiency, has a sufficient business justification to rebut any claim of unconsented-to intrusion.<sup>56</sup>

The causes of action comprising the common law right of privacy, though affording valuable privacy protection to society as a whole, have almost no application to the employment relationship. In most cases, application of the technical legal definitions of consent, publicity, or private facts would bar an

---

51. See *Pearson v. Dodd*, 410 F.2d 701, 704 (D.C. Cir.), cert. denied, 395 U.S. 947 (1969). Intrusion is the only privacy tort that does not involve "informational betrayal." Note, *The Massachusetts Right of Privacy Statute: Decoy or Ugly Duckling?*, 9 Suffolk L. Rev. 1248, 1276 (1975).

52. See, e.g., *Galella v. Onassis*, 487 F.2d 986, 995 (2d Cir. 1973) ("constant surveillance" and "obstrusive and intruding presence"); *Dietemann v. Time, Inc.*, 449 F.2d 245, 246 (9th Cir. 1971) (surreptitious photographing and recording in private home); *Hamberger v. Eastman*, 106 N.H. 107, 108, 206 A.2d 239, 240 (1964) (electronic listening and recording device installed in plaintiffs' bedroom); *Nader v. General Motors Corp.*, 25 N.Y.2d 560, 570, 255 N.E.2d 765, 771, 307 N.Y.S.2d 647, 655 (1970) ("overzealous" surveillance which included following the plaintiff into a bank and observing the amount of money withdrawn from his bank account).

53. Privacy Report, *supra* note 8, at 240, 330-35.

54. Consent "negative[s] the existence of any [intentional] tort." W. Prosser, *supra* note 42, § 18, at 101; see Comment, *The Polygraph in Private Industry: Regulation or Elimination?*, 15 Buffalo L. Rev. 655, 667 (1966) (discussing express consent to polygraph). Although the consent in these circumstances is perhaps illusory, as a result of the economic necessity for the employee to submit to these practices or risk being fired, it does not rise to the level of duress traditionally required for negating the consent. The threat of losing employment, a form of economic coercion, is specifically cited by Dean Prosser as an example of an insufficient level of coercion for a finding of consent under duress. W. Prosser, *supra* note 42, § 18, at 106. The threat ordinarily must be of direct physical harm. *Id.*

55. See *Nader v. General Motors Corp.*, 25 N.Y.2d 560, 568-69, 255 N.E.2d 765, 770, 307 N.Y.S.2d 647, 654 (1970) (interviewing acquaintances of the plaintiff does not constitute an actionable invasion of privacy).

56. *Thomas v. General Electric Co.*, 207 F. Supp. 792, 799 (W.D. Ky. 1962).

employee's claim. Nevertheless, the conclusion remains inescapable that the practices that employees are subjected to invade interests in what is best identified as privacy.<sup>57</sup>

### C. *The Fair Credit Reporting Act*

The Fair Credit Reporting Act (FCRA), enacted by Congress in 1970,<sup>58</sup> remains the most important federal legislative effort to regulate privacy-invading activities in the private sector.<sup>59</sup> The FCRA was primarily designed to curtail the abuses by credit agencies in the reporting of personal information about individuals.<sup>60</sup> The almost indiscriminate disclosure of personal facts, concerning such matters as an individual's financial status, medical history, and sexual relationships, to virtually anyone that requested the information<sup>61</sup> often resulted in substantial embarrassment and humiliation to

57. See notes 14-23 *supra* and accompanying text.

58. Pub. L. No. 91-508, § 601, 84 Stat. 1127 (codified at 15 U.S.C. §§ 1681-1681t (1976)).

59. The Family Educational Rights and Privacy Act of 1974 (Buckley Amendment), 20 U.S.C. § 1232g (1976), is the other important federal privacy statute applicable to the private sector. It provides parents of school children with access to their child's school records, *id.* § 1232g(a)(1)(A), and requires that their written consent be obtained prior to the disclosure of information by the school to third parties. *Id.* § 1232g(b)(1). Although both of these rights are broader than comparable FCRA provisions, *see* notes 68, 74-76 *infra* and accompanying text, the FCRA is used to illustrate federal privacy legislation because it imposes a greater variety of requirements on credit agencies. The FCRA, for example, expressly provides a private cause of action for damages, 15 U.S.C. §§ 1681n-1681o (1976), whereas the Buckley Amendment does not. *See Girardier v. Webster College*, 563 F.2d 1267, 1276-77 (8th Cir. 1977). Furthermore, the lack of legislative hearings on the Buckley Amendment and sparsity of case law makes analysis of its provisions problematic. *See Rios v. Read*, 73 F.R.D. 589, 597 (E.D.N.Y. 1977).

60. *See* 15 U.S.C. § 1681 (1976). *See generally Protecting Privacy*, *supra* note 17, at 553-56; Note, *Protecting the Subjects of Credit Reports*, 80 Yale L.J. 1035, 1037-40 (1971) [hereinafter cited as *Protecting Subjects*].

There are actually two types of credit agencies. One, commonly known as the "credit bureau," specializes in the preparation of reports for credit purposes, primarily for merchants considering the extension of retail credit. These reports emphasize financial information, such as credit history, existing lines of credit, bank balances, and bill-paying habits, and frequently include information about the subject's employment history and marital life. Comment, *Commercial Credit Bureaus: The Right to Privacy and State Action*, 24 Am. U. L. Rev. 421, 423-24 (1975). The second type of credit agency, which has been termed the "credit reporting bureau," *see Protecting Privacy*, *supra* note 17, at 552, supplies more detailed reports than those supplied by credit bureaus. In addition to the information presented in a credit bureau's report, credit reporting bureaus also include comments on the character, reputation, and personal habits of the subject based upon interviews with friends, neighbors, and co-workers. Employers and insurance companies are leading users of such reports. *See* A. Westin & M. Baker, *supra* note 21, at 131.

The FCRA eliminates this terminology by defining all organizations subject to its requirements as "consumer reporting agencies," 15 U.S.C. § 1681a(f) (1976), but recognizes the distinction between the two types of reports by separately defining "consumer reports" (similar to credit bureau reports), *id.* § 1681a(d), and "investigative consumer reports" (similar to credit reporting bureau reports). *Id.* § 1681a(e). Although the provisions covering consumer reports are applicable to investigative consumer reports, *see* *Ley v. Boron Oil Co.*, 419 F. Supp. 1240, 1242 (W.D. Pa. 1976), some additional requirements for investigative consumer reports are provided. *See, e.g.*, 15 U.S.C. § 1681d (1976).

61. The relative ease with which persons having no legitimate need for information could gain access to credit reports about other individuals was illustrated by an experiment conducted

the subject of the report.<sup>62</sup> The reporting of inaccurate, incomplete, or obsolete information was frequently a direct cause of the denial of credit, employment, or insurance<sup>63</sup> to an individual who was generally unaware that such information was being reported.<sup>64</sup> Even if he did become aware, he had no legal right to require correction of the reports or to remedy the harm that was caused.<sup>65</sup>

The FCRA is relevant to the present inquiry for two reasons. First, because credit agencies frequently distribute their reports to employers which use them in making employment decisions,<sup>66</sup> the FCRA's regulation of credit agencies and users of credit reports grants private sector employees their only federally legislated privacy rights. Second, the FCRA's scheme of rights and remedies presents a possible model for similar regulation of employers in the private sector.

### 1. Employee Protection

The privacy rights afforded the employee under the FCRA are certainly tangible, albeit of limited scope. If an employer requests a credit report on a prospective employee and, as a result of information contained in that report, decides not to make a job offer, the employer must inform the rejected applicant of the name and address of the credit agency that supplied the report.<sup>67</sup> The applicant may then make a request of the credit agency to learn the "nature and substance" of most of the information maintained on him.<sup>68</sup> The credit agency must also disclose the sources of the information<sup>69</sup> and all

---

in 1970 which focused national attention on the credit reporting problem. CBS News invented a company and supplied it with letterheads, a mailing address, and telephone service. The fictitious company wrote to twenty-eight credit bureaus requesting reports on persons who had complained to their congressmen about credit bureaus. Of twenty-three responses, seven complete reports and three contractual offers to supply reports were received. Even though this occurred prior to the enactment of the FCRA, the credit bureaus were violating industry-wide regulations promulgated by the Associated Credit Bureaus of America that were in force at the time. *Protecting Subjects*, *supra* note 60, at 1039-40 & n.24.

62. See *Protecting Privacy*, *supra* note 17, at 554.

63. See *id.* at 555-56 (such decisions characterized as "irrational discriminations").

64. *Protecting Subjects*, *supra* note 60, at 1037.

65. Of course, an action for libel or slander might be available. *Id.* at 1049-54. Recovery against credit agencies is difficult, however, because they are protected by a qualified privilege which requires the plaintiff to show that the credit agency acted with malice. See, e.g., *Bloomfield v. Retail Credit Co.*, 14 Ill. App. 3d 158, 302 N.E.2d 88 (1973); *Thornton v. New S. Life Ins. Co.*, 262 S.C. 651, 207 S.E.2d 88 (1974).

66. *Protecting Privacy*, *supra* note 17, at 553.

67. 15 U.S.C. § 1681m(a) (1976). If an employer does make a job offer, there is no such requirement. Therefore, unless a successful applicant has independent knowledge of his rights under the FCRA and the name of the credit agency maintaining his file, his right of access will be vindicated only after an adverse decision has been made. See Hayden, *How Much Does the Boss Need to Know?*, 3 Civ. Lib. Rev. 23, 26 (Aug.-Sept. 1976).

68. 15 U.S.C. § 1681g(a)(1) (1976). "The intent [is] to permit the consumer to examine all the information in his file except for sources of investigative information, while not giving the consumer the right to physically handle his file." H.R. Rep. No. 1587, 91st Cong., 2d Sess. 29, reprinted in [1970] U.S. Code Cong. & Ad. News 4414, 4415.

69. 15 U.S.C. § 1681g(a)(2) (1976). Sources for the more detailed investigative consumer report need not be disclosed. *Id.*

recipients of reports within the preceding six months.<sup>70</sup> If the subject disputes the accuracy of any item in his file, he is entitled to have that item reinvestigated by the credit agency.<sup>71</sup> In the event that the reinvestigation does not resolve the dispute, the subject may have his version of the disputed facts included in subsequent reports.<sup>72</sup> If the reinvestigation results in the deletion of information from a report or causes the subject to dispute the results of the reinvestigation, the credit agency must, at the subject's request, notify prior recipients designated by the subject.<sup>73</sup>

The FCRA also provides that a credit agency's report may not include obsolete matters, defined by the Act to include certain specific types of information<sup>74</sup> as well as any adverse information that is more than seven years old when the report is made.<sup>75</sup> Also, if an employer requests a more in-depth report that will require neighbors, friends, or associates of the subject to be interviewed by the credit agency, the subject must first be notified that the investigation will be conducted.<sup>76</sup>

Although these rights under the FCRA enable an employee to have greater knowledge of the information being collected and disseminated about him, two recent cases illustrate the limited remedial value of the FCRA in the employment area.<sup>77</sup> In *Goodnough v. Alexander's, Inc.*,<sup>78</sup> a seventeen-year-old department store clerk was discharged after her employer learned from a credit report that she had been accused of shoplifting at the age of twelve. Because the information was less than seven years old and therefore not obsolete under the FCRA's standards, the credit agency had an absolute right to report it.<sup>79</sup> The clerk was also held to have no remedy against her employer

70. *Id.* § 1681g(a)(3).

71. *Id.* § 1681i(a).

72. *Id.* § 1681i(b)-(c). The credit agency is not required, however, to inform a subject of his right to file such a statement of dispute. *Roseman v. Retail Credit Co.*, 428 F. Supp. 643 (E.D. Pa. 1977); *Middlebrooks v. Retail Credit Co.*, 416 F. Supp. 1013, 1018 (N.D. Ga. 1976).

73. 15 U.S.C. § 1681i(d) (1976). In these situations, a subject must be notified of his right to make such a request. *Id.*

74. *Id.* § 1681c. The information that cannot be reported includes bankruptcies more than fourteen years old at the time of the report, and suits or judgments, delinquent accounts, paid tax liens, and information about arrests, indictments, or convictions that occurred more than seven years prior to the report. *Id.* §§ 1681c(a)(1)-(5).

75. *Id.* § 1681c(a)(6). None of the provisions in § 1681c(a) apply if the subject of the report is applying for a job at an annual salary of \$20,000 or more. *Id.* § 1681c(b)(3).

76. *Id.* § 1681d(a)(1). Such a notification need not be given when the report is being prepared to evaluate the subject for a job for which he has not specifically applied. *Id.* § 1681d(a)(2).

77. The Act has limited value in other contexts as well. *Cf. Sizemore v. Bambi Leasing Corp.*, 360 F. Supp. 252, 255 (N.D. Ga. 1973) (FCRA does not protect consumers applying for business credit); *Porter v. Talbot Perkins Children's Servs.*, 355 F. Supp. 174, 178-79 (S.D.N.Y. 1973) (child adoption agency is not a consumer reporting agency within the FCRA because its decisions are not economic ones).

78. 82 Misc. 2d 662, 370 N.Y.S.2d 388 (Sup. Ct. 1975).

79. *Id.* at 664-65, 370 N.Y.S.2d at 390-91. The court felt constrained to reach this decision by the specific provisions of the FCRA, but criticized the statute nonetheless. "The [FCRA] needs strengthening to make unduly prejudicial, questionable, or insignificant information of youthful discrimination unavailable. But, right now, there is no law against a reporting agency passing on such information, nor against a department store's moral abdication in using it. There is not even a statutory standard." *Id.* In other words, there is no relevancy standard. *See Herring v. Retail Credit Co.*, 266 S.C. 455, 459-60, 224 S.E.2d 663, 665 (1976). The absence of such a standard has

because she was employed "at will."<sup>80</sup>

In *Peller v. Retail Credit Co.*,<sup>81</sup> the plaintiff had applied for a job with a company that required all applicants to undergo lie detector tests. He was not hired because the test revealed that he had previously smoked marijuana. After being hired by another company, the plaintiff was dismissed when his new employer requested a copy of his credit report and discovered his prior marijuana use. The plaintiff's suit against the first employer and the administrator of the lie detector test, alleging violations of the FCRA and invasion of privacy, was dismissed.<sup>82</sup> The court held that neither of the defendants were subject to the FCRA's requirements because they were not consumer reporting agencies.<sup>83</sup> Furthermore, because the FCRA forbids invasion of privacy suits based on information that is obtained pursuant to its procedures unless there is a showing of malice,<sup>84</sup> the plaintiff's claims did not fall within the provisions of the Act.<sup>85</sup> The minimal requirements imposed on the users of credit reports<sup>86</sup> precluded any action against the second employer who had requested the report and dismissed the plaintiff.

In both cases, the individuals faced repeated injury by the continued reporting of information of questionable relevance. The prospect of an individual being unable to find employment for a seven year period because of arguably irrelevant information that subsequently finds its way into credit reports seems to be an unduly harsh punishment. The fact that the information is frequently obtained by methods that may themselves constitute invasions of privacy makes the widespread dissemination of that information a frightening possibility. These gaps in the FCRA's application to the employment context indicate the need for stronger limitations on the methods of collection used and the types of information collected,<sup>87</sup> and on the present ease with which such information may be obtained.<sup>88</sup>

## 2. The FCRA as a Model for Regulation of Employers

The most important provisions of the FCRA permit access by a subject to credit information, correction procedures, and damages when the subject suffers injury.<sup>89</sup> Such provisions have emerged as fundamental elements of informational privacy legislation.<sup>90</sup> Beyond these skeletal concepts, however,

---

been described as the fundamental weakness of the Act. *Protecting Privacy* *supra* note 17, at 560; see Hayden, *supra* note 67, at 26.

80. 82 Misc. 2d at 665, 370 N.Y.S.2d at 391; see note 24 *supra* and accompanying text.

81. 359 F. Supp. 1235 (N.D. Ga. 1973), *aff'd mem.*, 505 F.2d 733 (5th Cir. 1974).

