University of Baltimore Law Forum

Volume 14
Number 2 *Spring, 1984*

Article 5

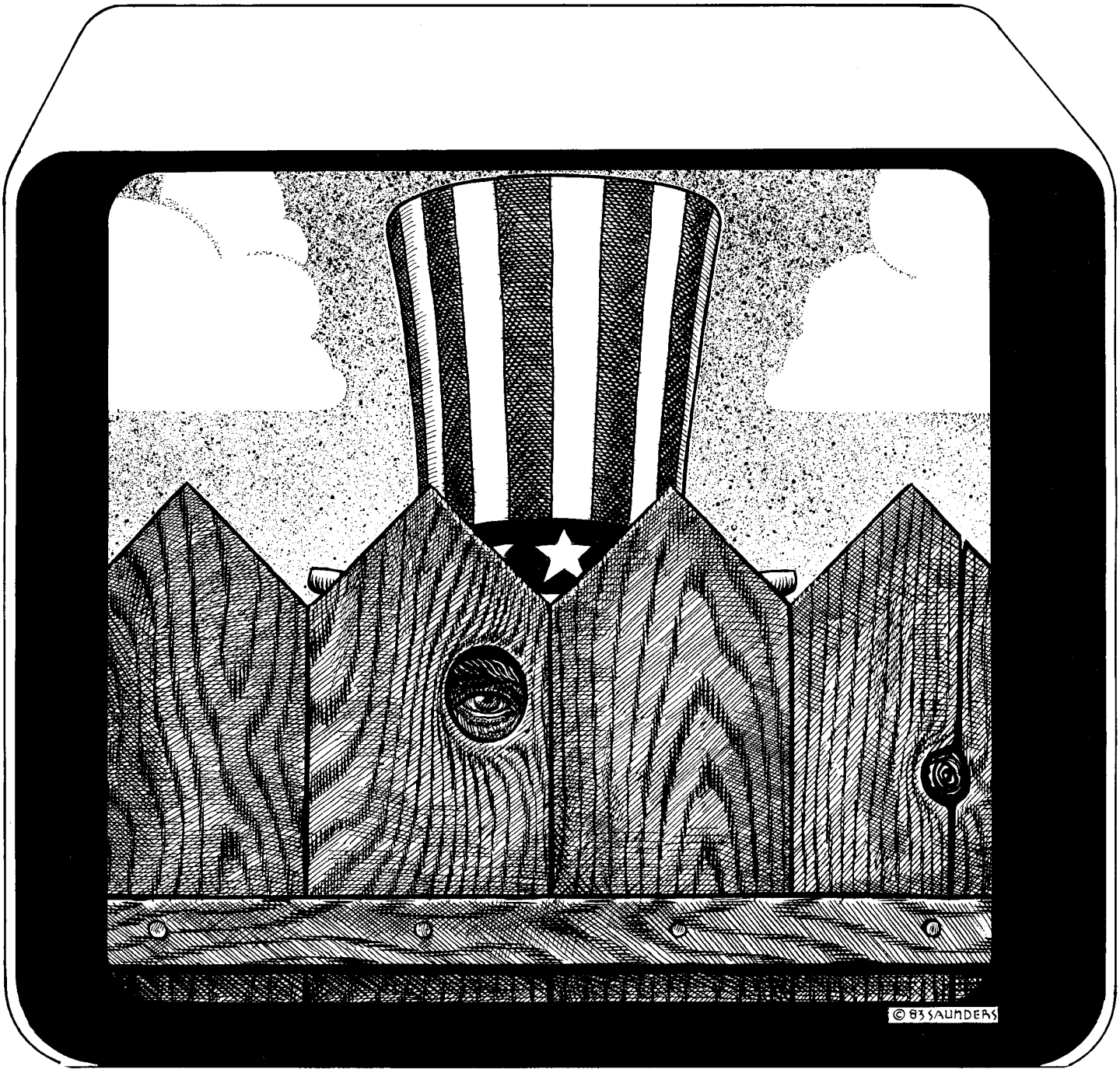
1984

Lost Privacy in the Computer Age: Computer Matching Programs Are Turning Uncle Sam into Big Brother

