UIC John Marshall Journal of Information Technology & Privacy Law

Volume 11
Issue 3 *Computer/Law Journal - Fall 1992*

Article 4

Fall 1992

Invasions of Privacy and Computer Matching Programs: A Different Perspective, 11 Computer L.J. 461 (1992)

Rubin E. Cruse Jr.

NOTE

INVASIONS OF PRIVACY AND COMPUTER MATCHING PROGRAMS: A DIFFERENT PERSPECTIVE

I. INTRODUCTION

The United States Federal Government initiated computer matching programs in the early 1970's,[1] and their use has since dramatically increased.[2] Computer matching "involves the comparison of two or more sets or systems of computerized records to search for individuals who may be included in more than one file."[3] Typically, federal agencies use computer matching to detect fraud, error or abuse in government programs, or to determine whether a specific applicant or recipient of benefits under a government program truly qualifies for those benefits.[4] By reducing such wastes, computer matching helps to ensure the integrity and efficiency of government programs.[5] The Office of Management and Budget, and the President's Council on Integrity and Efficiency, have attributed "substantial savings and recoveries of overpayment in federal benefit programs" to computer matching.[6]

Privacy advocates feel that the substantial savings in federal benefit programs do not occur without a significant cost. Congress has expressed concern that "the increasing use of computers and sophisticated information technology, while essential to the efficient operations of government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information."[7] Congress passed the Computer Matching and Privacy Protection Act of 1988[8] ("Computer Matching Act") to protect the privacy rights of individuals whose records are compared in computer

1. Jaffess v. Secretary, Dep't of Health, Educ. & Welfare, 393 F. Supp. 626 (1975); S. REP. NO. 516, 100th Cong., 2d Sess. 2 (1988).

2. S. REP. NO. 516, 100th Cong., 2d Sess. 4 (1988).

3. U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy*, OTA-CIT-296, 37 (June 1986).

4. S. REP. NO. 516, 100th Cong., 2d Sess. 2 (1988).

5. *Id.* at 5.

6. *Id.*

7. *Id.* at 6 (*citing* the Privacy Act of 1974, Pub. L. No. 93-579, § 2, 88 Stat. 1896 (1974)).

8. Pub. L. No. 100-503, 102 Stat. 2507 (1988) (*codified* at 5 U.S.C. § 552a).

matching programs.[9] One requirement of the Computer Matching Act is the submission of a cost-benefit analysis demonstrating that the benefits of a computer match will outweigh the privacy costs.[10]

This Note proposes that, contrary to popular opinion, computer matching does not necessarily invade a person's privacy. Computer matching that does invade one's privacy may be the exception rather than the rule and therefore a cost-benefit analysis is not needed.

The Note is divided into three sections. The first section analyzes the distinction between a loss of privacy and an invasion of privacy. Not every loss of privacy constitutes an invasion. This Note proposes that an invasion of privacy occurs when (1) there is a loss of privacy and (2) no consent is given for that loss. The second section of this Note analyzes two computer matching programs that would be subject to the provisions of the Computer Matching Act to show that they do not create an invasion of privacy. Such an analysis requires one to define clearly the notion of consent, a concept central to any invasion of privacy claim. The final section looks to the functions privacy serves to defend the use of Thomas Huff's definition of consent as the basis for determining whether computer matching programs create an invasion of privacy.[11]

II. DISTINCTION BETWEEN A LOSS AND AN INVASION OF PRIVACY

In order to determine whether computer matching programs create an invasion of privacy, one must first define the terms: privacy, loss and invasion. The definition of privacy is taken from the work of Ruth Gavison.[12] In her article, *Privacy and the Limits of Law*, she suggests that privacy is a limitation of others' access to an individual.[13] "A *loss* of privacy occurs as others obtain information about an individual, pay attention to him, or gain physical access to him."[14]

An invasion of privacy, however, is an "unreasonable intrusion upon the seclusion of another."[15] There are three elements which must be established for the tort of an invasion of privacy. These elements are: (1) an intrusion by the defendant; (2) into a matter which the

9. *Id.* at 1.

10. 5 U.S.C. § 552a(o)(1)(B) (1988).

11. *See infra* text accompanying notes 43-45. Huff states that our privacy is not invaded by a disclosure of information when we choose to place ourselves in a position where evaluations are expected.

12. Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 428 (1980).

13. *Id.*

14. *Id.* (emphasis added).

15. RESTATEMENT (SECOND) OF TORTS, § 652A(2)(6) (1976); 62A AM. JUR. 2D *Privacy* § 38 (1990).

plaintiff has a right to keep private; and (3) by the use of a method which is objectionable to the reasonable person.[16]

The single factor which distinguishes a loss of privacy from an invasion of privacy is "consent." A person can consent to allow another to obtain information about himself or herself, to pay attention to him or her, or to gain physical access to him or her (i.e. a person can consent to a loss of privacy).[17] In contrast, one cannot consent to an invasion of privacy. Although commentators have treated consent as a bar to a claim for damages upon a finding of a privacy invasion,[18] this author disputes that one can waive an invasion of privacy by consent. Consent is not a defense to an invasion. Consent means that no invasion of privacy can occur. By examining the three elements which establish an invasion of privacy, one can see how consent vitiates each element.

The first element requires an intrusion by the defendant. According to Webster's dictionary, to intrude is "to come or go in *without . . . permission*."[19] If one enters with permission, then one cannot intrude. Similarly, just as one cannot consent to an intrusion, one cannot consent to an invasion.