82. *Id.* at 1237.

83. *Id.*; see note 60 *supra*.

84. 15 U.S.C. § 1681h(e) (1976).

85. 359 F. Supp. at 1237.

86. See note 67 *supra* and accompanying text.

87. See pt. IV(B)(1) *infra*.

88. See pt. IV(B)(4) *infra*.

89. 15 U.S.C. §§ 1681n-1681o (1976) (actions for damages based on intentional or negligent violations).

90. See Privacy Act of 1974, 5 U.S.C. §§ 552a(d)(1)-(2), (g)(4) (1976); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. §§ 1232g(a)(1)(A), (a)(2) (1976). For a discussion of the Privacy Act of 1974, see pt. II(D) *infra*. See also Bagley, *The Politics of Privacy*, in *Privacy (A Summary of a Seminar on Privacy)* 55 (Council of State Governments ed. 1975).

the specific scheme of rights and remedies established by the FCRA is not susceptible to ready incorporation into other private sector privacy legislation. The FCRA is aimed at the particular problems of the credit reporting industry,<sup>91</sup> focusing on the actual processes of reporting credit information, the users of that information, and the damage that is likely to result from a misuse of the procedures. Regulation of credit agencies was relatively easy because certain specific practices of the credit agencies could be identified and made the subject of regulation. Private sector employers, however, are more varied in their collection practices and uses of personal information.<sup>92</sup> Employers collect many types of information, such as psychological, medical, intelligence, credit, and employment evaluations. The precise uses of this information may be difficult to identify as the critical factor in any one of the many decisions made affecting an employee. Because of the relative diversity and sheer number of employer practices, legislation must not only identify and limit specific abuses, but must also formulate broader objective standards that would apply fairly to all employers.<sup>93</sup>

The FCRA therefore fails to provide an adequate model for employee privacy legislation. In addition, the specific weaknesses of the statute, such as its lack of any general standard of relevance to evaluate what type of information may be reported,<sup>94</sup> its failure to require that a subject always be informed of his rights,<sup>95</sup> its limited access provision,<sup>96</sup> and its limitation on liability from actions for invasion of privacy,<sup>97</sup> all suggest that some refinement is needed before it will fully protect the privacy interests of consumers in general, much less serve as a model for other legislation.

#### D. *The Privacy Act of 1974*

The Privacy Act of 1974<sup>98</sup> establishes a complete framework of rights and remedies for the subjects of records that are maintained by federal agen-

---

91. Indeed, industry representatives were closely involved in the drafting of the legislation. See generally Denney, *Federal Fair Credit Reporting Act*, 88 Banking L.J. 579, 583-84 (1971). The statute has nevertheless been the subject of many specific criticisms. See, e.g., Privacy Report, *supra* note 8, at 70; *Protecting Privacy*, *supra* note 17, at 558-61.

92. The diversity of employer practices has frequently been noted. See, e.g., *Privacy: Joint Hearings on S.3418, S.3633, S.3116, S.2810, and S.2542 Before the Ad Hoc Subcomm. on Privacy and Information Systems of the Senate Comm. on Government Operations and the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 93d Cong., 2d Sess. 629-31 (1974) [hereinafter cited as *Privacy Hearings*] (statement of National Retail Merchants Association); Privacy Report, *supra* note 8, at 233. The Privacy Commission, however, suggests implementing some of its recommendations on employee privacy by amending the FCRA. See notes 148-50 *infra* and accompanying text.

93. An example of a specific provision would be to prohibit the use of lie detectors, see notes 255-72 *infra* and accompanying text, rather than attempting to prohibit all intrusive collection devices. The latter provision would undoubtedly create serious uncertainty because of the great number and variety of collection methods utilized by employers. A general provision that accommodates various employer practices, yet establishes a clear standard, would be to require an employee's consent to an employer's dissemination of information about him. See note 274 *infra* and accompanying text.

94. See note 79 *supra* and accompanying text.

95. See notes 67, 72, 76 *supra*.

96. See note 68 *supra*.

97. See note 82 *supra* and accompanying text.

98. 5 U.S.C. § 552a (1976).

cies.<sup>99</sup> The fundamental purpose of the Act is to require agencies to keep their records with due regard for the privacy interests of the subjects of those records, and to give the subjects some control over the process of collection, maintenance, use, and dissemination of information about them. Although the Act has no direct application to the private sector,<sup>100</sup> its comprehensive provisions are the clearest expression of federal policy in the area of informational privacy.<sup>101</sup>

The Act incorporates the basic elements of recordkeeping privacy protection that have evolved to date. Subject to various exceptions,<sup>102</sup> it provides

---

99. Before its enactment, the right of privacy was usually "subordinated to the more concrete objectives to be gained through particular requests for information." Eastman, *Enforcing the Right of Privacy Through the Privacy Act of 1974*, 34 Fed. B.J. 335, 335 (1975). Preliminary research conducted prior to the Privacy Act revealed 858 federal data banks containing more than 1.25 billion records on individuals. Privacy Hearings, *supra* note 92, at 4. A more complete survey, conducted in 1975, revealed 3.8 billion records. Privacy Report, *supra* note 8, at 529 n.35.

Prior to the enactment of the Privacy Act, there were several important studies and congressional hearings on the subject of the federal government's information, collection, and recordkeeping practices, and, more specifically, the effect of those practices on public employees. The most important study enunciated five principles of fair information practices, emphasizing the need for data subjects to be aware of, and have some control over, information systems. See Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Dep't of Health, Education and Welfare, Records, Computers, and the Rights of Citizens 41 (1973). For earlier congressional hearings, see, e.g., *Right to Privacy of Federal Employees: Hearing on H.R. 1281 and Related Bills Before the Subcomm. on Retirement and Employee Benefits of the House Comm. on Post Office and Civil Service*, 93d Cong., 1st & 2d Sess. (1973-1974); *Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 92d Cong., 1st Sess. (1971).

100. A provision that would have made the Privacy Act applicable to private sector organizations was present in the original Senate version of the Act, S. 3418, 93d Cong., 2d Sess. § 201(a), reprinted in *Privacy Hearings*, *supra* note 92, at 357. S. Rep. No. 1183, 93d Cong., 2d Sess. 50, reprinted in [1974] U.S. Code Cong. & Ad. News 6932, 6932. The provision was deleted, however, because of the prevailing view that analysis and empirical study on this question had not been performed. See Privacy Hearings, *supra* note 99, at 31-32 (discussion among Rep. Koch, Rep. Goldwater, and Sen. Jackson), 40-41 (statement of Elliot L. Richardson), 72 (statement of Alan Westin). A subsequent legislative attempt to extend the requirements of the Privacy Act to the private sector was rejected. See H.R. 1984, 94th Cong., 1st Sess., 121 Cong. Rec. 1216 (1975); Note, *Let Industry Beware: A Survey of Privacy Legislation and its Potential Impact on Business*, 11 Tulsa L.J. 68, 76-81 (1975). The Privacy Commission also rejected the direct application of the Privacy Act to the private sector. Privacy Report, *supra* note 8, at 497-98. The Privacy Act is, however, applicable to government contractors. 5 U.S.C. § 552a(m) (1976). See generally Bedell, *Government Contractors, and the Initial Steps of the Privacy Act*, 34 Fed. B.J. 330, 330-33 (1975).

101. See Eastman, *supra* note 99, at 335. The Privacy Act has had a substantial influence on subsequent state privacy legislation covering government agencies. Compare 5 U.S.C. § 552a(e)(3)(B)-(D) (1976) with Ark. Stat. Ann. § 16-806(a)-(c) (Supp. 1975) and Minn. Stat. Ann. § 15.165(2)(a)-(c) (West Supp. 1978).

102. See 5 U.S.C. §§ 552a(b)(1)-(11) (1976) (disclosures permitted without consent for a "routine use," to Congress, or for statistical purpose), (j) (general exemptions from the Act's requirement for the Central Intelligence Agency and law enforcement agencies), (k) (exemptions from specific provisions, such as access, for investigatory law enforcement information and employment recommendations supplied by a third party who received an express promise of confidentiality). Even when a reasonable claim for information is made, the policy against



that: (1) agencies may maintain only "relevant and necessary" information in their records;<sup>103</sup> (2) agencies should endeavor to collect information directly from the subjects of the records rather than from third parties;<sup>104</sup> (3) when individuals are requested to supply information, they must be informed of the purpose of collection and the uses to which the information will be put;<sup>105</sup> (4) individuals must be afforded an opportunity to examine their files upon request;<sup>106</sup> (5) individuals may request amendment of a record,<sup>107</sup> and, if the agency disagrees with an amendment request, may file a statement of disagreement which must be noted in subsequent disclosures, and the amendment or statement of disagreement must be sent to prior recipients of the record;<sup>108</sup> (6) records about an individual should not be disclosed to third parties without his written consent<sup>109</sup> unless the disclosure is for a "routine use";<sup>110</sup> (7) a record of all disclosures made about an individual must be made

---

disclosure requires anyone seeking information to identify an appropriate exemption. In *Local 2047, Am. Fed'n of Gov't Employees v. Defense Gen. Supply Center*, 423 F. Supp. 481 (E.D. Va. 1976), *aff'd per curiam*, 573 F.2d 184 (4th Cir. 1978), the plaintiff, a labor organization representing federal government employees, sought to obtain certain information about its members pursuant to the terms of a collective bargaining agreement. The government asserted the Privacy Act as a defense. The court accepted this defense, noting that the information sought did not fall within the routine use exemption that allows disclosure, *id.* at 484, and that the purposes of the Privacy Act overrode the collective bargaining agreement. *Id.* at 485. The court suggested that the union obtain such information directly from its members. *Id.* at 486 n.4. Although the effect of this case was to inconvenience the union, it illustrates that the exemptions to the Privacy Act will not be loosely construed. *Accord*, *Mervin v. Bonfanti*, 410 F. Supp. 1205 (D.D.C. 1976) (in camera examination of certain performance evaluations ordered to determine if material was, in fact, confidential and thus exempt from disclosure requirements).

103. 5 U.S.C. § 552a(e)(1) (1976). This requirement is intended to force agencies to evaluate their need for particular types of information. An agency must first establish that the collection of an item of information is relevant to its statutory purpose. Then, it must be determined that the information is necessary because the agency's needs "cannot reasonably be met through alternative means." S. Rep. 1183, 93d Cong., 2d Sess. 46, *reprinted in* [1974] U.S. Code Cong. & Ad. News 6916, 6961; *see* Privacy Report, *supra* note 8, at §13. For a discussion of the application of the relevant and necessary standard to private employees, *see* pt. IV(B)(1)(b) *infra*.

104. 5 U.S.C. § 552a(e)(2) (1976).

105. *Id.* § 552a(e)(3). This provision applies to an individual supplying information about himself or a third party.

106. *Id.* § 552a(d)(1).

107. *Id.* § 552a(d)(2).

108. *Id.* § 552a(d)(3)-(4).

109. *Id.* § 552a(b); *see* *Local 2047, Am. Fed'n of Gov't Employees v. Defense Gen. Supply Center*, 423 F. Supp. 481, 483 (E.D. Va. 1976), *aff'd per curiam*, 573 F.2d 184 (4th Cir. 1978).

110. 5 U.S.C. § 552a(b)(3) (1976). A "routine use" is defined as the use of a record "for a purpose which is compatible with the purpose for which it was collected." *Id.* § 552a(a)(7). Authority to promulgate such "routine uses" is delegated to the agencies, and each agency must develop a list of the categories of users and the purpose of each use. *Id.* § 552a(e)(4)(D). A routine use would be disclosures by the Internal Revenue Service to parties with whom it is engaged in litigation, *Harper v. United States*, 423 F. Supp. 192, 198 (D.S.C. 1976), or, in some circumstances, the disclosure of the names of employees to labor unions, *Local 2047, Am. Fed'n of Gov't Employees v. Defense Gen. Supply Center*, 423 F. Supp. 481, 484 (E.D. Va. 1976), *aff'd per curiam*, 573 F.2d 184 (4th Cir. 1978). Such routine uses will, however, be narrowly construed. *See id.* at 486.

available to him upon request;<sup>111</sup> and (8) individuals may sue for damages and injunctive relief for violations of the above provisions.<sup>112</sup>

The Privacy Act's provisions for access, correction, and damages are similar to the provisions of the FCRA.<sup>113</sup> The other provisions of the Privacy Act, however, are broader and more encompassing. These requirements, in contrast to the specific focus of the FCRA, are phrased in general terms because they are designed to apply to a variety of agencies that have different needs and procedures. The exemptions to the Act provide for special treatment of particular agencies that may require it.<sup>114</sup>

The Privacy Act should not, of course, be made directly applicable to private employers because many of its provisions are concerned with the particular practices of federal agencies. For several reasons, however, the Privacy Act is an appropriate model for regulation of the private sector employer. Its general purpose is to elucidate principles of informational privacy that can be implemented by different agencies that do not necessarily share common information-gathering practices.<sup>115</sup> The Act further complements its general requirements with particularized exemptions. This approach allows the statute to have wide application, while isolating those situations in which the requirements would be unfair, unnecessary, or simply obstructive.<sup>116</sup> Any regulation of private sector employers must similarly take into account their differing practices in order to avoid unnecessary interference with the efficient operation of their businesses. An approach that couples general requirements with particular exemptions is a practical method of fairly implementing principles of privacy protection when specific practices cannot be isolated for regulation.

The Privacy Act is a more appropriate model than the FCRA because federal agencies perform functions analogous to those performed by private employers. The FCRA primarily regulates the dissemination of information by credit agencies whose very function is to supply information to others. The Privacy Act, however, imposes requirements on agencies that, like employers, make varied uses and disclosures of the information that they collect. Both employers and agencies use this information to make specific decisions about employees or for other business purposes. This distinction is crucial because certain requirements that are inappropriate to a supplier of information are desirable in regulating a decisionmaker. It would be unfair to require a credit agency to collect only relevant and necessary information because that would require the agency to make separate, and virtually impossible, determinations as to the needs of each user of a credit report.<sup>117</sup> An employer or government agency, however, is in a better position to assess its needs for information and

---

111. 5 U.S.C. § 552a(c)(3) (1976).

112. *Id.* § 552a(g)(1).

113. See notes 68, 71-73, 89 *supra* and accompanying text.

114. See note 102 *supra*.

115. See S. Rep. 1183, 93d Cong., 2d Sess. 14-15, reprinted in [1974] U.S. Code Cong. & Ad. News 6916, 6929-30.

116. See generally Davidson, *The Privacy Act of 1974—Exceptions and Exemptions*, 34 Fed. B.J. 323 (1975).

117. The FCRA contains no provision comparable to the necessary and relevant standard of the Privacy Act. See note 79 *supra* and accompanying text.

to promulgate standards for what is relevant and necessary for its purposes. It is relatively easy for an employer or government agency to make such a judgment because they both collect particular information that is necessary in order to make the specific decisions that regularly arise.

The Privacy Act also supplies a superior analytical framework to the FCRA for designing employee privacy legislation because it recognizes that the information process is comprised of the four distinct stages of collection, maintenance, use, and dissemination. At each stage, different types of privacy interests are implicated.<sup>118</sup> These interests are often ignored by the FCRA analysis, which is primarily concerned with the dissemination of information. Because an employee may be subjected to a wide variety of privacy invasions, it is imperative that the framework for analysis be as inclusive as possible.

### III. MODELS OF EMPLOYEE PRIVACY PROTECTION

Prior to 1977, there was a dearth of proposals concerning the protection of the privacy interests of private sector employees. Two recent studies, however, have suggested methods to protect these interests and have proposed far-reaching reforms. Because these models would certainly be influential in the consideration of any legislation in this area,<sup>119</sup> they must be carefully examined to determine their comprehensiveness in protecting the rights of employees.