Miriam Lapp Azrael

LOST PRIVACY IN THE

by Miriam Lapp Azrael



Computer Matching Programs Are Turning Uncle Sam Into Big Brother

COMPUTER AGE

When computer matching programs made headlines in 1981,[1] privacy experts were shocked that government agencies were swapping personal data from separate computer files for unrelated purposes and were outraged to learn that the practice was considered "routine."[2]

In 1982, a Senate subcommittee held hearings to investigate computer matching.[3] The following June, a House subcommittee also inquired into the practice.[4] The House subcommittee's final report, issued in November, 1983, strongly criticized the Office of Management and Budget (OMB) for its lax oversight of computer matching programs and recommended strengthening the Privacy Act of 1974 (the Act)[5] to shore up eroding privacy protections.[6] Representative Glenn English (D. Okla.), Chairman of the House subcommittee that issued the report, introduced H.R. 3743,[7] which calls for the establishment of an independent, non-partisan agency to implement and enforce compliance with the Privacy Act and to develop and coordinate privacy protection policies. This bill is still in committee.[8]

Preserving the privacy of personal information in the computer age is a vexing problem that deserves immediate attention. This article analyzes the impact of computer matching programs on protected rights of privacy and recommends specific legislative solutions to limit privacy intrusions.

Overview

Before computers, information was burdensome to record, quickly forgotten and usually inaccessible. With modern technology, however, anyone with the means and the inclination can maintain in a single computer file the equivalent of twenty single-spaced typed pages, enough for a complete dossier, on every man, woman and child in the United States, and can retrieve information on any particular individual within thirty seconds.[9] The government does not now operate such an information system—not because it lacks the technology to do so, but because the idea of a centralized national data center so shocked the public's consciousness when Congress first considered the idea in the mid-1960's, that the proposal has never seriously been reconsidered.[10] Today, congressional approval of the idea is no longer necessary because computer matching programs are creating a *de facto* national data center.[11]

The computer files of the Internal Revenue Service (IRS), the Social Security Administration and the Census Bureau already contain almost everything there is to know about most American's finances, health and lifestyles.[12] Americans who regularly volunteer personal information about themselves to government agencies are often unaware of the fact that the government uses this information for many purposes, some of which are unrelated to those for which the information was originally gathered. For example, the IRS has allowed the Selective Service System to use computerized taxpayer files to identify draft non-registrants.[13] Soon, the Social Security Administration will open its computer banks to the Immigration and Naturalization Service to assist that agency in locating illegal aliens.[14] Hundreds of computer matches have already been conducted and more are contemplated every day.[15]

Preserving the privacy of personal information in the computer age is a vexing problem that deserves immediate attention.

Federal agencies also match their computer records with computerized records containing personal information about Americans procured from the private sector. The IRS has just purchased from commercial marketing firms computerized lists of American households containing market research projections of their estimated incomes.[16] In preliminary tests soon to be conducted, the IRS will match computerized lists of two million income-producing households in Wisconsin, Indiana, Nevada and Brooklyn, N.Y. with IRS lists of residents of those areas who filed income tax returns for the year 1982. Individuals whose names appear in the commercially prepared lists, but not in the IRS' lists, will be targeted for investigation.[17]

The linkage of computer data banks within the government and between the public and private sectors raises a number of questions: How can the public be sure that the personal data stored in government computer banks and used in computer matches is both current and accurate? Should government agencies be allowed common access to personal information volunteered by individuals for purposes that are unrelated to the objectives of a proposed computer match? Can the public prevent abusive and coercive computer matches from occurring?

Congress sought to resolve these and other questions when it passed the Privacy Act of 1974, which prohibits government agencies from disclosing personal data retrieved from systems of records without an individual's consent.[18] Although the Privacy Act does not expressly mention computer matching, its prohibitions apply to agencies that disclose personal records for use in computer matching programs.[19]

"Raw Hits" and Real People

Federal and state agencies use computer matching programs to detect fraud and abuse in government benefit programs. The process is ideally suited for this purpose because it allows administrators to rapidly compare data contained in separate computer files to identify inconsistencies or similarities that might otherwise escape notice. In 1977, Joseph A. Califano Jr., then Secretary of the Department of Health, Education and Welfare (HEW), in-