The second element requires that the plaintiff has a right to keep the information private. This right cannot be considered inalienable. If *X* cannot provide *Y* with information about *X* (i.e. "sell" his privacy), because *X*'s privacy right is inalienable, *X* and *Y* would not be able to engage in any sort of contractual relation. This infringes upon *X*'s liberty of action, a value that privacy is supposed to promote.[20] When *X* consents to provide information about himself to *Y*, he bargains away his right to keep that information private. Consent, in effect, extinguishes such a right with respect to *Y*.

The third element requires that the invader use a method which is objectionable to a reasonable person. In *Nader v. General Motors Corp.*,[21] the Court of Appeals of New York stated that the defendant's conduct must be "designed to elicit information which would not be available through *normal* inquiry or observation."[22] The court adopted a result-oriented approach, rather than a process-oriented approach, to determine the existence of this third element. That is to say, the emphasis is not on how the method was employed but on the information

16. 62A AM. JUR. 2D *Privacy* § 48 (1990).

17. *See infra* text accompanying notes 24-27 as an example of consent to a loss of privacy.

18. 62A AM. JUR. 2D *Privacy* § 59 (1990).

19. WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY OF THE ENGLISH LANGUAGE 1187 (1986) (emphasis added).

20. *See infra* text accompanying notes 42-44.

21. 25 N.Y.2d 560, 255 N.E.2d 765, 307 N.Y.S.2d 647 (1970).

22. *Id.* at 567, 255 N.E.2d at 769, 307 N.Y.S.2d at 652 (emphasis added).

it was designed to obtain. If the method is designed to elicit information which the plaintiff meant to keep private, then one could say that such a method is objectionable because it is designed to elicit information which would not be available through normal inquiry. A normal inquiry would not be designed to elicit information that a reasonable person would refuse to reveal. Consent, therefore, creates the parameters of a normal inquiry. Normal inquiries elicit information which the plaintiff has consented to release. Unreasonable inquiries elicit information which does not have this consent. Consent determines whether the method of inquiry is objectionable or not.

This analysis suggests that an invasion of privacy has two requirements: (1) there must be a loss of privacy and (2) this loss must occur without the consent of the individual. The next step is to apply this definition to determine whether computer matching programs create an invasion of privacy.

III. DO COMPUTER MATCHING PROGRAMS CREATE AN INVASION OF PRIVACY?

The Computer Matching Act covers two kinds of computer matching programs: (1) a comparison of records for the purpose of establishing or verifying eligibility for a federal benefit program, and (2) a comparison for the purpose of recouping payments or delinquent debts under benefit programs.[23] This Part determines whether the following two computer matching programs that fall within the purview of the Computer Matching Act create an invasion of privacy.

A. *JAFFESS V. SECRETARY, DEP'T OF HEALTH, EDUC. & WELFARE*

Ira Jaffess was receiving a disability benefits pension from the Veterans Administration ("VA") as well as Social Security benefits. The amount of VA benefits payable varies depending upon the veteran's annual income from other sources, including income received under the Social Security Act.[24] "A veteran who receives [VA] benefits is obligated by law to report changes in his annual income to the VA."[25] Mr. Jaffess did not report his Social Security benefits to the VA.

The VA subsequently conducted a computer match of persons who received VA benefits with those receiving Social Security benefits, information provided by the Department of Health, Education and Welfare ("HEW"). This comparison was "performed 'in order to locate persons who have failed to report their Social Security benefits to the VA as re-

23. 5 U.S.C. § 552(a)(8)(A)(i) (1988).

24. 38 U.S.C. § 521 (1988).

25. Jaffess v. Secretary, Dep't of Health, Educ. & Welfare, 393 F. Supp. 626, 628 (S.D.N.Y. 1975).

quired by law.' "[26] Through this comparison, the VA discovered a discrepancy between the information Mr. Jaffess had provided the VA and the information the HEW had. Mr. Jaffess was a "hit." On January 6, 1975, Mr. Jaffess received notice from the VA that his benefits would be reduced. Did the computer matching create a loss of privacy to which Mr. Jaffess did not consent?

1. *Obtaining Information About an Individual*

In answering this question, one must first determine whether some entity obtained information about Mr. Jaffess. On the face of things, the VA apparently obtained information about Mr. Jaffess regarding his Social Security benefits. However, in order to receive VA benefits, Mr. Jaffess was required to disclose information regarding his income. Mr. Jaffess voluntarily agreed to such an arrangement. Mr. Jaffess, then, voluntarily assumed a role or "image," and presented it to the VA. Any information conveyed by assuming this role may be considered a loss of privacy, but Mr. Jaffess consented to this loss by consenting to assume the role.[27]

The issue is whether the HEW invaded Mr. Jaffess's privacy by allowing the VA access to the Social Security records to conduct the computer match. Such an invasion of privacy did not occur. The role or image which Mr. Jaffess assumed called for him to disclose his income accurately to the VA. The VA's knowledge was that Mr. Jaffess had the acceptable level of income to receive VA benefits. The computer match did not provide the VA with any further information about Mr. Jaffess. It simply attempted to verify the accuracy of the information that Mr. Jaffess had already provided.

One response to this argument is that the VA now knows that Mr. Jaffess falsely reported his income to the VA. This is additional information about Mr. Jaffess that was not part of the agreement with the VA. Such information is beyond the scope of the consent given.

The premise of this argument is incorrect. When Mr. Jaffess reported his income to the VA, the VA believed that Mr. Jaffess would report his income accurately and would continue to do so in the future. Therefore, the VA received information regarding Mr. Jaffess's trustworthiness, which constituted a part of the image Mr. Jaffess had assumed. The computer match not only attempted to verify the accuracy of Mr. Jaffess's income, but also attempted to verify the information which the VA already had on Mr. Jaffess's trustworthiness.