#### A. *The Privacy Commission Approach*

The Privacy Protection Study Commission was established pursuant to the provisions of the Privacy Act to ascertain whether the principles and requirements of the Act should be applied to private sector organizations.<sup>120</sup> The Commission's report, issued in 1977, is a comprehensive study of the privacy issues raised by the recordkeeping relationships an individual maintains with various institutions, such as banks, insurance companies, credit card companies, and employers.<sup>121</sup> Rather than attempting to propose an omnibus solution to privacy problems in the private sector, the Commission chose to treat each relationship separately and to propose a model of rights and remedies for each type of relationship.<sup>122</sup>

Despite the specificity of many of its recommendations, the Commission's approach is based upon a broad conceptual framework. The central principle

---

118. See notes 14-23 *supra*.

119. Federal legislation incorporating many of the Privacy Commission's recommendations have already been introduced. See H.R. 10076, 95th Cong., 1st Sess., 123 Cong. Rec. H12,316 (daily ed. Nov. 11, 1977) (privacy protection for the subjects of credit, medical, tax, and education records); H.R. 434, 95th Cong., 1st Sess., 123 Cong. Rec. H192 (daily ed. Jan. 6, 1977) (prohibiting preemployment use of the polygraph test). Although H.R. 10076 includes many of the Privacy Commission's statutory proposals, it does not include those proposals that cover the employment relationship.

120. Pub. L. No. 93-579, § 5(b)(2), 88 Stat. 1906 (1974).

121. A "recordkeeping relationship" is one in which decisions concerning an individual are based upon information supplied either by the individual or a third party, such as a credit agency, and the information is maintained in a manual or computerized file. See generally Privacy Report, *supra* note 8, at 3-6.

122. *Id.* at 37-39.

of the analysis is "to strike a proper balance between the individual's personal privacy interests and society's information needs."<sup>123</sup> All of the specific recommendations ultimately flow from the Commission's perception of the proper application of this balancing principle. The Commission also identifies three broad policy objectives: (1) to minimize intrusiveness by creating "a proper balance between what an individual is expected to divulge to a record-keeping organization" and what information is actually necessary to conduct the relationship; (2) to maximize the fairness of decisions made on the basis of recorded information; and (3) to grant the subjects of records legitimate and enforceable expectations of confidentiality.<sup>124</sup>

### 1. Proposals for Expanding Employee Privacy Rights

The Privacy Commission enunciates eight general obligations of an employer to protect its employees' privacy. These obligations, which include limiting collection to relevant information, allowing employees access to their records, and limiting the dissemination of information about employees,<sup>125</sup> are similar to many of the general principles of privacy protection established by the Privacy Act.<sup>126</sup> Although the Commission's judgment that these obligations should govern privacy measures in the employment context is significant, it fails to provide more than a cursory analysis of how these principles would actually apply to the employment relationship, and offers few insights into the factors that were presumably considered in balancing the interests of employers and employees. Moreover, the Commission's specific recommendations are not always consistent with these eight general obligations. In some cases, therefore, it is difficult to determine which principles are actually governing the specific recommendations.

#### a. Intrusiveness

The Commission's first policy objective, to minimize intrusiveness, is the subject of three specific recommendations that would ban the use of certain techniques in collecting information. First, federal legislation should ban the use of the lie detector and other "truth-verification" equipment because they are unreliable and prevent individuals from exercising control over the information they divulge about themselves.<sup>127</sup> Second, the FCRA should be amended so as to prohibit the use of pretext interviews because an employment check should not be conducted as if it were a criminal investigation.<sup>128</sup> Finally, the Commission proposes that when an employer utilizes the services of a credit agency or other investigative firm to gather information about an

---

123. *Id.* at 3.

124. *Id.* at 14-15. The Commission points to the first amendment, law enforcement, and cost as values that must be balanced against the three broad policy objectives. *Id.* at 21-28, *see* pt. IV(A); *infra*; note 272 *infra*.

125. *Id.* at 237-38. The other obligations require employers to inform employees of the types and uses of records maintained about them, to adopt reasonable procedures for maintaining information, and to limit the use of information about employees within the company. *Id.*

126. *See* notes 102-12 *supra* and accompanying text.

127. Privacy Report, *supra* note 8, at 238-40; *see* notes 220-33 *infra* and accompanying text.

128. *Id.* at 240. The Commission also contends that such information can be obtained without resorting to concealment. *Id.*

employee, the employer should have a legal duty of reasonable care under the FCRA in the selection and use of these organizations.<sup>129</sup> Thus, an employer who had knowledge that a credit agency used prohibited practices, such as pretext interviews, would be liable for the credit agency's actions.<sup>130</sup>

Although these recommendations are worthwhile, they can be criticized as incomplete because they fail to discuss various techniques of collection that, though perhaps not part of a formal collection process, are nevertheless utilized by the employer. The Commission did not consider searches of an employee's desk or locker, as well as audio or video surveillance of an employee's actions or conversations. The emphasis on the collection of information during the job application process apparently caused the Commission to ignore other intrusive techniques that occur during the course of employment.<sup>131</sup>

The Commission can also be criticized because, although it proposes the prohibition of certain collection methods, it makes no effort to limit the extensiveness of an inquiry into matters that are legitimately within the scope of an employer's concern. Faced with the fact that some type of inquiry by an employer into an employee's medical history is appropriate, the Commission avoids the crucial question of the scope of such an inquiry by characterizing it as a "largely aesthetic" issue.<sup>132</sup> By so doing, the Commission contradicts its central principle of balancing what an individual should be required to divulge with what is required by the nature of the relationship. Its failure to examine this question also undermines its proposed general obligation that an employer collect only information that is relevant to specific decisions. An inquiry about an employee's heart condition for a job that entails substantial physical or mental stress is certainly relevant and appropriate. An inquiry concerning the same job as to whether the employee has ever contracted syphilis or had an abortion presents serious questions of relevance. To the employee faced with the latter questions, whether they are permitted or not is certainly more than an "aesthetic" issue.

#### b. Fairness

The recommendations that seek to maximize fairness in decisions based upon recorded information, the Commission's second broad policy objective, comprise the bulk of the employment proposals. The Commission proposes that employees should have rights of access and correction for most records,<sup>133</sup> and that the disclosure of certain records to other employees should be limited.<sup>134</sup> These rights, which are also incorporated in the Privacy Act,<sup>135</sup> are valuable and necessary.

---

129. *Id.* at 241.

130. *Id.*

131. The Commission also omits any discussion of the propriety of using personality tests which are used in a manner similar to lie detectors as preemployment screening devices. *See* notes 234-40 *supra* and accompanying text.

132. Privacy Report, *supra* note 8, at 238.

133. *Id.* at 253-65.

134. *Id.* at 265-67.

135. *See* notes 106-110 *supra* and accompanying text.

In seeking to maximize fairness, the Commission proposes limitations on the collection and use of arrest, conviction, and military records.<sup>136</sup> The primary criticism of this approach is not that the particular proposals are unwise, but rather that it fails to establish any general principles of fairness in the collection process. The focus on limiting only the collection of very specific items of information implies the approval of other areas of inquiry. A preferable approach, which would at the same time create a governing principle of collection encompassing all types of information, would be to recognize explicitly that fairness requires that only relevant and necessary information be collected.

### c. Confidentiality

Perhaps the most far-reaching of the Commission's proposals are those seeking to establish a general duty of the employer to safeguard the confidentiality of employee records in its possession, the Commission's third policy objective. These proposals, which require an employer to obtain the consent of an employee prior to making many disclosures,<sup>137</sup> recognize the need for the establishment of general principles from which appropriate exceptions can be made.<sup>138</sup> They properly grant the employee control over disclosures that affect him, such as sending letters of reference, but do not permit an employee to interfere with disclosures when the privacy interest is minimal, as for example when only directory information is involved, or when an employer is required by statute to disclose information about an employee.<sup>139</sup>

## 2. Implementation Strategy

Although the Commission makes wide-ranging proposals for the expansion of substantive employee privacy rights, the force of most proposals is largely negated by an implementation strategy that stresses voluntary adoption by employers of the suggested rights.<sup>140</sup> The Commission's primary rationale for this approach is that "absent collective bargaining, there is no general framework in the private sector which could accommodate disputes about recorded information."<sup>141</sup> The Commission reasoned that the lack of such a

---

136. Privacy Report, *supra* note 8, at 242-49.

137. The right of an individual to control the disclosure of information about himself is perhaps the most fundamental element of personal privacy. See note 273 *infra* and accompanying text.

138. This is also the Privacy Act's approach. See note 102 *supra* and accompanying text.

139. Other important exceptions proposed by the Commission include disclosures made pursuant to subpoenas and collective bargaining contracts. Privacy Report, *supra* note 8, at 273.

140. Of thirty-two specific recommendations, only seven suggest statutory provisions. *Id.* at 239-40, 241, 243, 250-51, 258. The Commission appeared to rely somewhat on the fact that some private employers are voluntarily implementing employee privacy rights. *Id.* at 233-34; see, e.g., Ewing & Lankenar, *IBM's Guidelines to Employee Privacy*, 54 Harv. Bus. Rev. 82 (Sept.-Oct. 1976). See also D. Ewing, *Freedom Inside the Organization* 133 (1977) (reliance on IBM's privacy guidelines); Metz, *Privacy Legislation: Yesterday, Today and Tomorrow*, 34 Fed. B.J. 311, 311 (1975). The American Civil Liberties Union has criticized the Commission's entire approach to the private sector by noting that the recommendations contain "general hortatory language extending rights without remedies." *Privacy in the U.S. Is an Illusion: Report*, 63 A.B.A. J. 1363, 1363 (1977).

141. Privacy Report, *supra* note 8, at 225.

framework within which employers could be compelled to meet their obligations would make it difficult to enforce any legislation governing employee records.<sup>142</sup>

The Commission established three general principles to determine the appropriate method of implementing its proposals: (1) incentives should be created for reform of privacy-invasive practices by granting record subjects a legal right to compel a recordkeeper to honor the subjects' substantive rights; (2) existing regulations, particularly the FCRA, should be used to implement recommendations; and (3) unnecessary costs should be avoided.<sup>143</sup> The Commission's emphasis on voluntary implementation is incompatible with its first principle of implementation that incentives should be created for reform. Absent the deterrent effect of a potential lawsuit to enforce rights, an employer has little incentive to comply with the Commission's recommendations. Furthermore, the third principle of implementation, that unnecessary costs should be avoided, would not be offended by an employee's right to bring suit because the primary costs of this new litigation would be borne by employers who fail to comply with the legislative standards. It is difficult to classify these costs as unnecessary.<sup>144</sup> The Commission's conclusion thus produces an internal inconsistency in the application of its own implementation alternatives.

An even more direct criticism can be made of the Commission's conclusion that legislation would be difficult to enforce. The experience with other legislation affecting the employment relationship, particularly the National Labor Relations Act,<sup>145</sup> and privacy legislation, such as the Privacy Act and the FCRA, presents a compelling argument that legislation is workable.<sup>146</sup> It would appear that the Commission's preference for a voluntary adoption strategy is designed to give employers time to adopt some of its more controversial proposals, and is not based on serious doctrinal opposition to the concept of employee privacy legislation.<sup>147</sup>

Although the Commission stresses voluntary implementation, it does endorse statutory enactment of some of its recommendations. These recommendations use the FCRA as a model "because it is the statute at the Federal level that deals most explicitly and comprehensively with privacy issues in the private sector."<sup>148</sup> By using the FCRA, the Commission is following its implementation principle of utilizing existing regulatory mechanisms wherever possible. This use of the FCRA, however, is misguided. The FCRA, which was designed to regulate a particular industry that disseminates

---

142. *Id.* at 232-33. A minority of the Commission disagreed with the voluntary approach. *Id.* at 233.

143. *Id.* at 30-31.

144. In explicating its principle of avoiding unnecessary cost, the Commission explicitly supported the view that additional costs may be imposed on noncomplying organizations. *Id.* at 31.

145. 29 U.S.C. §§ 151-168 (1970 & Supp. V 1975).

146. See notes 190, 208 *infra*.

147. "The Commission does, of course, recognize that a voluntary approach may not be effective." Privacy Report, *supra* note 8, at 232-33; see *id.* at 239-41.

148. *Id.* at 31.

information,<sup>149</sup> is stretched beyond recognition when it is used as an all-purpose private sector privacy statute. For example, the Commission proposes that the FCRA be amended to prohibit the collection of information about an individual from third parties through a pretext interview, justifying this approach as "a reasonable extension of the [FCRA's] goal of assuring that subjects of investigations are treated fairly."<sup>150</sup> This reasoning is faulty because the FCRA's specific goal is to ensure fairness in credit investigations, rather than fairness in all investigations. The FCRA, as a statute with a specific target, is ill-suited to the broad and varying practices of employers.<sup>151</sup>

The use of the FCRA to implement employee privacy rights would inhibit the development of a comprehensive legislative solution that would incorporate general principles of privacy law in the employment context. If the employment relationship is unique, as the Commission contends in justifying the reliance on voluntary adoption,<sup>152</sup> legislation should address itself to the specific needs of that relationship.

### B. *The Ewing Approach*

An ambitious proposal for the recognition of a wide range of employee rights has been advanced by Professor David Ewing of the Harvard Business School.<sup>153</sup> The central thesis of the Ewing model is that private sector employees should be afforded quasi-constitutional rights of speech, privacy, and due process.<sup>154</sup> The underlying justification for applying these constitutional principles to the private sector is that large corporations exert great control over the lives of their many employees and thus may be characterized as "minigovernments."<sup>155</sup> Ewing does not argue that the activities of large private sector employers constitute state action.<sup>156</sup> Rather, he constructs the

---

149. The FCRA's statement of findings specifically refers to the role of credit agencies, their role in commerce, and the need to regulate their activities to ensure privacy for the consumer. 15 U.S.C. § 1681(a)-(b) (1976).

150. Privacy Report, *supra* note 8, at 240.

151. See notes 91-92 *supra* and accompanying text.

152. Privacy Report, *supra* note 8, at 224-25, 232-33.

153. D. Ewing, *Freedom Inside The Organization* (1977) [hereinafter cited as Ewing Book]. Ewing has also published several articles that evaluate the attitudes of businessmen towards proposals for increasing employee rights. See Ewing, *What Business Thinks About Employee Rights*, 55 Harv. Bus. Rev. 81 (Sept.-Oct. 1977); Ewing, *Who Wants Employee Rights?*, 49 Harv. Bus. Rev. 22 (Nov.-Dec. 1971); Ewing, *Who Wants Corporate Democracy?*, 49 Harv. Bus. Rev. 12 (Sept.-Oct. 1971). For criticisms of Ewing's analysis, see Lynd, Book Review, 87 Yale L.J. 885 (1978); McLanahan, Book Review, 4 Employee Rel. L.J. 143 (1978).

154. "U.S. society is a paradox. The Constitution and Bill of Rights light up the sky over political campaigners, legislators, civic leaders, families, church people, and artists. But not so over employees. The employee sector of our civil liberties universe is more like a black hole, with rights so compacted, so imploded by the gravitational forces of legal tradition, that, like the giant black stars in the physical universe, light can scarcely escape." Ewing Book, *supra* note 153, at 5.