Miriam Lapp Azrael *is a third-year student at the University of Baltimore School of Law.*

augurated one of the first computer matches, a program called "Project Match," designed to identify federal employees who were fraudulently obtaining welfare benefits.[20]

In the pilot program (a test-run for an eventual match of five million federal employee records with welfare records from twenty-six states[21]), Secretary Califano matched HEW personnel files with welfare rolls provided by the District of Columbia. His goal was to identify "hits"[22]—individuals listed in both computer files. The initial match identified 638 hits, or 638 HEW employees who were also listed as welfare recipients. Gainfully employed people are generally ineligible for welfare benefits. These 638 employees were therefore automatically suspected of welfare fraud. The unscreened hits, or "raw hits," were targeted for preliminary investigation, after which 480 (75%) were eliminated from further scrutiny for various reasons. The names of the remaining 158 employees (the "solid hits") were forwarded to the Social Security Administration Integrity Staff for further investigation.[23]

Eventually, fifteen welfare mothers employed by HEW were indicted. No one ever told these women prior to their indictments that their names appeared as "hits" in a computer match; hence, they had no opportunity to explain their circumstances before Secretary Califano freely released their names to the press.[24] Of the fifteen indicted welfare mothers, five had their cases dismissed and four had the charges reduced to misdemeanors. The remaining six pled guilty and were sentenced to jail, but none had to serve prison time. For all of its efforts, HEW recovered less than $2,000.[25]

One woman whose case was dismissed was a former nursing student who accepted welfare after she found out that she had cervical cancer. After months of cobalt treatment, she decided to go back to work and found a job at HEW. She immediately told her social worker about her new job and was told not to worry if she received a few more welfare checks. When the checks kept coming, the woman could not resist the temptation to cash them to pay her mounting medical bills. Then Project Match identified her as a hit in its computer match. Soon after, the woman's friends called to tell her that her name was listed in the newspapers as a welfare cheat.

Following her indictment, the woman's court-appointed attorney advised her to plead guilty. Before accepting her plea, the trial judge asked her whether she had ever told her social worker about her job. When she replied that she had, the judge immediately dismissed her case.[26]

As this case and the following case illustrate, the identification of individuals as "hits" in computer matches often results in a presumption of their guilt, requiring individuals to *prove their innocence.*

In August, 1982, the Massachusetts Department of Welfare conducted a computer match to identify welfare recipients who had cash assets in excess of allowable limits. The Department provided to 117 cooperating Massachusetts banks copies of computer files containing social security numbers of all welfare recipients in the state. The banks were requested to electronically match these social security numbers against their customers' social security numbers and bank balances to determine who on the list of welfare recipients had bank account balances that exceeded allowable limits. The banks performed the match and afterwards returned lists of "raw hits." Then, without conducting any prior investigation, the Department sent out termination notices to every welfare recipient listed and referred their names to the Bureau of Special Investigations for fraud inquiry.[27]

One welfare recipient whose benefits were terminated was a resident of a nursing home whose bank account contained a certificate of deposit which she held in trust for a local funeral director to pay the expenses of her own funeral.[28] Another victim of this computer match was a woman who maintained a joint bank account with her brother, who was in the army. Though her brother owned most of the money in the account and the account exceeded the allowable limit by only $276, the Department still terminated her benefits. The termination was especially disturbing because she previously told her social worker about the account, and her social worker "told her not to worry about it."[29]

The Massachusetts Department of Welfare gave these welfare recipients no opportunity to explain their particular situations, except at administrative

appeal hearings at which recipients had the burden of proving that a mistake had been made. Additionally, the Department failed to account for inaccuracies in the computer data, such as transposed social security numbers, that could have mistakenly identified innocent people as welfare cheats and caused the erroneous termination of their benefits. (A class action suit has been filed by terminated welfare recipients to challenge the state's conduct and is now pending in a Massachusetts federal court.[30])

Project Match and the Massachusetts welfare/bank computer match are just two of hundreds of computer matches currently in progress or contemplated by federal or state agencies. Both matches utilized personal data disclosed by individuals for purposes unrelated to the objectives of the matches and used this information without the individuals' consent. Proponents praise computer matching for streamlining government benefit programs and saving taxpayers money. Inspector General Richard F. Kusserow, of the Department of Health and Human Services, calls computer matching a valuable "auditing technique" that can be used to "purify" a data base.[31]

Although shared access to information is an efficient use of resources, expediency must be balanced against important privacy considerations.