Professor Gavison presents a point that may still refute the idea

26. *Id.*

27. The idea of presenting an "image" shall be discussed in more detail in the last section regarding the notion of consent.

that the VA received no new information from the computer match. Her argument calls for a distinction between verbal and sensory knowledge.[28] The example she provides is as follows:

> [A]ssume *Y* learns that *X* is bald because he reads a verbal description of *X*. At a later time, *Y* sees *X* and, naturally, observes that *X* is bald. Has *Y* acquired any further information about *X*, and if so, what is it? It might be argued that even a rereading of a verbal description may reveal to *Y* further information about *X*, even though *Y* has no additional source of information.[29]

Assuming that such a rereading does produce additional information, this result would not occur with computer matching programs. If Mr. Jaffess had provided the VA with correct information, he would not be a hit when the computer match is conducted. Since there is no discrepancy between the information he provided the VA and the Social Security records, he would not be registered by the computer. The person conducting the computer match reads only the hits. Since Mr. Jaffess would not be a hit, he would not be reread, and so Professor Gavison's point would not apply. A computer rereads the information, not an individual.

Mr. Jaffess was, however, a hit. The VA read both his description of his Social Security benefits and the HEW's description of his Social Security benefits. If both descriptions had been the same, then one could argue that such a rereading produced additional information about Mr. Jaffess. But the only reason this rereading occurred is because of the discrepancy between the two sets of information. Before the computer match, the VA's information about Mr. Jaffess is that Mr. Jaffess's report of his income is true and that Mr. Jaffess is trustworthy. After the match, the VA does not know which record of Mr. Jaffess's income is correct or whether Mr. Jaffess falsely reported his income. This uncertainty reflects a loss of information. For example, if I read a description of Mr. Jaffess that states he is bald, I now have information about Mr. Jaffess. When I read a second description about Mr. Jaffess that states he is not bald, I now know that Mr. Jaffess is either bald or not bald. Therefore, I know nothing about the state of Mr. Jaffess's scalp, while before I read the second description, I did have such information. I have lost information about Mr. Jaffess. Computer matching programs thus seem to either (1) not affect the obtaining of information at all, as is the case when Mr. Jaffess is not a hit, or (2) question the validity of information the VA already has received, when Mr. Jaffess is a hit.

---

28. Gavison, *supra* note 12, at 430.

29. *Id.*

2. *Paying Attention to the Individual*

While computer matching may not further the level of information the VA has on Mr. Jaffess, some may feel that the computer match may be an invasion of privacy by bringing Mr. Jaffess to the attention of the VA, where, before, he had not been the subject of attention.[30] Professor Gavison states that

> *X* may be the subject of *Y*'s attention in two ways. First, *Y* may follow *X*, stare at him, listen to him, or observe him in any other way. Alternatively, *Y* may concentrate his thoughts on *X*. Only the first way . . . is directly related to a loss of privacy. Discussing, imagining, or thinking about another person is related to privacy in a more indirect way, if at all.[31]

The VA did not pay attention to Mr. Jaffess in the first sense. The VA observed information about Mr. Jaffess. They did not observe Mr. Jaffess, the individual. They have not followed him, stared at him, or listened to him, as the first sense states. Furthermore, the VA probably did not pay attention to Mr. Jaffess in the second sense either. Since, in all likelihood, there were many such hits, just like Mr. Jaffess,[32] and the VA did not conduct any further hearings or investigations, one must question whether the VA discussed, imagined, or even thought about Mr. Jaffess at all. Mr. Jaffess was simply one hit among many. The VA terminated his benefits because they now had less information about Mr. Jaffess than he had agreed to provide.

One may feel that the VA violated Mr. Jaffess's due process rights by lowering his benefits without a formal inquiry, but this has nothing to do with a loss of privacy. In fact, if the VA had conducted a formal hearing, they would have been more likely to have invaded his privacy. A formal hearing would focus more attention on Mr. Jaffess than simply terminating his benefits did. Any attention a person receives after a computer match comes not from the results of the match, but by any further verification or formal inquiry procedures regarding the results. Post-match verification is not a way of protecting against an invasion of privacy from a computer match. This verification may create an invasion of privacy that would not exist otherwise. One must weigh the value of due process against the value of privacy to determine the appropriate extent of such verification procedures.

---

30. *Id.* at 432.

31. *Id.*

32. The computer comparison was of all persons who received VA and Social Security benefits. Jaffess v. Secretary, Dep't of Health, Educ. & Welfare, 393 F. Supp. 626, 628 (S.D.N.Y. 1975).

3. *Gaining Physical Access to the Individual*

As Gavison has noted, "[i]ndividuals lose privacy when others gain physical access to them. Physical access here means physical proximity—that *Y* is close enough to touch or observe *X* through normal use of his senses."[33] The essence of the complaint is not that more information about a person has been acquired or that more attention has been drawn to him, but that his spatial aloneness has been diminished.

The computer matching program did not violate Mr. Jaffess's spatial aloneness because it did not allow physical access to him. Opponents may, however, argue that the reduction of benefits was a physical access to Mr. Jaffess and that the physical access was a direct result of the computer matching program.

Such a concept of physical access is quite troublesome. This notion of physical access embodies the idea that if *X* confers a benefit on *Y*, under certain conditions, and *Y* does not meet those conditions, *X* cannot reclaim the benefits conferred because they have become part of *Y*'s spatial aloneness. For example, if a bank were to loan money to *Y* to finance a house, and *Y* defaults, the bank should be allowed to repossess the house. This repossession is not a gain of physical access because there is no violation of physical proximity. If the bank, instead, let *Y* keep the house but forced *Y* to live with the bank president's mother-in-law, then there would be a diminishing of spatial aloneness.