155. *Id.* at 11-16. The Privacy Commission also focused on the activities of the largest corporations. Privacy Report, *supra* note 8, at 224. Because Ewing relied so heavily on the analogy between large corporations and government, his list of quasi-constitutional rights may not be applicable to small- or medium-sized employers. The Privacy Commission's recommendations also may not be applicable to smaller employees. See *id.*

156. See notes 34-35 *supra* and accompanying text.



"minigovernment" principle to argue that large employers should be subject to requirements analogous to those imposed on actual governments by the Constitution, requirements that may be implemented either voluntarily, judicially, or by legislation.<sup>157</sup>

A key characteristic of Ewing's proposals is that they are based upon a survey polling the attitudes of executives, supervisors, and other managers.<sup>158</sup> Although this empirical basis has generated criticism of the model on the ground that its proposals are framed by the attitudes of management,<sup>159</sup> it can also be regarded as one of its chief strengths. The survey reveals a surprising receptiveness of management to employee privacy interests and rebuts the common presumption that business is unalterably opposed to privacy measures.<sup>160</sup>

### 1. Substantive Employee Privacy Rights

The core of Ewing's entire analysis is a proposed employee bill of rights.<sup>161</sup> In many respects, his privacy recommendations are similar to those of the Privacy Commission. Ewing proposes that the use of lie detectors be prohibited, that an employee have a right of access to most of the information in his file, that no information be disclosed about an employee without his consent,

157. Ewing Book, *supra* note 153, at 150, 198, 203.

158. See Ewing, *What Business Thinks About Employee Rights*, 55 Harv. Bus. Rev. 81 (Sept.-Oct. 1977); Ewing, *Who Wants Employee Rights?*, 49 Harv. Bus. Rev. 22 (Nov.-Dec. 1971); Ewing, *Who Wants Corporate Democracy?*, 49 Harv. Bus. Rev. 12 (Sept.-Oct. 1971).

159. Lynd, *supra* note 153, at 894. Ewing's concern with the effect of employee rights on business is illustrated by a chapter entitled "Are Employee Rights a Threat to Capitalism?" Ewing Book, *supra* note 153, at 61-73. Lynd's criticism of Ewing's managerial outlook loses some of its force after consideration of this chapter, in which Ewing makes the hardly management-oriented suggestion that "the rights of private ownership, while important, must be qualified." *Id.* at 61. This concept of ownership would require as an element of legal title that corporations be accountable to the general public. *Id.* at 61-65. Although Ewing's citation to Henry Ford as authority for this view does tempt one to infer, as Lynd does from the analysis generally, that Ewing is harkening back to the days when corporate paternalism was part of the battle against unionism, the emphasis on corporate accountability to society, rather than merely to individual employees, suggests that the criticism is facile. This is not to imply that Ewing is antimanagement. In fact, Ewing supports his argument on the ground that it is "not likely to threaten the capitalistic bottom line." *Id.* at 66-68.

160. The survey discovered that: (1) 94% of the businessmen surveyed favored a policy forbidding the external disclosure of information about an employee without his consent; (2) 87% favored granting employees access to files, except for confidential opinions or qualifications for promotion; and (3) 61% favored limiting the availability of nonjob-related information, such as the employee's financial condition and nonjob-related medical problems, to the personnel department, and that such information should be unavailable to work supervisors. Ewing, *What Business Thinks About Employee Rights*, 55 Harv. Bus. Rev. 81, 86 (Sept.-Oct. 1977).

Business interests have, of course, frequently objected to possible privacy legislation. See, e.g., Bagley, *supra* note 90, at 52 (discussing the vehement objections of Rockwell International, Forest Lawn, and TRW/Credit Data, among others, to a proposed California omnibus bill to protect privacy). Ewing's survey does not suggest that corporations will not continue to object, but rather that the attitudes of individual businessmen reveal that, whatever the corporate position, certain measures are not considered unreasonable by those who would be faced with administering them.

161. Ewing Book, *supra* note 153, at 144-51.

and that the availability of the information to other employees within the company be restricted.<sup>162</sup>

Although Ewing's analysis is generally less comprehensive than the Privacy Commission's, in certain areas the proposals are more extensive. In particular, Ewing considers the scope of objectionable techniques of collecting information to be much broader than did the Privacy Commission<sup>163</sup> and would limit the use of personality and general intelligence tests, as well as the lie detector.<sup>164</sup> Tests that measure narrowly defined skills would be permitted.<sup>165</sup> He also proposes that fourth amendment standards be applied to an employer's search of an employee's desk or personal office files.<sup>166</sup> These proposals provide a broader and more descriptive conception of the range of employee privacy interests than that provided by the Privacy Commission.

## 2. Implementation Strategy

Ewing's approach to implementation of the proposed substantive employee rights proceeds on three levels. First, he favors voluntary implementation of his proposed bill of rights.<sup>167</sup> Consistent with the use of constitutional principles throughout his analysis, Ewing also proposes various types of hearing procedures, such as company courts, advisory boards, ombudspople, and arbitration, to process complaints of violations of an employee's rights.<sup>168</sup> Ewing envisions the voluntary establishment of these forums, and that the particular forum chosen will depend on the employer's overall personnel procedures and his attitudes towards personal privacy.<sup>169</sup>

Finally, Ewing suggests that legal remedies ought to be available. The remedies, however, would be used only when the preferred voluntary methods fail.<sup>170</sup> The remedies suggested are threefold. Primary reliance is placed upon federal legislation<sup>171</sup> that he proposes which would reject the concept of terminability at will and replace it with a "law of abusive discharge."<sup>172</sup> This

---

162. *Id.* at 134-37. In making his proposals, Ewing relies heavily on the privacy guidelines instituted by IBM. *Id.* at 133. See generally Ewing & Lankenner, *IBM's Guidelines to Employee Privacy*, 54 Harv. Bus. Rev. 82 (Sept.-Oct. 1976).

163. The Privacy Commission's recommendations to minimize intrusiveness discussed only lie detectors, pretext interviews, and the use of credit agencies or other investigative firms. See notes 127-31 *supra* and accompanying text.

164. Ewing Book, *supra* note 153, at 135.

165. For example, Ewing would permit typing tests for secretaries and, for prospective magazine editors, a sample article to edit. *Id.*

166. *Id.*

167. Although he never offers an explanation for this view, his preference for voluntary rights for employees." (emphasis added), 198-99.

168. *Id.* at 157-60, 162-72.

169. "Due process does *not* have to be legal in the sense that it is enforced by the courts, arbitration agencies, or other outside authorities. It does *not* have to be the same in detail from one organization to another." *Id.* at 156-57.

170. *Id.* at 199.

171. *Id.* at 203.

172. *Id.* at 200-04. "Abusive discharge" and "unjust dismissal" are terms that describe the termination of an "at will" employee for reasons that should arguably provide the employee with a cause of action against his former employer. See Blades, *supra* note 1, at 1413; Summers, *supra* note 3.

would permit an employee who is discharged as a result of exercising, or seeking to exercise, the substantive rights proposed to sue his employer in an administrative tribunal for damages and reinstatement.<sup>173</sup> Second, Ewing proposes the federal chartering of corporations, with each corporation being required, as a precondition of incorporation, to adopt his employee bill of rights.<sup>174</sup> Third, in some extreme cases, a court could order an employer to change its practices when the employer's practices threaten continued violations of employee rights, such as where no efforts are made to adopt procedures to protect those rights.<sup>175</sup>

The advantage of the Ewing implementation strategy over that of the Privacy Commission is that, while encouraging employers to adopt voluntary procedures, it recognizes that a legal remedy may be necessary in some situations. Its weakness is that only the first legal remedy, the cause of action for "abusive discharge," grants individual relief to an employee. If an employer denies other rights to an employee, such as refusing to grant access to a personnel file or disclosing information without an employee's consent, and the voluntary procedures of company courts or advisory boards do not uphold the employee's right of access, the employee is left without legal recourse. An action for abusive discharge, while a proposal of major significance, simply does not cover the majority of situations where privacy rights may be violated but discharge is not threatened. This gap in Ewing's proposal can be traced to his failure to propose that the employee's rights be enacted into law.<sup>176</sup> An employee obviously cannot be given the right to sue when an employer has not violated any legal requirement.

Ewing's analysis, like that of the Privacy Commission, is basically a scheme of general rights with neither an effective method of compelling employer compliance nor a comprehensive remedy for employees when violations occur. Furthermore, the proposals are set forth without a sufficient analytical presentation to determine their validity.<sup>177</sup> Thus, a comprehensive theory of employee privacy that can justify judicial or legislative intervention is lacking. In addition to merely listing recommended employee rights, such a theory must analyze the interests of the employer as well as the employee, conceive of and explicate the range of practices that may violate privacy, and, taking into consideration existing privacy legislation, as well as other legislation affecting the employment relationship, suggest a scheme of rights and remedies that can protect against infringements of employee privacy.

---

173. Ewing Book, *supra* note 153, at 200, 206. Under Ewing's proposal, federal courts would hear only appeals. *Id.* at 206. A tort, rather than contract, measure of damages would be used to permit the awarding of punitive damages which would serve as a deterrent against especially egregious practices. *Id.* at 201-02.

174. *Id.* at 205-06.

175. *Id.* at 209-10.

176. Ewing does, however, suggest that a company's adoption of these rights might be made a prerequisite under a federal incorporation statute, a proposal that is not elaborated on. *See* note 174 *supra* and accompanying text.

177. Ewing does consider generally whether an employee bill of rights is a threat to employer's interests. Ewing Book, *supra* note 153, at 61-73. This consideration of employer interests is not presented, however, when the specific recommendations for employee privacy are set forth.

## IV. A PROPOSAL FOR LEGISLATION

As prior discussion has demonstrated, the privacy invasions that are characteristic of the employment relationship are generally not protected against by existing privacy law.<sup>178</sup> Protection against these invasions thus requires either a radical judicial reinterpretation of entrenched concepts, such as consent, publicity, and state action, or a legislative solution. The obvious legal obstacles to the former approach indicate that legislation is preferable.<sup>179</sup>

The power of Congress to protect the privacy rights of private sector employees cannot be seriously questioned. Numerous existing statutes affecting the employment relationship have been upheld as valid exercises of congressional power under the commerce clause.<sup>180</sup> The protection of privacy would also be a proper legislative objective. As the Eighth Circuit noted in upholding the constitutionality of the FCRA, the "statute supports and protects a significant personal right, the right to privacy."<sup>181</sup> The most serious

178. See pt. II *supra*.

179. Despite the Privacy Commission's failure to endorse legislation, some type of legislation governing privacy in the employment relationship is likely in the foreseeable future. See Murg & Maledon, *Privacy Legislation—Implications for Employers*, 3 Employee Rel. L.J. 168, 176 (1977); Note, *Let Industry Beware: A Survey of Privacy Legislation and its Potential Impact on Business*, 11 Tulsa L.J. 68, 69 (1975). See generally, Westin, *An Era of Regulation*, in *Privacy (A Summary of a Seminar on Privacy)* 47-49 (Council of State Governments ed. 1975).

Separate federal legislative treatment of the employment relationship will continue the trend, exemplified by the FCRA and the Buckley Amendment, to devise specific solutions to the privacy issues presented in particular areas of the private sector. The difficulty in drafting legislation that encompasses many recordkeeping relationships was a major reason why the Privacy Act was applied to neither state and local governments nor the private sector. See Sen. Rep. No. 1183, 93d Cong., 2d Sess. 19, reprinted in [1974] U.S. Code Cong. & Ad. News 6916, 6934.

180. See, e.g., *United States v. Darby*, 312 U.S. 100, 114-15 (1941) (upholding the wage and hour provisions of the Fair Labor Standards Act of 1938, ch. 676, §§ 1-19, 52 Stat. 1060 (current version at 29 U.S.C. §§ 201-219 (1970 & Supp. 1975) (amended 1977))); *NLRB v. Jones & Laughlin Steel Corp.*, 310 U.S. 1, 7 (1937) (upholding the National Labor Relations Act). The rights that Congress seeks to protect need not be commercial ones, but rather may specifically relate to the welfare of employees and may have a very indirect effect on interstate commerce. "[T]he post-*Jones & Laughlin* cases adopt a concept of causation so attenuated as to bring within the commerce power virtually all economic activity in the nation." Schwartz, *National League of Cities v. Usery—The Commerce Power and State Sovereignty Redivivus*, 46 Fordham L. Rev. 1115, 1120 (1978); see *Heart of Atlanta Motel, Inc. v. United States*, 379 U.S. 241, 255-57 (1964) (upholding legislation prohibiting discrimination in public accommodation on basis that motel's guests were engaged in interstate trips); *United States v. Darby*, 312 U.S. at 114-15 (upholding wage and hour regulations because Congress can prevent the flow in interstate commerce of "goods produced under substandard labor conditions"). Since the expansion of the commerce power in *Jones & Laughlin*, the only case to hold that Congress exceeded its commerce power has been *National League of Cities v. Usery*, 426 U.S. 833 (1976) (extension of minimum wage guidelines to state employees is a violation of state sovereignty).

181. *Millstone v. O'Hanlon Reports, Inc.*, 528 F.2d 829, 833 (8th Cir. 1976). Employers might contend that the various requirements imposed by privacy legislation would deprive them of their property rights without the due process required by the fifth amendment. Regulations of business to further the public welfare, however, have consistently been upheld as long as they are a rational exercise of legislative power. See, e.g., *California Bankers Ass'n v. Shultz*, 416 U.S. 21, 45-46 (1974); *Heart of Atlanta Motel, Inc. v. United States*, 379 U.S. 241, 258-60 (1964). The New Jersey Supreme Court upheld a statute prohibiting the use of lie detectors, noting that

challenge to legislation is not whether it will meet constitutional requirements, but whether it can strike a fair balance between the privacy interests of employees and the business interests of employers.

### A. *Interests of the Employer*

All regulation of business activities entails costs for the party that must adapt its practices to the legislated standards. Whether such costs outweigh the benefits to be derived from the regulation is a matter of balancing competing public policy values.<sup>182</sup> In the privacy area, the benefits to employees of eliminating privacy-invading practices include a greater sense of personal autonomy, better psychological health, facilitated personal development, and a context in which love, friendship, and trust are fostered.<sup>183</sup> The interests of employers that may foreseeably be affected by privacy legislation must also be considered in order to determine what practices can be proscribed without an unacceptably harsh impact.

#### 1. Monetary Costs of Compliance

The potential cost of privacy legislation to employers cannot be predicted with precision.<sup>184</sup> Although it is certain that privacy legislation would directly cause significant expenditures to some employers,<sup>185</sup> the key question is the acceptability of such costs relative to the benefits that will be conferred on employees.<sup>186</sup> The question is really threefold: (1) What types of costs can properly be attributed to privacy legislation? (2) How can those costs be justified? (3) What effect will specific statutory provisions have on costs?

Employers have argued that legislation would require prohibitively expensive modifications of their computer or manual data systems.<sup>187</sup> It has been noted, however, that the types of costs properly attributable to legislation are limited.<sup>188</sup> Expenditures for the protection of privacy—those seeking to ensure that only accurate, relevant, and timely information is collected, used, and disclosed—should not include the costs of ensuring the confidentiality of information maintained by an employer, because the latter is a cost of the

---

private property rights are not absolute and may be infringed upon if the particular statute reflects a reasonable balance between an employer's rights and an employee's interest in privacy. *State v. Community Distributions, Inc.*, 64 N.J. 479, 486, 317 A.2d 697, 698-99 (1974).

182. See Privacy Report, *supra* note 8, at 21-29; Greguras, *Informational Privacy and the Private Sector*, 11 Creighton L. Rev. 312, 313-15 (1977).

183. See note 41 *supra*.

184. See Ware, *Panel on Systems Cost and the Economic Impact of Implementing Privacy Legislation*, in *Privacy (A Summary of a Seminar on Privacy)* 40 (Council of State Governments ed. 1975) [hereinafter cited as *Economic Impact*].

185. *Id.*

186. Professor Ewing has concluded that implementing his proposals for employee constitutionalism will not threaten profits. Ewing Book, *supra* note 153, at 66-68.

187. See Privacy Hearings, *supra* note 92, at 525, 528, 667; Bagley, *supra* note 90, at 52. A contention that the cost burden of legislation violated the employer's due process rights would probably not present a formidable constitutional argument. Other statutes have withstood such an attack. See *California Bankers Ass'n v. Shultz*, 416 U.S. 21, 50 (1974); *Heart of Atlanta Motel, Inc. v. United States*, 379 U.S. 241, 260 (1964).