Opponents of computer matching programs criticize them for subjecting innocent people to close government scrutiny of their personal records without any prior particularized suspicion of wrongdoing. Privacy experts call computer matching a perversion of the presumption of innocence and a violation of the public's expectation of privacy in their personal records.[32] Yet, computer matching is virtually unregulated. President Reagan zealously promotes the use of computer matching programs and advocates expanding them.[33] The OMB (headed by David Stockman, a Reagan appointee), has the authority to oversee and issue guidelines for computer matching programs, but disclaims authority to prevent proposed computer matches, even those that fail to meet minimum legal requirements.[34] The situation has prompted Professor David Linowes, former chairman of the Privacy Protection Study Commission that first recommended adoption of the Privacy Act, to call computer matching "the biggest threat to privacy today."[35]

Creation Of A *De Facto* National Data Center

The federal government first began computerizing its records soon after World War II, when the Bureau of the Census bought the first commercially available computer.[36] Despite its head-start into the computer age, government information systems are decentralized and notoriously inefficient.[37] In the mid-1960's, the Bureau of the Budget (now the OMB) sought to improve efficiency by proposing the creation of a centralized National Data Center that "would maintain in a single computer all of the statistical data accumulated by scores of different federal agencies about everyone in the United States."[38] Some people thought this idea was "eminently logical,"[39] but others feared that a national data center would lead to uncontrolled intelligence gathering and surveillance operations.

The threat to personal privacy became hard to ignore once advocates of the Center admitted that some data would have to contain personal identifiers.[40] Soon, Congressmen, newspapers, magazines, law reviews and popular books all strongly criticized the idea. Lacking public support, the National Data Center proposal died in Congress in 1968. A chief advocate of the proposal has since conceded that its failure to address privacy considerations was a "gigantic oversight."[41] In 1969, privacy legislation was introduced into Congress, but it was not until after the Watergate scandals that Congress passed the Privacy Act of 1974.

Like a national data center, computer matching affords immediate access by government agencies to vast quantities of personal information. Although shared access to information is an efficient use of resources, expediency must be balanced against important privacy considerations. Professor Arthur R. Miller, an authority on privacy issues, writes that "when an individual is deprived of control over the spigot that governs the flow of information pertaining to him, ...he becomes subservient to those people and institutions that are able to manipulate it."[42] Thus, unregulated expansion of the government's information gathering network could shift the balance of power out of the hands of the electorate and into the hands of the government, which is precisely the danger George Orwell warned of in his book, 1984.

There are also practical reasons why the government should not pry into the personal records of its citizens without their consent. If Americans cannot trust their government to respect their informational privacy, then Americans will no longer comply voluntarily with the government's requests for personal information. The collection of income taxes, for example, which relies almost entirely upon the public's voluntary disclosure of confidential financial information would be grossly undermined. Accordingly, both theoretical and practical reasons exist for supporting privacy protection legislation.

"Records" and "Systems of Records" Under The Privacy Act

By 1974, federal agencies had amassed nearly *three billion* records on individuals and maintained as few as 800 and as many as 6,000 separate data banks.[43] Advances in computerized data systems and their effect upon personal privacy prompted Congress to enact the Privacy Act. The Legislative History contains the following references to computers:

> (2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information.
>
> ...
>
> (5) in order to protect the privacy of individuals identified in information systems maintained by federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use and dissemination of information by such agencies.[44]

Under the Act, individuals may gain access to their government files or to

information pertaining to them in the possession of a government agency and may correct information that is inaccurate, irrelevant, untimely or incomplete.[45] In addition, the Act establishes standards of conduct for the government's collection, maintenance, use and disclosure of personal records.[46]

The Act does not, however, apply to all information maintained by government agencies. It only applies to those records maintained within a system of records. To qualify as a "record," information maintained by a government agency must contain a personal identifier such as a person's name, social security number "or other identifying particular assigned the individual, such as a finger or voice print or a photograph."[47] To qualify as a "system of records," the records must be "retrieved" by a personal identifier.[48] The government's disclosure of information that is neither a "record" nor contained within a "system of records" is unreviewable under the Act.