The foregoing analysis suggests that the computer match in *Jaffess* did not invade Mr. Jaffess's privacy. The next computer match to be analyzed will solidify this point.

B. COMPUTER MATCH BY THE DEPARTMENT OF EDUCATION

In 1982, the Department of Education ("DE") compared by computer a list of delinquent student loan debtors against a list of federal employee active and retired rolls.[34] This computer match recovered $3.4 million in delinquent loan payments.[35] According to the Debt Collection Act of 1982,

> [w]hen the head of an agency . . . determines that an employee . . . is indebted to the United States for debts to which the United States is entitled to be repaid at the time of the determination by the head of an agency . . . , or is notified of such a debt by the head of another agency . . . , the amount of the indebtedness may be collected in monthly installments, or at officially established pay intervals, by deduction from

33. Gavison, *supra* note 12, at 433.

34. *Hearing before the Subcommittee on Oversight of Gov. Management of the Committee on Governmental Affairs*, S. REP. NO. 2756, 99th Cong., 2d Sess. 62 (1986).

35. S. REP. NO. 516, 100th Cong., 2d Sess. 2 (1988).

the current pay account of the individual.[36]

Does this computer match create an invasion of privacy?

1. *Obtaining Information About an Individual*

To analyze whether any additional information has come out of the computer match, consider the hypothetical federal employee *X* who has received student loans and is now delinquent in repaying them.

The issue is what information did *X* supply to the DE in order to receive the loans. *X* does not have to inform the DE as to whether or not he is a federal employee as a condition of receiving the loan. This is not part of the price of the loan. Therefore, when the DE does a computer match with the list of federal employees, they will gain information about *X*'s status as a federal employee without *X*'s consent.

One argument against this conception of the agreement between the DE and *X* is that part of the price for receiving a student loan requires *X* to pay back the loan. Since *X* is now being forced to pay it back, the DE should have access to the information that *X* is a federal employee as agreed upon for the DE to collect *X*'s debt through wages. This analysis, however, ignores the fact that if *X* had paid the loan back, the DE would not know he was a federal employee. After the computer match, the DE knows that *X* is a federal employee. Thus, the only instance threatening an invasion of privacy occurs when *X* has breached his contract with the DE. If *X* had paid his loan, he would not have been involved in the match. The DE would not have received information about him and would not have invaded *X*'s privacy.

Such a rationale for recognizing an invasion of privacy when *X* breaches the contract is worrisome because it rejects the basic notion that expectation damages should be awarded for a breach of contract. When *X* fails to repay the loan and breaches the contract, the DE is entitled to its expectation damages which is equivalent to the loan money. The DE, however, gets more than the loan money. It receives knowledge that *X* is a federal employee. This additional information punishes *X* just as if a court had awarded punitive damages for breach of a contract.

An additional unfairness to *X* arises when the DE's information is incorrect. Suppose *X* has paid his debt, but the DE records him as being delinquent. After the match, the DE receives information that *X* is a federal employee even though *X* has not breached his obligation to repay the debt. This scenario differs from *Jaffess*. In *Jaffess*, the VA had information before the match that was *A*.[37] After the computer match,

36. Debt Collection Act of 1982, § 5(a), Pub. L. No. 97-365, 96 Stat. 1749, 1751 (codified at 5 U.S.C. § 5514(a)(1) (1988)).

37. *A* = Mr. Jaffess's income is at the acceptable level.

the VA arrived at a point where the information was either *A* or not-*A*. In the DE hypothetical case, the DE has information before the match that is either *B* or not-*B*.[38] After the match, the DE has information that is *B*. By comparison, the VA obtains less information about Mr. Jaffess than it was entitled to have, whereas the DE has more information about *X* than it was entitled to have.

One objection to this analysis is that the DE has not received any information about *X* that *X* had not already consented to provide. The following scenario exemplifies the indirect consent of *X* to the DE's access to *X*'s student loan information if *X* is a federal employee.

When *X* gets a job at some federal agency, *ABC*, the agency will inquire whether *X* has defaulted on any student loans. Assume that *X* provides false information and says he is not a delinquent student loan debtor. After *X* starts to receive benefits from the government (his paycheck), *ABC* conducts a computer match with the DE and discovers the discrepancy. This situation is similar to *Jaffess*. *ABC* now has less information about *X* than *X* had agreed to provide. *ABC* can now deduct money from *X*'s pay in order to pay the debt. When *ABC* provides this money to the DE, it is basically telling the DE that *X* is a federal employee and this money pays his debt. The computer match would not be an invasion of privacy, because if *X* had initially told the truth that he was a student loan defaulter, *X* would know that *ABC* would deduct money from his pay and give it to the DE which would then know that *X* is a federal employee. *X* has, therefore, indirectly, consented to the DE to provide information that he is a federal employee.

The weak link in this indirect consent model is in the assumption that *X* would know that *ABC* would deduct the money and give it to the DE. If *X* does not know that *ABC* would use the deductions from his salary to pay the DE, then *X* has not given consent to this loss of privacy. Such a situation does not, however, seem likely. *ABC* can inform *X* directly, which means *X* has given consent. If *ABC* does not, the analysis is more complicated. Since *X* knows to whom he has defaulted, and that *ABC* will collect his debt,[39] *X* should know who receives the money. Under either analysis, a computer match does not necessarily result in an invasion of privacy.