188. *Economic Impact*, *supra* note 184, at 41.

information system itself. As stated by Dr. Willis Ware, a member of the Privacy Commission:

Any information system should have safeguards against accidental or malicious damage or misuse of the information it contains, because its very existence indicates that it is relevant and critical to the appropriate functioning of the organization that maintains it. Thus, information system security should be charged to the basic purpose for which the system exists, even though the security measures contribute to protection of privacy. In systems with well-developed security measures, additional requirements for privacy protection are likely to be of modest cost. In systems with lax security, greater levels of expenditure obviously will be necessary.<sup>189</sup>

Thus, the cost of security must be distinguished from those costs imposed by establishing procedures for employee access to information and consent to disclosure, the true costs of privacy legislation.

The costs of implementing privacy legislation are also typically overestimated by including improvements in information systems that are only collateral to privacy protection, and by allowing an unnecessarily large margin for uncertain contingencies.<sup>190</sup> This point, and the above distinction between information system security and other privacy measures, convey the same general idea: true costs of privacy legislation are less than the total costs that an employer will incur as a result of such legislation.

Even if such a limited cost approach were utilized, the cost of implementing privacy legislation would still not be insignificant. Employers might be required to alter their personnel procedures and to hire privacy coordinators to handle requests for access and correction and to process consents to disclosure.<sup>191</sup> Although it is certainly possible to posit a level of cost that would render legislation an undue burden to employers and the economy as a whole, significant expenditures below this threshold can still be viewed broadly as a proper cost of protecting an important interest of society. The cost of environmental legislation,<sup>192</sup> for example, though not free from debate, represents a major investment for many companies, but is acceptable because the legislation protects important individual and societal interests in health and natural resources. The protection of privacy is also recognized as an important value in our society.<sup>193</sup> As technological innovations expand the capabilities for privacy invasion, the protection of this value will require some costly changes. These costs can be viewed as a proper way of regulating the undesired externalities of a developing technology.<sup>194</sup>

---

189. *Id.*

190. *Id.* The actual costs of implementing the Privacy Act were much less than had originally been expected. Privacy Report, *supra* note 8, at 500. The costs to educational institutions of implementing the Buckley Amendment have thus far proved to be reasonable. *Id.* at 418; Cudlipp, *The Family Educational Rights and Privacy Act Two Years Later*, 11 U. Rich. L. Rev. 33, 40 (1976).

191. See *Economic Impact*, *supra* note 184, at 42.

192. See *id.* at 40.

193. Congress has declared that "the right to privacy is a personal and fundamental right protected by the Constitution . . . ." Privacy Act of 1974, Pub. L. No. 93-579, § 2(a)(4), 88 Stat. 1896 (1974).

194. See *Economic Impact*, *supra* note 184, at 40. "Concededly most of the scientific endeavors of the recent past constitute advances and have aided measurably in the improvement of

Cost, although not an absolute barrier to legislation, should be considered in designing specific statutory provisions.<sup>195</sup> For example, provisions requiring notification before records are established or disclosed would be expensive.<sup>196</sup> Therefore, in the interest of minimizing costs, these rights could be limited.<sup>197</sup> On the other hand, provisions for employee access to records and rights of correction, though expensive to implement,<sup>198</sup> will ultimately benefit the employer by assisting it in ensuring the accuracy of its personnel information. Monetary costs of access procedures could be further offset by charging a reasonable fee to an employee who utilizes these procedures.<sup>199</sup> This would be a fair way of spreading the costs of legislation because an access request is not an indication that the employer has violated any of its employee's privacy rights. If correction of an employee's record is required, however, the cost should be borne by the employer because it is more likely to reflect improper recordkeeping procedures. Rather than simply accepting or rejecting particular employee rights because of cost, the employer's interest in minimizing expenses should be recognized and utilized as a factor in tailoring the specific requirements of each provision.

## 2. Security

Employers have a vital interest in maintaining the security of their businesses against theft by employees.<sup>200</sup> For retail stores, losses due to employee theft are substantially greater than those caused by shoplifting.<sup>201</sup> An employer has a definite need to obtain information that will enable it to make personnel decisions that will minimize the chances of theft.<sup>202</sup> As a result, employers often justify the use of lie detectors, investigatory reports, arrest and conviction records, and surveillance as a means of excluding a potential culprit from becoming an employee or discovering the commission of a theft by an employee.<sup>203</sup>

Given the unquestioned severity of the theft problem of many employers, privacy legislation should not require the employer to sacrifice security. In considering the intrusiveness of certain methods of collection, however, the

---

civilization. But some of these may become the artifacts of tyranny if their utilization is not stringently controlled." *United States v. Perkins*, 383 F. Supp. 922, 926 (N.D. Ohio 1974).

195. See *Economic Impact*, *supra* note 184, at 43; Bagley, *supra* note 90, at 51-52.

196. Bagley, *supra* note 90, at 51-52.

197. Under the Privacy Act, certain "routine uses" may be made without the consent of the record subject. 5 U.S.C. § 552a(b)(3) (1976), *discussed at* note 110 *supra* and accompanying text. The Buckley Amendment also permits an educational institution to disclose certain information without the consent of the parent or student. 20 U.S.C. § 1232g(b)(1) (1976).

198. See Swan, *Privacy and Record Keeping: Remedies for the Misuse of Accurate Information*, 54 N.C. L. Rev. 585, 605-06 & n.70 (1976).

199. Some existing statutes provide for similar charges. See Freedom of Information Act, 5 U.S.C. § 552(4)(A) (1970); FCRA, 15 U.S.C. § 1681j (1976).

200. See generally S. Astor, *supra* note 14.

201. U.S. Dep't of Commerce, Crimes Against Business 6 (1976). All levels of employees, from management to security, participate in such thefts. *Id.*; see S. Astor, *supra* note 14, at 12-13.

202. Indeed, employers may even be under pressure from insurance companies to adopt strict security measures. U.S. Dep't of Commerce, Crimes Against Business 7 (1976).

203. See S. Astor, *supra* note 14, at 65-66, 69-79, 89-101, 118-19.

availability of sufficient alternative methods that are less intrusive, though perhaps more costly,<sup>204</sup> should be determined. For example, most of the information obtained through the use of lie detector examinations can also be obtained by using investigatory reports and letters of reference.<sup>205</sup> An employer may be forced to sacrifice the use of certain methods, and may even be required to forego some of the specific information provided by particular methods, but he should not be expected to sacrifice security altogether.

### 3. Efficiency and Personnel Decisions

All employers have a general interest in operating their businesses efficiently. Reasonable measures that are designed to improve the functioning of a business and are not directed at individual employees should not ordinarily be prohibited. In *Thomas v. General Electric Co.*,<sup>206</sup> a company had taken motion pictures to study the layout of its plant and to monitor the movements of employees in performing their jobs. The court properly upheld this procedure against a claim of privacy invasion by pointing out its value to the company and the additional cost that would be entailed to use alternative methods of comparable value.<sup>207</sup> Prohibiting this procedure could unnecessarily interfere with an employer's efficiency. The enactment of legislation providing a subject with rights of access, correction, and control over disclosures, however, would not appear to diminish significantly the efficiency of an organization's operations. The experience under other privacy legislation is that the affected organizations have been able to adapt to the disruptions caused by the legislation with only minor impact.<sup>208</sup>

A related employer efficiency interest is the interest in having adequate

---

204. At this level, the relevant employer interest is cost rather than security. Tiffany's claims that it uses lie detectors rather than traditional background checks because they are cheaper (\$25 to \$40 for a lie detector exam and \$50 for a background check). Quindlen, *Polygraph Tests for Jobs: Truth and Consequences*, N.Y. Times, Aug. 19, 1977, at B1, col. 1. Compelling an employer to use alternative methods may thus result in increased costs "but in that regard it is not to be differentiated from the many costly regulatory business restrictions . . ." *State v. Community Distribs., Inc.*, 64 N.J. 479, 486, 317 A.2d 697, 700 (1974) (upholding statute prohibiting use of lie detectors in employment).

205. See Hermann, *Privacy, The Prospective Employee, and Employment Testing: The Need to Restrict Polygraph and Personality Testing*, 47 Wash. L. Rev. 73, 152 (1971); Comment, *Privacy: The Polygraph in Employment*, 30 Ark. L. Rev. 35, 40 (1976) [hereinafter cited as *The Polygraph in Employment*].

206. 207 F. Supp. 792 (W.D. Ky. 1962).

207. *Id.* at 793, 799.

208. Under the FCRA, a subject of a credit report has a right to learn the "nature and substance" of what is in his files and the sources of information. 15 U.S.C. § 1681g(a)(1)-(2) (1976). One large credit company that anticipated a "landslide" of such requests from persons who had been turned down for credit experienced only a 0.2% increase over the requests made prior to the enactment of the statute. A. Westin & M. Baker, *supra* note 21, at 137-38. Access requests made pursuant to the Privacy Act have also not been overwhelming. Privacy Report, *supra* note 8, at 508. Similarly, educational institutions have not been unduly burdened by the access requirements of the Buckley Amendment. *Id.* at 417. One advantage of increasing computerization is that access requests may be handled more easily. A. Westin & M. Baker, *supra* note 21, at 258.



information about employees to make intelligent personnel decisions.<sup>209</sup> A major bank has argued that unless personnel data is exempted from privacy legislation, "the process of selection and promotion of employees will be intimidated and hindered, resulting in a reduction of competence and productivity, and an increase in cost to be borne by the economy . . . ."<sup>210</sup> Privacy legislation, however, need not abrogate the employer's traditional discretion in personnel decisions. Instead, it should be designed to ensure that decisions are made on the basis of accurate, relevant, and timely information, with access to personnel information limited to those having a need to know.<sup>211</sup> In addition to promoting fairness in personnel decisionmaking, these objectives may further benefit the employer by improving the efficiency and correctness of personnel decisions.

### B. Framework

The following proposal will utilize as a framework for analysis the four distinct stages of the information process: collection, maintenance, use, and dissemination. This classification has the advantage of tracking the usual chronological flow of information and emphasizes the interrelatedness of the privacy interests arising at each level. The framework underscores that if a comprehensive solution is desired, isolated regulation of particular areas will probably be ineffective.

#### 1. Collection

The collection process encompasses two distinct issues: (1) whether certain methods used by employers to collect information are so violative of an employee's privacy that their use should be prohibited or limited; and (2) whether employers should be barred from collecting certain types of information that are irrelevant, confidential, or likely to be used unfairly in personnel or other decisions.

##### a. Methods of Collection

The collection of information about employees has developed into a sophisticated process in which the employer has a vast array of technological and psychological devices at its disposal. Methods of collection that unduly intrude upon the physical or mental privacy of individuals should be regulated. In considering whether the use of particular methods should be limited or prohibited, the values that underlie the constitutional and common law rights of privacy provide useful criteria.<sup>212</sup>

---

209. Cf. *Geary v. United States Steel Corp.*, 456 Pa. 171, 181, 319 A.2d 174, 179 (1974) (permitting at will employee to sue for wrongful termination could adversely affect the personnel process).

210. Privacy Hearings, *supra* note 92, at 528 (statement of Chase Manhattan Bank).

211. See pt. IV(B)(3)(a) *infra*.

212. "The character of the problems posed by psychological testing, the polygraph and electronic storage of personal data can better be grasped if seen in the perspective of the common law intrusion and disclosure cases." Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. Rev. 962, 1006 (1964). Several commentators have argued that, if the state action problem could be surmounted, the use of the lie detector can be viewed as a violation of the fourth and fifth amendments. See, e.g., Hermann, *supra* note 205, at 128-37;

The application form is, of course, a necessary device for gathering basic information about an employee. The simple process of completing an application for employment, considered apart from the particular types of questions asked,<sup>213</sup> does not reasonably implicate any personal privacy interests. Employers not only collect information directly from an employee, however, but also may gather information from third parties. The most common practice is to request reports from credit agencies that frequently are based upon interviews with friends, neighbors, and relatives.<sup>214</sup> The Privacy Commission has made the valid proposal that an employer be required to notify an employee of any such inquiry, whether the inquiry is conducted by the employer itself or by a credit agency.<sup>215</sup> An employer would also be required to notify an employee about the type of information that is sought and the collection techniques that will be utilized,<sup>216</sup> and would be charged with a legal duty of reasonable care in selecting a credit agency.<sup>217</sup> Such requirements recognize that if users of credit reports are held legally accountable, they may exert pressure on credit agencies to conduct their investigations with a minimum of intrusive practices.

The search of an employee's desk, personal files, or locker presents a more serious invasion of employee privacy. In considering the propriety of employer searches, a significant distinction can be made between an employee's files that are employment-related and his personal files or locker. In the former situation, the files are maintained for the employer's benefit and are unlikely to include personal information. Therefore, as Professor Ewing suggests, the search of property likely to contain work-related information, such as desks, should be permitted if a supervisor has an immediate need to find a particular item of information.<sup>218</sup> In the case of the employee's personal files or locker, however, an employer should not have a license to rummage through them

---

Markson, *A Reexamination of the Role of Lie Detectors in Labor Relations*, 22 Lab. L.J. 394, 400 (1971); *The Polygraph in Employment*, *supra* note 205, at 42-43. Constitutional privacy law has also been applied to personality testing. Hermann, *supra* note 205, at 128-37.

The present analysis does not attempt any direct application of common law and constitutional privacy law because of the many legal obstacles that are presented. See pt. II(A), (B) *supra*. They are employed by analogy, however, to reflect the present limits and concerns of privacy law. To the extent that cogent arguments can be made that lie detectors and other means of collection infringe upon interests similar to those protected by common law and constitutional privacy law, the public policy arguments for their legislative prohibition are strengthened. See Committee on Labor and Social Security Legislation, Association of the Bar of the City of New York, *The Polygraph in Employment: The Consequences of its Search for Truth*, 28 The Rec. 464, 475 (1973).

213. See pt. IV(B)(1)(b) *infra*.

214. Although the FCRA already regulates these reports, it provides insufficient regulation of the employer because it imposes only minimal requirements on a user of a credit report. See notes 67-76 *supra* and accompanying text.

215. Privacy Report, *supra* note 8, at 241.

216. *Id.* at 250.

217. *Id.* at 241. The value of these proposals is diminished because they leave intact the FCRA's exemptions from the general notice requirements those reports that are prepared for employment purposes when the subject has not specifically applied for the job. 15 U.S.C. § 1681d(a)(2) (1976).

218. See Ewing Book, *supra* note 153, at 135.

simply because they happen to be maintained on an employer's premises.<sup>219</sup> In all cases, searches of places that are not ordinarily the repository for work-related information should be forbidden. When criminal activity is suspected, an employer should be required to contact law enforcement authorities, who are bound to abide by the fourth amendment's prohibition against unreasonable searches and seizures.

The lie detector test is a common truth-verification device used by employers.<sup>220</sup> Although the accuracy of the test has been disputed,<sup>221</sup> the more important question is, assuming that the test is accurate in most cases, whether the widespread use of the lie detector presents such an impermissible affront to physical and mental dignity and privacy so as to warrant its regulation or prohibition.<sup>222</sup> The lie detector test is a broad review of an

---

219. See Craver, *supra* note 3, at 49 (1977). Professor Craver distinguishes searches of property located in a company container, such as a locker, and searches of property not so situated. He would permit regular searches of the first variety as long as an employer promulgated rules to govern the search. Other property could be searched if the employer had "probable cause to believe that relevant evidence [would] be uncovered." *Id.* (footnote omitted). Because a restriction on either type of search within the employer's premises will limit an employer's proprietary interest, a distinction based upon whether or not property is located in a company container seems unnecessary. A more appropriate classification is to distinguish between an employer's business interest in employment-related information and property, and an employee's privacy interest in personal information and property.

220. Approximately 200,000 private sector employees take lie detector tests each year. Committee on Federal Legislation, New York State Bar Association, *Polygraph Testing in Employment* (Oct. 1974), reprinted in 123 Cong. Rec. H1867 (daily ed. March 8, 1977) (remarks of Rep. Koch). The polygraph is composed of: (1) a corrugated rubber tube that is attached to the subject's chest to measure the respiratory rate; (2) an inflated rubber cuff attached to the arm that measures blood pressure and pulse rate; and (3) two electrodes attached to the hand that measure the flow of electric current (galvanic skin response) as the rate of perspiration increases. Comment, *The Polygraph in Private Industry: Regulation or Elimination?*, 15 Buffalo L. Rev. 655, 658 (1965).