The leading case interpreting the "system of records" definition is *Smiertka v. Department of Treasury*,[49] in which the court held that the Privacy Act is inapplicable where the particular record disclosed was incapable of being retrieved by the plaintiff's personal identifier, even though it was retrievable by other reasonable means. Smiertka, a discharged IRS employee, sued the Department of the Treasury to obtain access under the Privacy Act to certain daily investigation reports. These reports, prepared by IRS investigators as routine summaries of their work, contained references to the agency's investigation of Smiertka that led to his eventual discharge. The court upheld the agency's denial of access to these reports on the grounds that they were not indexed according to Smiertka's name or other personal identifier. The fact that they could be retrieved easily by the name of the investigator who wrote the reports was "wholly beside the point."[50]

The holding in *Smiertka* was explained in *Savarese v. U.S. Department of Health, Education and Welfare*,[51] in which the court reasoned that if it upheld a Privacy Act claim where the disclosure did not result from the retrieval of plaintiff's records from within a system of records, then

> no government employee could utter a single word concerning any person without first reviewing all systems of records within the agency to determine whether or not the information in question was contained therein.... It borders on the absurd to contend that all officals should have a pansophic recall concerning every record within every system of records within the agency.[52]

Recent cases have followed this analysis. In one particularly troubling case, *Olberdung v. U.S. Department of Defense*,[53] decided in June, 1983, the Court of Appeals for the Eighth Circuit upheld the lower court's dismissal of the plaintiff's Privacy Act claim on the grounds that the Army General who disclosed the plaintiff's psychiatric test results, without the plaintiff's consent, recalled the information from his own memory and did not retrieve the information from a "system of records." The fact that the test results could have been retrieved from the Madigan Army Medical Center's system of records which indexed the records according to the plaintiff's name was held to be immaterial.

As a threshold test for bringing agency conduct within the scope of the Privacy Act, the "system of records" definition is too narrow.

This case illustrates the inadequacy of the "system of records" definition. The object of the Privacy Act is to protect the privacy of individuals. An unauthorized disclosure of personal information invades an individual's privacy regardless of the manner in which the information is retrieved. An individual whose psychiatric test results are disclosed without his prior consent suffers no less of a loss of privacy when these records are retrieved from a system of records, than when they are recollected from a bureaucrat's own memory.

As a threshold test for bringing agency conduct within the scope of the Privacy Act, the "system of records" definition is too narrow. It freely exempts invasive disclosures on purely mechanical grounds. But assuming that an agency's recordkeeping has passed through this narrow hoop, its conduct may still escape Privacy Act scrutiny through the trapdoor of one of the Act's twelve exceptions.[54]

One such exception is the "routine use" exception.[55] The term "routine use" is defined as "the use of [a] record for a purpose which is *compatible* with the purpose for which it was collected" [emphasis added].[56] Agencies are required to publish annual notices in the Federal Register describing each routine use of records contained within each system of records. This notice must indicate the purpose for each purported routine use and the categories of each user.[57]

Privacy experts express grave concern over the breadth of this exception and over the fact that the twelve exceptions have all but swallowed up the general rule that prohibits non-consensual disclosures of personal information.[58] Moreover, the courts have not critically analyzed the application of this exception in particular circumstances. In *Parks v. I.R.S.*,[59] for example, the Court of Appeals for the Tenth Circuit held that an agency's non-consensual disclosure of the identities of employees who contributed to savings bond solicitations was not a "routine use" of agency information, not because the purported routine use failed to meet substantive definitional requirements, but rather because the agency failed to publish a notice in the Federal Register. Privacy experts wonder whether all an agency need do is publish Federal Register notices to qualify their disclosures of personal information under the "routine use" exception to escape Privacy Act compliance.[60] John H. Shattuck, National Legislative Director of the American Civil Liberties Union, is concerned that the test of "compatibility" under the "routine use" exception has become so elastic that it is now virtually ignored. In his prepared statement submitted to Rep. Glenn English's House subcommittee in June, 1983, Mr. Shattuck commented that "[i]n practice, 'routine use' has come to mean any use which an agency deems to be appropriate. So long as a 'notice of routine use' is published in the Federal Register, just about anything goes."[61]

Computer Matching Under The Privacy Act

The Privacy Act does not specifically mention computer matching, and as

yet, there is no body of case law on the subject. If computer matches were subject to the Privacy Act, agencies would have to notify and obtain the prior written consent of all individuals whose computer records were involved in any computer matching program.[62] The time and expense involved would be prohibitive. In Project Match, for example, the data base of just one of the computer files involved in the match contained the records of two million individuals.[63] Certainly, if computer matching did not fall within one of the exceptions to the Privacy Act, it would come to an abrupt halt.