2. *Paying Attention to the Individual and Gaining Physical Access to the Individual*

The DE's computer matching also fails to satisfy the last elements of Gavison's index for testing an invasion of privacy. As under *Jaffess*, the level of attention necessary to trigger an invasion of privacy de-

38. *B* = *X* is a federal employee.

39. 5 U.S.C. § 5514(a)(1) (1988).

pends upon the verification and formal hearing procedures that occur after the computer match. Also, a reduction of wages if *X* is a federal employee does not violate *X*'s spatial aloneness just as a reduction of veteran's benefits did not increase physical access to Mr. Jaffess.

IV. THE NOTION OF CONSENT

The key element to the foregoing analysis is the word consent. In *Jaffess*, Mr. Jaffess consented to provide information regarding his Social Security benefits to the VA. The computer match was merely an attempt to verify information that had already been provided with consent.[40] Similarly, in the DE's computer match, the argument is that *X* indirectly consented to provide information that he is a federal employee to the DE.[41]

One may, however, reasonably argue that neither Mr. Jaffess nor *X* really consented at all. While Mr. Jaffess did agree to provide information regarding his Social Security benefits to the VA, he chose to withhold certain information. After the computer match, the VA obtains information that can indicate either a failure to report benefits or reporting benefits when *X* never received them.[42] Since there is no evidence that Mr. Jaffess gave explicit consent to the HEW to allow his Social Security information to be used to verify information he gave to the VA, one may argue that the information from the HEW is being used for a purpose that was not originally intended. Such a situation is exactly why one fears an invasion of privacy.

This argument also applies to the DE's computer match. The consent that was derived is an indirect consent. Since *X* did not explicitly say that the DE is entitled to know whether he is a federal employee, then the information that *ABC* has (that *X* is a federal employee) is being used for a purpose that was not originally intended (i.e. for the purpose of debt collection).

The question is how to correctly define consent. This Part suggests that consent should be drawn in a broader sense, and not in the explicit, narrow sense just mentioned. The definition of consent suggested is taken from the work of Thomas Huff.[43] Huff states that

> [o]ur privacy is invaded by disclosures of information when the sort of information which could make us subject to evaluation is transmitted to persons who lack the authority to evaluate us. . . .
>
> . . . .
>
> . . . [O]ur privacy is . . . waived in those circumstances in which evalua-

40. *See supra* text accompanying notes 23-27.

41. *See supra* text accompanying notes 37-39.

42. *Id.*

43. Huff, *Thinking Clearly About Privacy*, 55 WASH. L. REV. 777, 782 (1980).

> tion is *appropriate* or approved. . . . *[O]ur privacy is not invaded by the disclosure of information because we choose to place ourselves in a position where evaluations are expected. . . . [W]here information is released without our permission, or is sought in contexts in which we have not sought evaluation,* . . . [then] our privacy is invaded.[44]

The rationale for adopting Huff's idea of consent comes from looking at the ways privacy serves the individual.

A. CONSENT AND THE FUNCTIONS OF PRIVACY

1. *Promote Liberty of Action*

Professor Gavison states

> privacy . . . severs the individual's conduct from knowledge of the conduct by others. Privacy thus . . . functions to promote liberty of action, [by] removing the unpleasant consequences of certain actions and thus increasing the liberty to perform them.[45]
>
> . . . .
>
> This promotion of liberty of action links privacy to a variety of individual goals.

These goals are as follows.

2. *Promote Human Relations*

Professor Gavison argues:

> Privacy also functions to promote liberty in ways that enhance the capacity of individuals to create and maintain human relations of different intensities. Privacy enables individuals to establish a plurality of roles and presentations [i.e. images] to the world. This control over "editing" one's self is crucial, for it is through the images of others that human relations are created and maintained.[46]

This liberty to edit one's self, however, is not unfettered. "Privacy is derived from liberty in the sense that we tend to allow privacy to the extent that its promotion of liberty is considered desirable."[47] The question to address is whether computer matching programs have a desirable effect on one's liberty to edit one's self.

In the computer matching programs discussed, both Mr. Jaffess and *X* presented images of themselves that contained false information.[48] The computer matching programs verified the truthfulness of the images presented. Both Mr. Jaffess and *X* now have difficulty in

---

44. *Id.* (emphasis added).

45. Gavison, *supra* note 12, at 448.

46. *Id.* at 450.

47. *Id.* at 451.

48. Mr. Jaffess gave the image to the VA that he had a level of social security benefits that allowed him to receive VA benefits. *X* gave the image to ABC that he was not a student loan defaulter.

presenting such images. They have lost control of their ability to present certain images. Nevertheless, this loss is a desirable effect.

As Professor Gavison stated, "control over *'editing'* one's self is crucial."[49] The word edit, according to Webster's dictionary, means (1) to select, revise, etc., or (2) to assemble by cutting, rearranging, etc.[50] Edit does not mean to present false information as if it were true. Edit connotes selecting to show only certain true aspects of one's self, not fabricating an image. Fabrication goes beyond the scope of editing.

One can consider the distinction as being between malfeasance and nonfeasance. When a person withholds certain information about himself, this can be considered a nonfeasant image that is presented. When he or she presents false information, this is a malfeasant image. To edit one's self cannot, therefore, mean to present a malfeasant image because a malfeasant image goes beyond the definition of edit.