New truth-verification devices continue to be developed. One such device is the Psychological Stress Evaluator (PSE), which measures stress in a person's voice. A recent "advance" in this device would allow an individual to be tested by telephone without his knowledge. *Telephone Voice Analyzer is Designed To Spot a Liar*, N.Y. Times, Feb. 20, 1978, at D1, col. 1. Another device detects lies by observing split-second facial expressions ("micromomentaries") which supposedly occur when a person tells a lie. The inventor stated that "[w]e know that a psychopath, a psychopathic liar, can beat a polygraph test. . . . But to the best of my knowledge, he can't beat this. . . ." [The inventor] has been besieged with requests from such diverse entities as Sears, Roebuck Corporation and the United States Treasury Department to teach his techniques. . . . "Teacher Says Videotape Detects Lies in Some Facial Expressions", N.Y. Times, Sept. 25, 1977, § 1, at 20, col. 4; see Craver, *supra* note 3, at 29-30.

221. Compare Lykken, *Polygraph Tests in Business Unscientific, Unamerican, Illegal*, 44 Hennepin Law. 4, 28 (May-June 1976) with Ansley, *Examiner Reviews Criticism by Psychologist*, 44 Hennepin Law. 5, 31 (May-June 1976). Some courts have also questioned its reliability. "[A]n innocent employee taking such a test could be risking loss of job and reputation at odds similar to those in Russian roulette." *Swope v. Florida Indus. Comm'n*, 159 So.2d 653, 654 (Fla. Dist. Ct. App. 1964); accord, *Livingston & Sons, Inc. v. Constance*, 115 Ohio App. 437, 438, 185 N.E.2d 655, 656 (1961).

222. Many states have passed statutes that restrict the use of the lie detector. Such statutes typically prohibit either requiring, demanding, requesting, suggesting, soliciting, influencing, subjecting, or causing a job applicant or employee to take a polygraph examination. The type of

employee's life under circumstances certain to produce anxiety, and its intrusive nature has been well-documented.<sup>223</sup> The use of the lie detector should be prohibited because it affects interests so closely akin to those which already receive protection under the common law and constitutional privacy rights.<sup>224</sup> The common law cause of action for intrusion protects against "the obtaining of . . . information by improperly intrusive means."<sup>225</sup> Similarly, under the fourth amendment, what an individual "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."<sup>226</sup> Under this standard, the lie detector test can be viewed as a search that "strips the subject bare" and "invade[s] objective expectations of privacy."<sup>227</sup>

The fifth amendment's privilege against self-incrimination provides a useful analogy in analyzing the interests invaded by the lie detector test. The

restriction is indicated parenthetically below. Alaska Stat. § 23.10.037 (1972) (request or suggestion); Cal. Lab. Code § 432.2 (West 1971) (requirement or demand); Conn. Gen. Stat. Ann. § 31-51g (West Supp. 1978) (requirement or request); Del. Code Ann. tit. 19, § 704 (1975) (requirement, request or suggestion); Hawaii Rev. Stat. § 378-21 to -22 (1976) (requirement); Idaho Code §§ 44-903 to -904 (1977) (requirement); Md. Ann. Code art. 100, § 95 (Supp. 1977) (requirement or demand); Mass. Ann. Laws ch. 149, § 19B (Michie/Law. Co-op 1976) (subject or request); Mich. Comp. Laws Ann. § 338.1726(1) (1976) (requirement); Minn. Stat. Ann. § 181.75 (West Supp. 1978) (requirement or solicit); Mont. Rev. Codes Ann. § 41-119 (Supp. 1977) (requirement); N.J. Stat. Ann. § 2A:170-90.1 (1971) (requirement, request, or influence); Or. Rev. Stat. §§ 659.225, .990(7) (1977) (requirement); 18 Pa. Cons. Stat. Ann. § 7321 (Purdon 1973) (requirement); R.I. Gen. Laws §§ 28-6.1-1 to .1-2 (1968) (requirement or subject); Wash. Rev. Code Ann. §§ 49.44.120-.130 (Supp. 1977) (requirement). The distinction between those states that prohibit "requesting" the employee to take the test and those that merely prohibit "requiring" such a test is significant. It has been held that an employer can request an employee to take a test when the statutory language only mentions "requiring". 43 Op. Cal. Att'y Gen. 25 (1964).

New York has recently passed a statute that prohibits the use of the PSE on applicants or employees. 1978 N.Y. Laws ch. 30 (to be codified in N.Y. Lab. Law §§ 733-739).

223. See, e.g., A. Westin, *Privacy and Freedom* 154, 239-40 (1967).

224. Most commentators agree with this conclusion. See, e.g., Privacy Report, *supra* note 8, at 239-40; Committee on Labor and Social Security Legislation, Association of the Bar of the City of New York, *The Polygraph in Employment: The Consequences of its Search for Truth*, 28 The Rec. 464, 465 (1973); Hermann, *supra* note 205, at 102; Markson, *A Reexamination of the Role of Lie Detectors in Labor Relations*, 22 Lab. L.J. 394, 406 (1971). Professor Craver would prohibit the preemployment use of lie detectors, but would permit its use in investigating employee defalcations in some cases. Craver, *supra* note 3, at 36-37. The constitutional analogy used herein is equally, if not more, applicable to the latter case because it is concerned with criminal contexts.

The employee's consent to the polygraph or other collection techniques, whether express or implied, or whether given out of the fear of losing employment, precludes direct application of the common law right of privacy. See note 54 *supra* and accompanying text. Nevertheless, the oft-cited element of coercion that is presented in gaining the employee's consent, see, e.g., *State v. Community Distributions, Inc.*, 64 N.J. 479, 484, 317 A.2d 697, 699 (1974); Hermann, *supra* note 205, at 77, underscores the need for a legislative remedy.

225. *Pearson v. Dodd*, 410 F.2d 701, 704 (D.C. Cir.), *cert. denied*, 395 U.S. 947 (1969). For an intrusion action analysis of the lie detector test, see *The Polygraph in Employment*, *supra* note 205, at 39-40.

226. *Katz v. United States*, 389 U.S. 347, 351-52 (1967). In *Katz*, the Court rejected the view that only tangible personal property is protected by the fourth amendment and found that an intrusion into a property interest is unnecessary. *Id.* at 353.

227. Hermann, *supra* note 205, at 135.

information elicited often includes prior convictions or criminal acts, such as drug use, theft, or sexual offenses.<sup>228</sup> The virtually compulsory extraction of such incriminating information by the physiological responses to the lie detector can be compared to methods that have been rejected under the fifth amendment.<sup>229</sup> Indeed, although the intrusion is perhaps not as shocking, the use of the lie detector is closer to the pumping of the defendant's stomach in *Rochin v. California*<sup>230</sup> that was found to be an unlawful forced confession<sup>231</sup> than to the fifth amendment's ideal of a voluntary and knowing confession under nonintimidating circumstances. Moreover, in *Schmerber v. California*,<sup>232</sup> the Court noted that the compulsory use of the lie detector yields the type of forced testimonial responses that are prohibited by the fifth amendment.<sup>233</sup>

The personality test is a similarly broad review of an employee's personal life. In sharp contrast to limited vocational tests that measure specific skills, such as typing,<sup>234</sup> the personality test measures emotional adjustment, social relations, motivation, and interests.<sup>235</sup> Obtaining such information through attitudinal responses can be considered a mental "search" for private facts.<sup>236</sup>

---

228. See S. Astor, *supra* note 14, at 74, 76.

229. Hermann, *supra* note 205, at 130.

230. 342 U.S. 165 (1952).

231. *Id.* at 172.

232. 384 U.S. 757 (1966).

233. "To compel a person to submit to testing in which an effort will be made to determine his guilt or innocence on the basis of physiological responses, whether willed or not, is to evoke the spirit and history of the Fifth Amendment." *Id.* at 764.

234. See Ewing Book, *supra* note 153, at 135.

235. Hermann, *supra* note 205, at 104. There are two types of personality tests. The first is an inventory test that provides an objective measure of the subject's interest in certain types of activities or of particular personality traits and is used to predict job performance. The Minnesota Multiphasic Personality Inventory (MMPI) is the best known type of inventory test. *Id.* at 104-06. The intimate facts sought by the MMPI are evidenced by the following questions which must be answered true or false "without thinking or deliberation."

"C. Questions relating to family matters and social life

"Some of my family have habits that bother and annoy me very much.

"I loved my father.

"My relatives are nearly all in sympathy with me.

"My parents often objected to the kind of people I went around with.

"D. Questions relating to sexual matters

"I am worried about sex matters.

"I wish I were not bothered by thoughts about sex.

"When a man is with a woman he is usually thinking about things related to her sex.

"There is something wrong with my sex organs." *Psychological Tests and Constitutional Rights: Hearings Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 89th Cong., 1st Sess. 169-70 (1965) [hereinafter cited as *Psychological Hearings*] (statement of Monroe Freedman).

The second type of personality test is projective. The most common, the Rorschach ink blot test, requires the subject to observe several types of ink blots and to describe what he sees in each. Hermann, *supra* note 205, at 106-07. See generally *id.* at 102-14. For a summary of objections to personality testing, see *Psychological Hearings*, *supra* at 187-89 (statement of A. Westin).

236. "Personality tests seek to ferret out a man's innermost thoughts on family life, religion,

Fifth amendment interests are implicated because personality tests ordinarily require testimonial self-incriminations, as illustrated by the question, "Have you engaged in any unusual sexual practices?"<sup>237</sup> In fact, the coercion, anxiety, and scope of interests affected by personality tests are almost identical to those affected by the lie detector. Its use, therefore, should be prohibited for the same reasons.<sup>238</sup> This proposal is buttressed by the fact that the fourth amendment requires that those methods of collecting information that are less likely to invade privacy should be used before more intrusive methods are employed.<sup>239</sup> Applied to the employment context, the availability of application forms, letters of reference, interviews, and physical examinations suggest that the more intrusive lie detector and personality tests should not be permitted.<sup>240</sup>

Fingerprinting, blood tests, physical examinations, and surveillance of work areas<sup>241</sup> can be distinguished from lie detector and personality tests because their scope of inquiry is not as broad. Fingerprinting, for example, is "only a means of verifying the required information" and "involves no additional intrusion."<sup>242</sup> The Court in *Schmerber v. United States*<sup>243</sup> distinguished blood tests, fingerprinting, and photographing from lie detectors because they are more closely akin to the gathering of evidence than to the compulsory extraction of incriminating testimony.<sup>244</sup> This distinction is equally applicable to the employment context. An employer should be permitted to gather facts through the use of methods of accepted reliability that seek to discover specific facts. A routine physical examination or blood test is

racial attitudes, national origin, politics, atheism, ideology, sex, and the like." *Osborn v. United States*, 385 U.S. 323, 342 (1966) (Douglas, J., dissenting) (footnote omitted).

237. *Psychological Hearings*, *supra* note 274, at 176-77.

238. See Hermann, *supra* note 205, at 128-37 (analyzing both lie detector and personality tests under the standards of constitutional privacy law).

239. See, e.g., *Stanley v. Georgia*, 394 U.S. 557, 569-72 (Stewart, J., concurring) (1969).

240. Hermann, *supra* note 205, at 152; *The Polygraph in Employment*, *supra* note 205, at 40.

241. These methods have all been upheld as valid methods of collection. See *Division 241, Amalgamated Transit Union v. Suscy*, 538 F.2d 1264 (7th Cir.), *cert. denied*, 429 U.S. 1029 (1976) (rules requiring blood and urine tests for public bus drivers after any serious accident or suspicion of intoxication is not a violation of the fourth amendment because the state had a reasonable objective in furthering public safety and the actual conditions and the manner of the intrusion were not unreasonable); *Thom v. New York Stock Exchange*, 306 F. Supp. 1002 (S.D.N.Y. 1969) (statute requiring fingerprinting of stock exchange workers held constitutional as valid exercise of police power in combatting theft in the securities industry), *aff'd per curiam sub nom. Miller v. New York Stock Exchange*, 425 F.2d 1074 (2d Cir.), *cert. denied*, 398 U.S. 905 (1970); *Thomas v. General Elec. Co.*, 207 F. Supp. 792 (W.D. Ky. 1962) (taking motion pictures of employees by an employer does not violate the employees' right to privacy when the purpose was to study manufacturing methods and processes); *Pitcher v. Iberia Parish School Board*, 280 So.2d 603, 607-08 (La. Ct. App. 1973) (requirement that public schoolteacher submit to annual physical examination is a reasonable interference with the right to privacy), *cert. denied*, 416 U.S. 904 (1974).

242. *Thom v. New York Stock Exchange*, 306 F. Supp. 1002, 1009 (S.D.N.Y. 1969), *aff'd per curiam sub nom. Miller v. New York Stock Exchange*, 425 F.2d 1074 (2d Cir.), *cert. denied*, 398 U.S. 905 (1970).

243. 384 U.S. 757 (1966).

244. *Id.* at 764.

so commonplace that it can be considered neither an offensive prying nor an invasion of any reasonable expectation of privacy.<sup>245</sup> The photographing of employees in work areas can be a reasonable method for an employer to improve efficiency, and it only records what is already open to public view.<sup>246</sup>

The objective of prohibiting or regulating the use of certain methods of collection is to prevent the collection process from becoming an intimidating ordeal. A job applicant or employee should not be required to bare his innermost thoughts by submitting to methods that produce anxiety and humiliation in an atmosphere of criminal-like interrogation. An employee's personal property should not be open to employer searches merely because an employer suspects wrongdoing. Furthermore, an employer should not be permitted to conduct surreptitious background investigations by interviewing an individual's close friends and relations. Requiring that the subject at least be notified of such an investigation would seem a minimal protection that would not be burdensome to employers. Absent legislation, many employees may continue to be subjected to an inquisitorial process of collection from which even criminals are protected by constitutional guarantees.

#### b. Types of Information

Limiting the types of information that an employer may collect requires the establishment of two separate standards. The first should require that all information collected be relevant to the purpose for which it is gathered. The second should establish criteria for excluding specific types of personal facts which, though relevant, are either so private that they ought to be beyond the scope of inquiry, or are so prejudicial that they would be unfairly used in making an employment decision. These facts would be deemed relevant but unnecessary.

A relevance standard is already incorporated into the Privacy Act,<sup>247</sup> and its extension to other contexts has already been proposed.<sup>248</sup> This standard would prohibit the collection of information about political beliefs or sexual preference. Obsolete information, which is regulated by the FCRA,<sup>249</sup> should also be deemed irrelevant.<sup>250</sup> The judicial concept of job-relatedness<sup>251</sup> and

---

245. See *Breithaupt v. Abram*, 352 U.S. 432, 439 (1957).

246. Under the common law action for public disclosure of private facts, for example, whatever an individual voluntarily exposes to the public may be lawfully observed, and photographs may be taken and disseminated. See, e.g., *Gill v. Hearst Publishing Co.*, 40 Cal.2d 224, 230, 253 P.2d 441, 444-45 (1953).

247. 5 U.S.C. § 552a(e)(1) (1976).

248. See Roscoe Pound-American Trial Lawyers Foundation, *Privacy in a Free Society* 30 (1974) [hereinafter cited as *Roscoe Pound*] (proposing extension of relevancy standard throughout the private sector); Hayden, *How Much Does the Boss Need to Know?*, 3 Civ. Lib. Rev. 23, 26 (Aug.-Sept. 1976) (proposing relevancy standard under the FCRA).

249. 15 U.S.C. § 1681c (1976), discussed at notes 74-75 *supra* and accompanying text.