Proponents of computer matching do all they can to ensure that computer matching programs are exempt from Privacy Act disclosure requirements. In Computer Matching Guidelines promulgated by the OMB in 1975 and overhauled by the Reagan administration in 1982,[64] agency disclosures of personal records to conduct computer matches is a permissible routine use of agency records.[65] The OMB does not, however, enforce the substantive requirements to qualify disclosures under this exception. Lax enforcement troubles even those who advocate computer matching.

In December, 1982, Thomas F. McBride, Associate Dean of Stanford Law School and Former Inspector General of the U.S. Department of Labor, testified before a Senate subcommittee investigating computer matching programs and candidly admitted that

> I have always been somewhat baffled by what seems to me to be a somewhat illusory protection, the routine use clause of the Privacy Act. Basically, what those [agencies] conducting matches have done, those subject to the Privacy Act, is to publish notice and add the match as a routine use [of agency records], even though it did not seem to have a clear nexus to the purpose for which the data was originally collected.... I've often been puzzled as to whether there is some distortion of the intention of the legislation. Routine use has become pro forma.[66]

Six months later, Christopher DeMuth, OMB Administrator for Information and Regulatory Affairs, testified before Rep. English's House subcommittee and shocked Rep. English by revealing that the OMB essentially rubberstamps agencies' purported routine uses, thus confirming former Inspector General McBride's observations. When asked by Rep. English whether qualifying as a routine use had any substantive element apart from the procedural requirement of publishing Federal Register notices, Mr. DeMuth replied that

> [a]gencies come to us [OMB] and ask us about specific systems [of records] and how [their proposed routine use] fits within the law. They describe to us their programs and the nature of information and what kinds of uses were made of it in the past. We try to settle these things on a case-by-case basis. *We do not have any authority to say yes or no as to a given routine use* [emphasis added].[67]

"In practice, 'routine use' has come to mean any use which an agency deems to be appropriate. So long as a 'notice of routine use' is published in the Federal Register, just about anything goes."

Later in his testimony he added

> My understandings of the Privacy Act and OMB's regulatory authority under the act is that it does not give us the authority to tell an agency head or any agency's senior Privacy Act official that a certain use would not fit within the routine use definition of the act...— to overrule the agency official administratively. Routine use determinations are given to the agency head ultimately under the act ...[*we*] *cannot deny routine uses* [emphasis added].[68]

If OMB, which is authorized to oversee implementation of the Privacy Act, is not effectively policing compliance with its substantive requirements, then who is? The answer is, unfortunately, no one. Enforcement, such as it is, is left entirely up to the public.

Recovery Under The Privacy Act

To recover under the Act for an agency's unauthorized disclosure of personal information, whether in the course of computer matching or otherwise, an individual must establish that:

(1) the agency acted intentionally or willfully;[69]
(2) he thereby sustained an "adverse effect";[70] and
(3) he suffered an out-of-pocket loss. (Courts have limited recovery to out-of-pocket losses for physical injuries only; emotional or mental injuries are non-compensable.[71])

John Shattuck says that "short of proving that one has been mutilated by a government computer," this damage requirement is impossible to meet. Thus, plaintiffs who bring Privacy Act claims seldom recover damages.[72]

Apart from the difficulty of proving damages, the Act is unenforceable because it fails to provide injunctive relief for wrongful disclosure. In other words, an individual who wishes to challenge the Internal Revenue Service's disclosure of his tax return information to the Selective Service System for a computer match to identify draft nonregistrants can do nothing to prevent the computer match from occurring. His only remedy is to collect damages after the match has been conducted and after his privacy has been violated, and then, only if he can establish the three elements listed above.