Even if the term edit could be construed to allow for a malfeasant image, such a construction is not desirable. "Socrates warns at the beginning of the *Crito*, our concern should not be with the opinions men have of us, but rather with the truth of those opinions."[51] The reason for allowing one to edit one's self is to facilitate human relations. If, however, *Y* cannot verify that the image *X* presents is true, then *Y* will not be willing to bear the risk of its falsity by becoming involved in certain relations with *X*. To allow editing to include the idea of the malfeasant image is to harm the very reason for its existence.

Put simply, when one knowingly presents false information about himself to another (the malfeasant image), it is appropriate for the other to evaluate the information. This evaluation is necessary to promote human relations. The Huff-type consent has, therefore, been given. The evaluation may cause a loss of reputation, but it does not cause a loss of privacy to which there is no consent. Note that this consent extends only to the verification of information provided. To attempt to discover undisclosed information through a verification procedure is a breach of the nonfeasant image and is an invasion of privacy.

Computer matching programs serve to facilitate human relations by making detection of the malfeasant image easier, thus giving people more faith in the truthfulness of an image that is presented. The computer matching programs discussed in this Note go strictly to detecting the malfeasant image. There is, however, the concern that not all computer matching programs are used strictly for verification purposes.

---

49. Gavison, *supra* note 12, at 450 (emphasis added).

50. WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY OF THE ENGLISH LANGUAGE 723 (1986).

51. Huff, *supra* note 43, at 783.

Some fear that they may be used to delve into the nonfeasant image. For example, after receiving information from the HEW regarding the level of Social Security benefits (pertinent to detecting a malfeasant image), the VA may receive some other information that Mr. Jaffess provided to the HEW but did not provide to the VA. This information would breach the nonfeasant image that Mr. Jaffess presented to the VA.

While this may be a legitimate concern, it can be resolved easily. Federal agencies use computer matching to detect fraud, error and abuse in government programs or to determine whether a specific applicant or recipient of benefits under a government program truly qualifies for benefits.[52] One could argue that there is little reason for them to gather information about an individual beyond the agency's verification needs. Gathering such extraneous information on a large scale takes up space in a computer memory and incurs costs. Even if one still feels that there is such a concern, simple measures can be taken to prevent a breach of the nonfeasant image. First, the agency should ensure that every computer match is drawn narrowly to serve either (1) the purpose of establishing or verifying eligibility for a federal benefit program, or (2) the purpose of collecting payments or delinquent debts under such programs.[53] Computer matching can be conducted narrowly,[54] so there is less of a chance that there will be an intrusion into the nonfeasant image. Such narrowing is not expensive so that costs will not deter an agency from adhering to the restrictive searches.

Second, an agency should destroy the computer match results after the verification is completed.[55] In this way any extraneous information that may have been caught in the computer match will be destroyed and cannot be passed on to other agencies in the event of future computer matches.

A related issue involves the occurrence of computer error. If person *X* provides correct information to the VA about his Social Security

52. S. REP. NO. 516, 100th Cong., 2d Sess. 2 (1988).

53. The Computer Matching Act can provide this measure because it requires that a computer match can only occur if there is a written agreement specifying (1) the purpose and legal authority for conducting the program and (2) a description of the records that will be matched, including *each* data element that will be used. 5 U.S.C. § 552a(o)(1)(A), (C) (1988). However, it also requires a cost-benefit analysis to insure that the benefits outweigh the privacy costs of such a match. 5 U.S.C. § 552a(o)(1)(B) (1988). What this Note has argued is that, if the computer match is narrowly drawn to serve one of the two given purposes, then no invasion of privacy will occur, thus rendering the need for such a balancing test moot.

54. H.R. REP. NO. 802, 100th Cong., 2d Sess. 4 (1988) (stating that matching can identify people in one program who are also involved in a second program and who have a specific characteristic).

55. 5 U.S.C. § 552a(o)(1)(I) (1988).

benefits, but the computer match still records him as a hit, has *X*'s privacy been invaded? The answer is that the computer matching program, itself, does not create an invasion of privacy. *X* has placed himself in a position where evaluation of information provided is expected. Consent has been given. As long as there is no breach of the nonfeasant image, no new information has been disclosed and no invasion of privacy has occurred.

One response to this argument is that while *X* consented to evaluation of the information provided, *X* did not consent to the loss of privacy that comes from the attention now paid to *X*. Since *X* gave truthful information, *X* did not expect to be caught in a computer matching program used to verify his information.

Any attention a person receives after a computer match comes not from the results of the match but from further verification or formal inquiry procedures regarding the results.[56] If our only concern is privacy, then the best thing to do to protect privacy would be to immediately discontinue *X*'s benefits. No attention is paid to *X*, and there is less of a chance that a breach of the nonfeasant image will occur because no further inquiry is made. This situation requires that *X* have the responsibility of proving that the computer match made a mistake. If the costs of such a responsibility prove to be too great, then *X* has a disincentive to engage in certain human relations. In an ironic twist, protecting privacy in this manner impedes promotion of human relations.

Post-match verification procedures are used to recognize a person's due process rights and are desired for that reason. They are part of the evaluation of information and are therefore expected. While one must strike a balance between due process and privacy rights in determining the level of post-match verification procedures, such a topic is beyond the scope of this Note. Due process procedures can create an invasion of privacy, but a computer matching program itself does not.

3. *Promote Autonomy*

The promotion of liberty, in promoting human relations, involves a distinction between the liberty to make a truthful image, and the liberty to make any image. This Note suggests that privacy does not protect one's liberty to present a false or malfeasant image for reasons that promote human relations. Autonomy, however, may be a value that calls for privacy to protect any and all images, including malfeasant ones. Professor Gavison has stated:

> Autonomy is another value that is linked to the function of privacy in promoting liberty. Moral autonomy is the reflective and critical accept-

56. *See supra* text accompanying notes 31-33.