250. The FCRA does not include any relevancy standard. If an item does not fall within the specific terms of the obsolete information section, the credit agency has a right to report the information, regardless of its relevance. *Herring v. Retail Credit Co.*, 266 S.C. 455, 456, 224 S.E.2d 663, 664 (1976); see note 79 *supra*. The proposed standard would not attempt to list specific matters that would be deemed irrelevant, but would have the determination to judicial decision. Like the Privacy Act's treatment of relevancy, specific exceptions could be made. 5 U.S.C. § 552a(k) (1976), discussed at note 102 *supra* and accompanying text.

251. See Craver, *supra* note 3, at 42 n.197.

the requirement that questions be as specific as possible should also govern the relevancy inquiry.<sup>252</sup>

A more difficult question is presented when relevant information is sought to be excluded. The value of relevant information to an employer in making decisions must be assumed. Establishing criteria for determining what inquiries ought to be proscribed in order to protect privacy interests is difficult because different individuals will deem different types of information to be confidential. Allowing each applicant or employee to determine what types of questions he can be asked would be an unpredictable and unworkable restriction on an employer. Therefore, any legislative restriction of inquiries into specific areas should require that the information withheld be: (1) matters deemed to be private by a reasonable man (an objective standard of privacy); and (2) matters that could be used unfairly in making personnel decisions. Existing statutes that restrict the collection of records of prior arrests not resulting in conviction satisfy these criteria.<sup>253</sup> The first criterion is met because the ordinary man seeking employment would certainly prefer to keep such facts private. The second criterion of fairness is satisfied because arrest records should not be used as evidence of guilt.<sup>254</sup>

An employer's present discretion in selecting the types of information that it will collect may result in an overbroad disclosure of personal facts, political beliefs, and associations.<sup>255</sup> By limiting an employer's inquiry into those matters that are relevant and necessary, the interests of an employer in gathering needed information are recognized without permitting an employer the right to delve into every matter of an employee's life.<sup>256</sup>

---

252. Employers are already prohibited from inquiring into irrelevant matters that could be the basis of discrimination. See, e.g., Or. Rev. Stat. § 659.030 (1977); 32 Op. Att'y Gen. Or. 17-18 (1964) (prohibiting an employer's inquiry into race, religion, color, or national origin). But see *Spencer v. Toussaint*, 408 F. Supp. 1067, 1074 (E.D. Mich. 1976) (no privacy invasion by inquiring about psychological history on application form).

253. See, e.g., Cal. Lab. Code § 432.7 (West Supp. 1978); Md. Ann. Code art. 27, § 740 (1976). See also Privacy Report, *supra* note 8, at 243.

254. Limiting collection of information about past indiscretions, such as infrequent use of soft drugs, is subject to a similar type of analysis. The argument against such a limitation is that the principle of forgiveness has traditionally been an exception to a more fundamental principle of personal responsibility. Therefore, the argument runs, the employer should have the right to know such facts in order to treat individuals according to their deeds or misdeeds. A. Westin & M. Baker, *supra* note 21, at 267-68. This argument does not take into account the unfairness that may result by allowing an employer to base decisions on these matters. In *Roberts v. Civil Service Bd.*, 75 Mich. App. 654, 255 N.W.2d 724 (1977), the court, in reinstating a policeman who had been discharged for smoking marijuana, stated that "[w]ere we to similarly treat others who, if known, have on occasion in their youth smoked marijuana, illegally drank liquor, . . . engaged in an illegal Saturday night poker game, or even participated in an illegal lottery, the ranks of the police force and other important public service groups might well be significantly reduced." *Id.* at 657, 255 N.W.2d at 726. But see *Peller v. Retail Credit Co.*, 359 F. Supp. 1235 (N.D. Ga. 1973), *aff'd mem.*, 505 F.2d 733 (5th Cir. 1974); *Goodnough v. Alexander's, Inc.*, 82 Misc. 2d 662, 370 N.Y.S.2d 388 (Sup. Ct. 1975), discussed at notes 78-86 *supra* and accompanying text.

255. At the constitutional level, the compelled disclosure of organization membership violates the first amendment right of freedom of association. See *NAACP v. Alabama*, 357 U.S. 449, 462-66 (1958).

256. See *American Fed'n of Gov't Employees Local 421 v. Schlesinger*, 443 F. Supp. 431, 434 (D.D.C. 1978) (questionnaire sent to government employees requiring disclosure of "religious,



## 2. Maintenance

The maintenance of records involves procedures for storing and retrieving personal information. From a privacy perspective, the focus is on designing adequate safeguards to protect the confidentiality<sup>257</sup> and integrity of the information maintained in an employer's recordkeeping system. Legislation should require employers to adopt reasonable procedures to ensure the security of records.<sup>258</sup> If an individual suffers an "adverse effect," as, for example, when a third party gains access to private information, civil remedies should be provided.<sup>259</sup>

Another proposal that has been made for regulating the maintenance of records would require an employer to purge his files of information after a specified number of years have passed.<sup>260</sup> This limitation, however, would be costly and unnecessary. As long as an employee is granted access to his file and exercises his right to correct or supplement it,<sup>261</sup> he will be protected against the use of obsolete information. Requiring an employer to keep track of the length of time that many different types of information are maintained and then to purge it would be an unnecessary inconvenience and expense, particularly when provisions for access and limits on dissemination of information are provided.

## 3. Use

After an employer has collected and incorporated information into an employee's file, internal use of the information begins. The scope of the use category is the flow of information within an organization for various purposes, such as performance evaluations or determinations of eligibility for fringe benefits. The use category consists of two related but analytically distinct acts: (1) the disclosure of information to various individuals; and (2) the decisions made on the basis of that information.

### a. Disclosure

The internal disclosure of information in an employee's file to the personnel department, the payroll department, or supervisory personnel is necessary for

---

social, political, educational, and fraternal associations" unconstitutionally abridges right of free association).

257. Confidentiality is to be distinguished from privacy. "*Privacy* . . . is independent of technological safeguards; it involves the social policy issues of what information should be collected at all and how much information should be assembled in one information system. *Confidentiality* is the central issue for which technological safeguards are relevant. Where an organization has promised those from whom it collects information that unauthorized uses will not be made . . . making good that promise of confidentiality requires record security controls in both manual and computerized files." A. Westin & M. Baker, *supra* note 21, at 393.

258. The Privacy Act requires that agencies establish "appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity" 5 U.S.C. § 552a(e)(10) (1976). Agencies also must promulgate "rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records" *Id.* § 552a(e)(9).

259. *See id.* §§ 552a(g)(1)(D), (g)(4) (damage action for failure to comply with any provision that results in an "adverse effect on an individual").

260. *See* Roscoe Pound, *supra* note 248, at 31.

261. *See* notes 268-69 *infra* and accompanying text.

a business to make its various decisions intelligently. Nevertheless, not all personnel who need to review particular information about an employee should have access to his entire file. It is simply unnecessary for a supervisor preparing a performance evaluation to have access to information concerning an employee's medical problems and financial history. Similarly, it is unnecessary for the administrator of a fringe benefit program, such as health or life insurance, to see an employee's performance evaluations.<sup>262</sup>

Preventing such improper internal disclosures can be achieved by requiring that disclosures be permitted only if made for a "routine use" to designated personnel having a need to know particular items of information. Each employer should establish "routine uses" for every type of information that is either collected, such as financial information, or generated, such as performance evaluations. The acceptability of each routine use would be judged according to whether it is compatible with the purpose for which the information was collected.<sup>263</sup> For example, routine uses for a performance evaluation would include decisions about promotions, raises, or discharge. Routine uses for medical information would include decisions about hiring and employee medical and life insurance plans. In manual labor jobs, specific medical facts, such as physical strength, might be continually reexamined and used to determine an employee's fitness for a particular job.

After determining what information can be utilized in making a particular decision, an employer should designate those individuals who should be granted access to particular information based on their "need to know."<sup>264</sup> A foreman and the manager or committee responsible for raises and promotions might be given access to performance evaluations. The administrator of various company insurance programs and the company doctor would have access to medical information.<sup>265</sup> Limiting access to information based on a "need to know" would not hinder the efficiency of an employer's operations, and yet would provide an employee with valuable protection against indiscriminate disclosures within the company.

#### b. Decisionmaking

The second level of internal uses focuses on the decisions made on the basis of information maintained by an employer. Although the first level is concerned only with the fact of disclosure, the second considers whether it is an

---

262. The Privacy Commission observed that "so long as there are no absolute barriers to an employer's use of its employee medical and insurance claims records . . . a privacy problem of potentially major proportions exists." Privacy Report, *supra* note 8, at 229. An employee presently has no right to prevent such disclosures, assuming he is even aware that they might occur, because he lacks a property interest in the records which are owned by his employer. *Cf. United States v. Miller*, 425 U.S. 435, 440-41 (1976) (bank depositor has no property interest in records about him that are maintained by a bank).

263. This definition is taken from the Privacy Act, 5 U.S.C. § 552a(a)(7) (1976), discussed at note 110 *supra* and accompanying text. The Privacy Commission has endorsed the application of the routine use principle to internal disclosures by federal agencies. Privacy Report, *supra* note 8, at 519.

264. See Privacy Report, *supra* note 8, at 265.

265. In Connecticut, arrest record information is only available to personnel department employees. Conn. Gen. Stat. Ann. § 31-51i (West 1972).

invasion of privacy for employment decisions to be made as a result of inaccurate, incomplete, or irrelevant facts. It is at this level that the interests of the employer in making employment decisions are paramount. An employee could be allowed redress for decisions made on the basis of inaccurate information or information that a particular individual had no right to see, but the possibility of disgruntled employees challenging every decision that affects them under such a provision is both real and unacceptable.<sup>266</sup> This would potentially bring almost all employment decisions under judicial scrutiny.<sup>267</sup>

A more moderate alternative, which has the same goal of preventing unfair decisions, is to grant an employee the right of access to his file for the purpose of making corrections or supplementations.<sup>268</sup> It would be the employee's responsibility to exercise this right of access. If he fails to do so and a decision about him is based on inaccurate, incomplete, or irrelevant facts, he would be precluded from directly challenging his employer's decisions. Exemptions to employee access could be provided for information that was supplied by third parties under an express or implied promise of confidentiality.<sup>269</sup> Existing statutory access provisions have thus far not produced the deluge of requests that were predicted by opponents.<sup>270</sup> Access, therefore, is a workable procedure that will enable employees to protect their interests in fair decisionmaking without actually subjecting those decisions to constant outside scrutiny.

#### 4. Dissemination

Dissemination refers to the disclosure of information about an employee to people or agencies outside the employment relationship. Internal use of

---

266. See Summers, *supra* note 3, at 524.

267. Nevertheless, a cause of action for the employee should be permitted when improper information practices are a factor in his discharge. See pt. IV(C)(2) *infra*. Some state statutes regulate specific employment decisions when they may unfairly invade a privacy interest of the employee. See, e.g., Mich. Comp. Laws Ann. § 338.1726(1)-(2) (1976) (employee cannot be discharged solely because of the results of a polygraph test); N.Y. Correc. Law § 752 (McKinney Supp. 1977) (employment cannot be denied on the ground that an applicant has been convicted of a criminal offense unless there is a direct relationship between the offense and the employment sought, or if an unreasonable risk to safety or property would result). For an application of the Michigan statute, see *Roberts v. Civil Service Bd.*, 75 Mich. App. 654, 658-60, 255 N.W.2d 724, 726-27 (1977).

268. See Cal. Lab. Code § 1198.5 (West Supp. 1978); Me. Rev. Stat. tit. 5, § 638 (Supp. 1977). Courts have not been receptive to nonstatutory access requests based on a privacy interest. In *Gotkin v. Miller*, 379 F. Supp. 859 (E.D.N.Y. 1974), *aff'd*, 514 F.2d 125 (2d Cir. 1975), a former mental patient sought access to her medical records on the basis of a right to privacy under the ninth amendment. The court not only refused access, but had difficulty in conceiving how a privacy interest could be involved when no disclosure of the records was threatened. *Id.* at 863-64. This reflects the prevailing judicial interpretation of privacy as threatened by disclosure but not recognizing the importance of the right of access. See A. Westin & M. Baker, *supra* note 21, at 19; Roscoe Pound, *supra* note 248, at 34.

269. Personal references would be the most common example. See Privacy Act, 5 U.S.C. § 552a(k)(5) (1976); Cal. Lab. Code § 1198.5 (West Supp. 1978). When an employee requests access to particular information and an employer claims that the information is exempt, the court should have the power to examine the records in camera to determine whether they should be released. See *Mervin v. Bonfanti*, 410 F. Supp. 1205, 1207 (D.D.C. 1976); 5 U.S.C. § 552a(g)(3)(A) (1976).

270. See note 208 *supra*.

information about an employee is generally a necessary function of conducting a business because it relates to promotions, reassignments, and work performance of an employee. Although employees will be affected by these internal uses, the primary purpose is to benefit the employer by having people perform work most suited to their abilities. External disclosures, however, are ordinarily discretionary<sup>271</sup> and primarily affect the life of the employee rather than the operation of the business. They frequently take the form of references for an employee seeking a new job or of data that is disclosed to credit agencies. The adverse effect of a negative dissemination may continue for many years.<sup>272</sup>

The right to control knowledge about oneself is probably the most frequently cited central principle of privacy.<sup>273</sup> The most effective change in the law would be to recognize this principle and grant an employee a legal right of control over disclosures of personal information by his employer.<sup>274</sup> The legal

271. Nondiscretionary disclosures include responses to legal process, such as subpoenas, and the reports required by numerous government regulations. See generally Murg & Maledon, *Privacy Legislation—Implications for Employers*, 3 Employee Rel. L.J. 168, 169-70 (1977).

272. See notes 78-86 *supra* and accompanying text. The Privacy Commission aptly summarized the state of privacy law with respect to the disclosure of information about employees when it stated that "[t]he confidentiality of [employee] records is maintained today solely at the discretion of the employer and can be transgressed at any time . . . ." Privacy Report, *supra* note 8, at 269.

In nonemployment contexts, the subjects of records kept by others have generally been unsuccessful in asserting a legal interest in those records. In *United States v. Miller*, 425 U.S. 435 (1976), the Court denied the subject a right to prevent disclosure because of his lack of a property interest in records. *Id.* at 440-41. An alternative method of deciding the case might have been to emphasize that since *Katz v. United States*, 329 U.S. 347 (1967), fourth amendment protection has not rested exclusively on property interests.

Prior to *Miller*, a depositor traditionally had some legal expectation of confidentiality in communications with his bank. Note, *Bank Recordkeeping and the Customer's Expectation of Confidentiality*, 26 Cath. L. Rev. 89, 93-94 (1976); see *Shapiro v. Chase Manhattan Bank*, 84 Misc. 2d 938, 941-43, 376 N.Y.S.2d 365, 369-70 (Sup. Ct. 1975), appeal dismissed, 53 A.D.2d 542, 384 N.Y.S.2d 795 (1976). Since the decision in *Miller*, however, a depositor has no right to prevent the disclosure of his bank records. See *United States v. Blackwood*, Nos. 78-1358 to 1360, slip op. at 4 (10th Cir. Aug. 28, 1978).

273. See, e.g., Note, *The Massachusetts Right of Privacy Statute: Decoy or Ugly Duckling?*, 9 Suffolk L. Rev. 1248, 1258 n.41 (1975).

274. One commentator has stated: "In developed societies, the only way a person may be given the complete measure of both the sense and the fact of control is through a legal title to control . . . . Privacy is more than an absence of information abroad about ourselves; it encompasses a feeling of security in being able to control that information. By using the impersonal, public and ultimate institution of law to grant persons this control, at once the right to control is put far beyond question and at the same time indicates how seriously that right is taken." Pipe, *Privacy: Establishing Restrictions on Government Inquiry*, 18 Am. U. L. Rev. 516, 519 (1969).