> ance of social norms, with obedience based on an independent moral evaluation of their worth. Autonomy requires the capacity to make an independent moral judgment, the willingness to exercise it, and the courage to act on the results of this exercise even when the judgment is not a popular one. . . .
>
> . . . .
>
> . . . No matter how open a society may be, there is a danger that behavior that deviates from norms will result in harsh sanctions. The prospect of this hostile reaction has an inhibitive effect. Privacy is needed to enable the individual to deliberate and establish his opinions.[57]

This argument seems to suggest that a person should be allowed to present a malfeasant image protected by a privacy right so that the individual's true opinions will not be subject to harsh sanctions. Privacy permits an individual to express his judgments to a group of like-minded people. After a period of germination, such individuals may be more willing to declare their unpopular views in public.[58] This way, the individual is better able to achieve moral autonomy.

There is a problem with Professor Gavison's argument once it is applied to protection of the malfeasant image. As defined, "[a]utonomy requires the capacity to make an independent moral judgment, the willingness to exercise it, and the courage to act on the results of this exercise even when the judgment is not a popular one."[59] The individual who presents a malfeasant image has, necessarily, exercised his autonomy. He has made an independent moral judgment that it is acceptable for him to lie in order for him to receive benefits. This Note believes such a judgment to have been made independently because society, as a whole, does not consider lying as acceptable behavior. The individual has the willingness to exercise autonomy and the courage to act on the results of this exercise even when the judgment is not a popular one. The courage element, however, seems to be circumvented by a notion that even a malfeasant image should be protected by a privacy right.

Courage implies that there is a certain risk involved in making an unpopular judgment. This risk comes from an evaluation of the truth of the judgment or opinion. By recognizing the risk, a person finds it necessary to be able to defend his opinion. In order to defend his opinion, he must scrutinize it carefully and know exactly why he holds such an opinion. After conducting such an analysis, a person is more likely to be "self-respecting, self-possessed, and venturesome"[60] (i.e. autonomous).

If, however, a malfeasant image is not subject to evaluation, then

---

57. Gavison, *supra* note 12, at 449-50.

58. *Id.* at 450.

59. *Id.* at 449.

60. Huff, *supra* note 43, at 783.

the risk factor is gone. There is no need to scrutinize one's opinion carefully, and one cannot be truly autonomous.

> Certainly, the weaker our image of ourselves, both as vulnerable to gossip and as morally weak, the more distorted becomes our fear of being found out and the more strongly we desire to control our image. A person who is self-respecting, self-possessed, and venturesome is doubtless less afraid of what might be found out about him or her.[61]

Protection of the malfeasant image from evaluation does not, therefore, help a person become more autonomous. It may actually impede such development.

As, however, Professor Gavison has stated,

> No matter how open a society may be . . . there is a danger that behavior that deviates from norms will result in harsh sanctions . . . [therefore] [p]rivacy is needed to enable the individual to deliberate and establish his opinions. If public reaction seems likely to be unfavorable, privacy may permit an individual to express his judgments to a group of like-minded people. After a period of germination, such individuals may be more willing to declare their unpopular views in public.[62]

The problem with this idea is the hypothesis that people with weak images of themselves, the ones who desire protection of the malfeasant image, will get together with other weak individuals and that this gathering will lead to an ability to accept the risk factor. The question is: Why would a weak individual ever leave the sanctuary of privacy and expose himself to the evaluation of others? While Professor Gavison proposes a period of germination, one can also see a period of stagnation as being more probable. Professor Gavison's idea is that these weak people will become strong people and will accept the risk of announcing their opinion.[63] The risk factor provides the necessary incentive to becoming autonomous. If a weak person never has to submit his or her image for evaluation, then there would be no incentive to bolster confidence in one's image.

Another facet of the issue is the relationship between the idea that privacy helps create moral autonomy and the idea that privacy enhances an individual's dignity. The idea that privacy is sometimes needed to enhance moral autonomy by protecting an individual's malfeasant image seems fairly paternalistic. The fact that privacy is used to protect an individual means that the individual is unable to protect him or her self. This appears to be an assault on the person's dignity as a human being. Yet, privacy is also used to protect a person's dignity. These two goals of privacy seem to be at odds. How can privacy both

61. *Id.*
62. Gavison, *supra* note 12, at 450.
63. *Id.*

promote an individual's dignity and yet be so paternalistic? The way to reconcile this problem is by returning to the idea "that our concern should not be with the opinions men have of us but rather with the truth of those opinions."[64]

4. *Promote Human Dignity*

Stanley Benn has suggested "that a general principle of privacy might be grounded on the more general principle of respect for persons. . . . To *respect* someone as a person is to concede that one ought to take account of the way in which his enterprise might be affected by one's own decisions."[65] Benn concluded:

> A [person] will have grounds for resentment if the examiner appears insensible to the fact that it is a person he is examining, a subject to whom it makes a difference that he is observed, who will also have a view about what is discovered or demonstrated, and will put his own value on it.[66]

This close connection between the general principle of privacy and respect for persons creates the dangers of computerized data banks. It is the "*resentment* that anyone—even a thoroughly trustworthy official—should be able at will to satisfy any curiosity, without the knowledge let alone the consent of the subject."[67]

A computer matching program used to verify an image that has been presented (i.e. detect the malfeasant image) may impose an invasion of privacy because it infringes upon a person's dignity by treating him or her as an object, rather than a subject. This Note argues that it does not infringe upon a person's dignity. Conversely, to allow privacy to protect the malfeasant image infringes upon a person's dignity by treating him or her as an object rather than as a subject. Huff has agreed that our privacy is invaded when "we are treated as the potential objects of other's gratuitous evaluations rather than as persons."[68] Huff has, however, stated that "our privacy is not invaded by the disclosure of information because we choose to place ourselves in a position where evaluations are expected."[69] Stanley Benn also stated that it is not "the fact of scrutiny as such that is offensive, but only unlicensed

---

64. Huff, *supra* note 43, at 783.

65. Benn, *Privacy, Freedom, and Respect for Persons*, in NOMOS XIII, PRIVACY 1, 8-9 (R. Pennock & J. Chapman eds. 1971) (Yearbook of the American Society for Political and Legal Philosophy).