Limitations on the employer's right to communicate truthful information about an employee to third parties might be challenged as a violation of the employer's right of free speech. See Privacy Report, *supra* note 8, at 21-24; Greguras, *Informational Privacy and the Private Sector*, 11 Creighton L. Rev. 312, 313-14 (1977). Although the Buckley Amendment contains a similar limitation on disclosure, 20 U.S.C. § 1232g(b)(1) (1976), the Supreme Court has not been called upon to determine its constitutionality. A relevant consideration in this determination is whether most employer disclosures about employees are properly classified as "commercial speech." Although this is an uncertain proposition because most commercial speech cases have dealt with

principle underlying a right of control is the "expectation of privacy" that an employee has in the records maintained about him by an employer.<sup>275</sup> An employee, relying on such an expectation, should be able to assume that the information collected about him by his employer will be used only within the employing organization.<sup>276</sup> This expectation should form the basis for a statutory requirement of employee consent to external disclosures.<sup>277</sup>

An employee's right to control disseminations should be qualified to permit an employer to make disclosures without consent when an employer has established routine uses for certain types of information and has informed employees of those uses at the time that the relevant information is col-

---

advertising, one commentator has asserted that employer references can be so classified. Comment, *Qualified Privilege to Defame Employees and Credit Applicants*, 12 Harv. C.R.-C.L. 143, 177-78 (1977). Although commercial speech has been afforded some first amendment protections, see *Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council*, 425 U.S. 748 (1976), it still receives a lesser degree of protection than other forms of speech. *Id.* at 771-72 n.24. For example, in *Millstone v. O'Hanlon Reports, Inc.*, 528 F.2d 829 (8th Cir. 1976), the court found credit reports to be commercial speech and sustained the constitutionality of the FCRA. The court held that the right to communicate credit reports was outweighed by the protection afforded "a significant personal right, the right to privacy." *Id.* at 833.

275. In California, a right of control based on such an "expectation of privacy" is recognized for the subjects of certain records. See *Valley Bank v. Superior Court*, 15 Cal. 3d 652, 542 P.2d 977, 125 Cal. Rptr. 553 (1975); *Burrows v. Superior Court*, 13 Cal.3d 238, 529 P.2d 590, 118 Cal. Rptr. 166 (1974). This "expectation of privacy" has not yet been applied to the employment context. California has advanced beyond most states in protecting privacy. See Cal. Const. art. 1, § 1 (privacy is an inalienable right); Cal. Lab. Code § 1198.5 (West Supp. 1978) (access by employees to their personnel files). The Privacy Commission has endorsed the California approach, but only to the extent that a government entity seeks records about an individual from a recordkeeper such as a bank or an employer. See *Privacy Report*, *supra* note 8, at 357. Although the Privacy Commission also separately supports an expectation of confidentiality against disclosures by employers to private parties, *id.* at 270-73, it is uncertain whether this is merely a policy judgment or whether it is based on the California model.

276. *Cf. United States v. Miller*, 425 U.S. 435, 449 (1976), (Brennan, J., dissenting) ("A bank customer's reasonable expectation is that, absent compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes.") (quoting *Burrows v. Superior Court*, 13 Cal.3d 238, 243, 529 P.2d 590, 593, 118 Cal. Rptr. 166, 169 (1974)).

277. The proliferation of privacy statutes that limit disseminations indicates a general awareness of the need to recognize the rights of the subjects of records as well as those of the recordkeeper. In addition to the Privacy Act, 5 U.S.C. § 552a(b) (1976), and the Buckley Amendment, 20 U.S.C. § 1232g(b)(1) (1976), several state statutes, though not granting the general right of control provided by the two federal statutes, preserve the confidentiality of public employee records. See, e.g., Colo. Rev. Stat. § 24-72-204 (3)(a)(I)-(III) (1973) (medical, psychological, and scholastic achievement data, personnel files, and letters of reference); Iowa Code Ann. § 68A.7(10)-(11) (West 1973) (personal information in confidential personnel records); N.Y. Pub. Off. Law § 89(2) (a)-(b)(i) (McKinney Supp. 1977) (any information that would constitute an unwarranted invasion of personal privacy, including "employment, medical or credit histories or personal references of applicants for employment"). Several states have also enacted statutes that limit the dissemination of arrest records of private employees. See, e.g., Cal. Lab. Code § 432.7(f) (West Supp. 1978); Ill. Ann. Stat. ch. 38, §§ 206-7 (Smith-Hurd Supp. 1978); Me. Rev. Stat. tit. 16, §§ 601-07 (Supp. 1977-78); Md. Ann. Code art. 27, § 739 (1976). Nevertheless, statutes that protect only particular types of information fail to recognize the general privacy interest of an employee in records maintained about him.

lected.<sup>278</sup> A routine use would be deemed appropriate if it is made during the ordinary course of an employer's business and if the disclosure is reasonably necessary to the efficient operation of the business. An acceptable routine use would be the disclosure to potential or present business customers of an employee's skill, experience, educational background, and performance rating. Similar disclosures to the employer's consultants, attorneys, and accountants would also be permissible. These uses should be contrasted with letters of reference or disseminations of information to credit agencies that are not made in pursuit of an employer's ordinary business and are unlikely to affect the efficient operation of the employer's business. Rather, the effect of such disclosures is borne primarily by employees. A right to control these disclosures is, therefore, particularly appropriate.

Routine uses would vary for each employer. Employers could not, however, abuse the provision by establishing an all-inclusive list of routine uses. Gratuitous derogatory comments about an employee could not be made a routine use under any standard.<sup>279</sup>

In addition to the routine use exception, a statute should enumerate specific situations when disclosure would be permitted without an employee's consent.<sup>280</sup> These exceptions would include, but not be limited to, reports to government agencies, responses to judicial or administrative subpoenas, and responses to specific requests for the fact, dates, and location of employment, and the position held.<sup>281</sup>

This statutory scheme recognizes a dual interest in employment records—ting legitimate business disseminations, which would be exempted as a routine use. These provisions reflect a reasonable balance of the dual interests by permitting legitimate business disseminations which would be exempted as a routine use from the employee consent requirement. At the same time, employees would be protected from unwanted disseminations that could have a lasting effect on their lives.

### C. Remedies

#### 1. An Action for "Privacy Discrimination"

An employer presently "enforces" his information-gathering and record-keeping practices through his right to discipline or dismiss an employee at any time.<sup>282</sup> If employee privacy legislation were to leave this right intact, the possibility of reprisals against employees exercising the rights granted would be great and the legislation's value negated.<sup>283</sup> Consequently, legislation

---

278. The Privacy Act has a comparable provision. See 5 U.S.C. § 552a(e)(3)(C) (1976). See generally *Harper v. United States*, 423 F. Supp. 192, 197-98 (D.S.C. 1976). For a discussion of the routine use concept as applied to the use category, see notes 263-65 *supra* and accompanying text.

279. See *Mazaleski v. Treusdell*, 562 F.2d 701, 713 n.31 (D.C. Cir. 1977).

280. This approach is modeled on the Privacy Act, which also couples a routine use exception, 5 U.S.C. § 552a(e)(3)(C) (1976), with specific exceptions, *id.* § 552a(k).

281. The Privacy Commission has approved these exceptions, as well as several others. See Privacy Report, *supra* note 8, at 272-73.

282. See notes 24-26 *supra* and accompanying text.

283. Indeed, the Privacy Commission explicitly recognized this when it cited the possibility of employer reprisals as a reason why legislation would be inappropriate. Privacy Report, *supra* note

should provide a statutory cause of action to an employee who is not hired, denied a promotion, demoted, or discharged as a result of seeking to exercise his rights.<sup>284</sup> This "privacy discrimination" cause of action would deter employers from interfering with an employee's rights to object to a proscribed collection method, to seek access to his files, or to require his consent prior to certain disseminations.

An employee who has established that he was discharged because of exercising his privacy rights should also, depending on the particular circumstances of the case, be granted back pay and reinstatement.<sup>285</sup> An employee who has been discriminated against in other ways short of discharge should be able to obtain an injunction to prohibit the employer from continuing the discrimination. In addition to such remedies, damages for privacy discrimination should be measured under a tort standard and thus include recovery for injury to reputation and mental distress.<sup>286</sup> In order to deter future employer violations, punitive damages should also be available.<sup>287</sup>

## 2. Actions for Violation of Statutory Requirements

The failure of an employer to meet the requirements of an employee privacy statute should be the basis for remedial action in three distinct contexts. First,

---

8, at 232. By creating a remedial mechanism within the legislation, the present analysis eliminates this argument against legislation.

284. Smaller employers should not be subject to any remedial actions. The jurisdictional standards of the National Labor Relations Board (NLRB), which usually require a minimum dollar volume for particular types of employers, could serve as a model for designing similar limits on employee privacy actions. *See, e.g.,* LaCrescent Constant Care Center, Inc. v. NLRB, 510 F.2d 1319, 1323 n.19 (8th Cir. 1975); San Francisco Local Joint Executive Bd. of Culinary Workers v. NLRB, 501 F.2d 794, 796-97 (D.C. Cir. 1974); 29 C.F.R. 103.1-3 (1977). *See generally* A. Cox, D. Bok & R. Gorman, *Labor Law* 97-98 (8th ed. 1977).

285. Section 8(a)(3) of the National Labor Relations Act (NLRA), 29 U.S.C. § 158(a)(3) (1970), is closely analogous to the proposed cause of action. It provides that an employer may not discriminate "in regard to hire or tenure of employment or any term or condition of employment to encourage or discourage membership in any labor organization." *Id.* Under § 10(c) of the NLRA, the NLRB may issue a cease and desist order to the employer and may order reinstatement of employees "with or without back pay." *Id.* § 160(c). Although the NLRB's findings are usually accorded great weight and will be set aside only if unsupported by substantial evidence, *Universal Camera Corp. v. NLRB*, 340 U.S. 474 (1951), a finding of reinstatement may be overturned if an employee has committed criminal acts, threatens the safety of persons or property, or disrupts the operation of a business. *See, e.g., NLRB v. Apico Inns of California, Inc.*, 512 F.2d 1171 (9th Cir. 1975) (prior to discharge, the employee, a bartender, made profane remarks in the presence of customers, drank while on duty, and made lewd comments to waitresses and customers); *NLRB v. Big Three Industrial Gas & Equipment Co.*, 405 F.2d 1140 (5th Cir. 1969) (employee, a truck driver, was an habitual violator of traffic laws). Title VII of the Civil Rights Act of 1964 also contains a provision that outlaws discrimination against employees who exercise their statutory rights. 42 U.S.C. § 2000e-3(a) (Supp. V 1975).

286. Damages for other forms of discrimination outlawed by statute are also based in tort law. *See Note, Damage Remedies Under the Age Discrimination in Employment Act*, 43 Brooklyn L. Rev. 47, 51-58 (1976). The action for prima facie tort, which focuses on the defendant's bad motives, is appropriate in many cases of discharge, *Blades, supra* note 1, at 1422-23, and would be particularly so when a discharge or other discrimination is a reprisal against an employee who takes advantage of his privacy rights.

287. *See Ewing Book, supra* note 153, at 201.

an employee may be directly injured as a result of an employer's violation when, for example, the employer wrongfully disseminates information to a third party without receiving an employee's consent, and that information is subsequently used as a basis for denying credit or employment to the employee.<sup>288</sup> A job applicant also might be denied employment because of an employer's wrongful requirement that he take a lie detector or personality test. In these situations, a suit should be permitted to recover actual damages.<sup>289</sup> To encourage employees to exercise their rights, any plaintiff sustaining injury should be entitled to a minimum recovery.<sup>290</sup> Liability for actual damages should also be imposed on an employer who negligently violates the statute and thereby causes harm to an employee.<sup>291</sup> Thus, an employer could not carelessly maintain his records and then claim lack of intent when injury is caused by a negligent dissemination. For employers who intentionally violate the statute, punitive damages should be available as a deterrent.<sup>292</sup>

The second context of employer violations may occur when the employer fails to comply with the statutory requirements, but no injury has been caused to an employee. For example, if an employer refuses to allow an employee to correct his record, or tells an employee to take a lie detector test, no damage has yet occurred. Nevertheless, there is a strong probability of harm to the employee. He should be permitted to sue for injunctive relief, requiring the employer to produce the records sought, or enjoining the employer from requiring the lie detector test as a condition of employment.<sup>293</sup>

The third context is similar to the second, except that, in this situation, an employer's actions are part of a continuing practice or policy that violates a requirement of the statute. An employer might have a policy of allowing supervisors to review an employee's entire file or might require that all employees submit information concerning their arrest records. Individual

---

288. 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), *discussed at* notes 81-86 *supra* and accompanying text.

289. The Privacy Act and the FCRA permit similar actions. See Privacy Act, 5 U.S.C. § 552a(g)(4) (1976); FCRA, 15 U.S.C. §§ 1681n-1681p (1976).

290. The Privacy Act provides for a minimum recovery of \$1,000. 5 U.S.C. § 552a(g)(4)(A) (1976).

291. See FCRA, 15 U.S.C. § 1681o (1976).

292. Under the FCRA punitive damages may be recovered without a showing of actual damages, *id.* § 1681n(2), because they are designed "not to compensate the plaintiff, but solely to punish the defendant." *Ackerley v. Credit Bureau of Sheridan, Inc.*, 385 F. Supp. 658, 661 (D. Wyo. 1974). The most important case on damages under the FCRA is probably *Millstone v. O'Hanlon Reports, Inc.*, 528 F.2d 829 (8th Cir. 1976). In *Millstone*, the plaintiff's car insurance policy was cancelled after the defendant furnished a credit report to the insurance company that falsely stated that the plaintiff was a "hippie," attended protest demonstrations, was suspected of drug use, and was rumored to have been evicted from three places. The court awarded \$2,500 in actual damages, \$25,000 in punitive damages and \$12,500 in attorney's fees. *Id.* at 831. Injunctive relief should also be available. Relief of this nature is common under Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e to 2000e-17 (1970 & Supp. V 1975). See, e.g., *Stokley v. Lewis Carpet Mills, Inc.*, [1977] 14 Empl. Prac. Dec. (CCH) ¶ 7592 (N.D. Ga. 1977) (employees who were discharged as a result of discrimination obtained an injunction against their former employer to prevent him from stating in any employment records that they were terminated for cause).

293. See Privacy Act, 5 U.S.C. § 552a(g)(3)(A) (1976).



actions for injunctive relief would not sufficiently combat the threat of repeated violations. A government agency, perhaps the Department of Labor, should be given the power to sue an employer to obtain injunctions against the continuation of such practices.<sup>294</sup> The threat of such actions should provide an additional deterrent against employers which fail to abide by statutory provisions.

#### CONCLUSION

Since the famous article by Warren and Brandeis in 1890, the law of privacy has developed rapidly. It now includes four different types of common law actions, various constitutional guarantees, and a recent proliferation of state and federal statutes. The exclusion of private sector employees from these existing protections is inexcusable. The employee's privacy interests are closely analogous to those interests that are protected by existing privacy actions. The failure of privacy measures to protect employees borders on the irrational because the employment relationship requires many employees to submit to a more varied array of intrusive practices than almost any other relationship between an individual and an organization in contemporary society.

This Comment's proposal for comprehensive employee privacy legislation is an effort to formulate a reasonable accommodation between the interests of the employee and the very real, and often compelling, countervailing interests of employers. The explication of the various interests of employers and employees and the resolution of those interests presented should indicate that the overdue task of recognizing a legal right of privacy for private employees can be accomplished with fairness, manageable cost, and a minimal burden to employers.

*Martin N. Flics*

---

294. This agency should not be given the power to promulgate rules and regulations that establish procedures for employer compliance with the statute. The continuous intervention of a government agency to monitor the internal recordkeeping practices of a private employer would probably require employers to prepare numerous reports for agency review and would be an unprecedented governmental invasion into the private sector. The avoidance of such recordkeeping requirements has limited the costs of compliance with the Buckley Amendment. See Cudlipp, *The Family Educational Rights and Privacy Act Two Years Later*, 11 U. Rich. L. Rev. 33, 40 (1976). Furthermore, the intricate, complex, and probably inefficient bureaucracy that would be required to oversee the recordkeeping practices of almost all private employers would be a massive, and perhaps impossible, undertaking. See Privacy Report, *supra* note 8, at 232.