66. *Id.* at 8.

67. *Id.* at 12 (emphasis added).

68. Huff, *supra* note 43, at 782; *see also* Reiman, *Privacy, Intimacy, and Personhood*, 6 PHIL. & PUB. AFF. 26 (1976).

69. Huff, *supra* note 43, at 782. *See supra* note 44 and accompanying text.

scrutiny."[70]

"Finding oneself an object of scrutiny . . . brings one to a new consciousness of oneself, as something seen through another's eyes."[71] According to Jean-Paul Sartre, "[i]t is only through the regard of the other that the observed becomes aware of himself as an object, knowable, having a determinate character . . . . His consciousness of pure freedom as subject, as originator and chooser, . . . is at once assailed by it . . . ."[72] Sartre describes the human relation as "an obsessional need" to conquer that observer's freedom which is undermining one's belief in one's own freedom.[73] Benn explains the struggle:

> Ego [the Observed's regard of oneself] is aware of Alter [observed as seen through the eyes of the observer] not only as a fact, an object in his world, but also as the subject of a quite independent world of Alter's own, wherein Ego himself is mere object. The relationship between the two is essentially hostile. Each, doubting his own freedom, is driven to assert the primacy of his own subjectivity [as originator and chooser]. But the struggle for mastery, as Sartre readily admits, is a self-frustrating response; Alter's reassurance would be worthless unless to Ego it was freely given, yet the freedom to give it would at once refute it.[74]

Benn's response is that Sartre does not show why the awareness of others as subjects must evoke a hostile response. The observed, recognizing Sartre's dilemma, can infer from it that the observer also sees the observed as a subject and has the same problem.[75] This recognition can create a bond between the observer and the observed rather than a source of resentment when each accords the other the same dignity as a subject.[76] The Huff-type consent is the manifestation of this bond. When the observed initially presents an image to the observer, the observed is still recognized as a subject because he or she is the originator and designer of the image presented. While recognizing that such an act may be an attack upon the observer as subject, the Huff-type consent allows evaluation of the observed's image by the observer. In this respect, the observer is regarded as a subject (an evaluator of the observed's image) and not an object. This way, both can achieve a new consciousness of themselves without resorting to Sartre's hostile dilemma. The computer matching program, which serves to evaluate the image presented, is an effective tool in enhancing Benn's bond, thus enhancing the dignity of both observer and observed.

---

70. Benn, *supra* note 66, at 8.
71. *Id.* at 7.
72. *Id.*; *see* JEAN-PAUL SARTRE, *Le pour-autrui*, in L'ETRE ET LE NEANT Part 3 (1953).
73. Benn, *supra* note 72, at 7.
74. *Id.*
75. *Id.* at 8.
76. *Id.*

Consider, however, the consequences of protecting the malfeasant image from evaluation. The rationale for doing so would be that such evaluation creates resentment by treating the observed as an object. This implies that Sartre is correct regarding his hostile dilemma. Stanley Benn has pointed out that,

> [w]hat Sartre conceived as a phenomenologically necessary dilemma, however, reappears in R.D. Laing's *The Divided Self* as a characteristically schizoid perception of the world, the response of a personality denied free development, trying to preserve itself from domination by hiding away a "real self" where it cannot be absorbed or overwhelmed. The [schizophrenic person's] problem arises because he or she cannot believe fully in his or her own existence as a person. . . .
>
> . . . .
>
> . . . It is because the schizophrenic person cannot believe in himself as a person, that he cannot form [Benn's] "bond," or accept the respectful regard of another.[77]

Therefore, protecting the malfeasant image implies that people need to preserve themselves from domination by being able to hide away a real self which cannot be evaluated. Allowing evaluation of the malfeasant image causes resentment. Protecting the malfeasant image, then, relegates all people to a state of schizophrenia. Since any evaluation causes resentment, they are necessarily unable to form Benn's bond. As Benn has stated, "such persons do not believe in themselves as persons." Such a definition of privacy severely infringes upon human dignity, a function which privacy is supposed to promote.

V. CONCLUSION

This Note has shown that computer matching programs do not create an invasion of privacy when their purpose is to evaluate an image that a person has voluntarily presented. Efforts to regulate computer matching programs should be minimal, in light of the ways that computer matching programs promote the functions of privacy. Regulations need only ensure that the purpose of the match is evaluation or verification (detection of the malfeasant image) and that the results will not be used for any other purpose.

*Rubin E. Cruse, Jr.**

77. *Id.* at 7-8 (citing R.D. LAING, THE DIVIDED SELF (1965)).

* B.A., University of Michigan, Ann Arbor, 1989; J.D., University of Southern California, 1992. The author would like to thank Professor Ronald Garet for his suggestions and input which put this Note into its final form. The author also would like to thank Rubin E. Cruse, Marlene D. Cruse, and Jason E. Cruse, whose suggestions and input have helped put the author into his final form.