Recommendations For Privacy Act Reform

To prevent further erosion of the privacy protections Congress sought to implement under the Privacy Act, Congress should:

1. Pass H.R. 3743,[73] which calls for the creation of an independent, nonpartisan, permanent Privacy Protection Commission to develop and coordinate privacy protection policies and oversee compliance with the Privacy Act.

2. Limit and refine the definition of "routine use" to prohibit the government's unauthorized use of personal information for any purpose that is inconsistent with the reasonable ex-

pectations of individuals whom the government asks to disclose personal information.

3. Provide injunctive relief for wrongful disclosures even where no "adverse effect" results from the disclosure.

4. Require that all agencies conducting computer matches publicly disclose (i) a cost/benefit analysis prior to the match, (ii) a description of all records to be compared in the match, and (iii) the basis for determining that the objectives of the match are compatible with the purposes for which the information was originally collected and the reasonable expectations of the parties from whom the information was collected.

Conclusion

Computer matching is a tool; it is not evil in itself. Like any tool, its potential for harm rests in the sound discretion of its user. In enacting the Privacy Act, Congress sought to limit the government's discretion in its use and handling of personal information. Unfortunately, as it is presently interpreted, the Act falls short of accomplishing this goal.

Many bureaucrats believe that "only those who have something to hide" care about safeguarding the privacy of their personal records.

Many bureaucrats believe that "only those who have something to hide" care about safeguarding the privacy of their personal records.[74] Proponents of computer matching, many of whom share this view, have come to regard the Privacy Act as a regulatory inconvenience that stands in the way of fiscal efficiency. Administrators who disagree with the objectives of the Privacy Act have craftily devised ways of getting around it. Courts have altogether ignored the spirit of the Act and enforce only its procedural requirements. If computer matching is permitted to continue unchecked, the government will soon have at its disposal the resources of a national data center and the license to use personal information stored within its data banks as a means of political coercion.

The increasing dilution of informational privacy protection in this country also has international implications that few people realize. Recently, the Council of Europe sent a directive to the Reagan administration suggesting that transborder data flows may be interrupted or "seriously restricted," unless the United States implements stronger privacy protection at the national level. The Reagan administration has responded by stating that "[t]he U.S. legal structure provides adequate safeguards [sic] protection of personal privacy."[75] Considering the total abdication by the OMB of its oversight authority under the Privacy Act and the concurrent pressure by the Reagan administration to expand computer matching of unrelated personal information, this statement is indefensible. If those in power consider current privacy protections to be "adequate," then George Orwell's predictions for 1984 are more accurate than we think.

Notes

1 *See, e.g.,* Kirchner, *Privacy: A History of Computer Matching in Federal Government,* COMPUTERWORLD, December 14, 1981, at 1.

2 *See infra* note 55 and accompanying text.

3 *Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs: Hearings Before the Subcomm. on Oversight of Government Management of the Senate Committee on Government Affairs,* 97th Cong., 2d Sess. (1982) [hereinafter cited as *Computer Matching Hearings*].

4 *Oversight of the Privacy Act of 1974: Hearings Before the Subcomm. on Government, Information, Justice and Agriculture of the House Committee on Government Operations,* 98th Cong., 1st Sess. (1983) [hereinafter cited as *Privacy Act Hearings*].

5 5 U.S.C. § 552a (1982).

6 J. Brooks, WHO CARES ABOUT PRIVACY? OVERSIGHT OF THE PRIVACY ACT OF 1974 BY THE OFFICE OF MANAGEMENT AND BUDGET AND BY THE CONGRESS, H. Rep. No. 455, 98th Cong., 1st Sess. 23-24 (1983).

7 98th Cong., 1st Sess. (1983).

8 Telephone conversation with the Office of the House Committee on Government Operations (February 21, 1984).

9 Soma and Wehmhoefer, *A Legal and Technical Assessment of the Effect of Computers on Privacy,* 60 DEN. L.J. 449, 451-52 (1983).

10 D. Flaherty, *Privacy and Government Data Banks: An International Perspective* 263 (1979); *See generally Privacy and Efficient Government: Proposals for a National Data Center,* 82 HARV. L. REV. 400 (1968).

11 *Privacy Act Hearings, supra* note 4, at 269.

12 Cronkite, *Foreword* to D. BURNHAM, THE RISE OF THE COMPUTER STATE at viii (1983).

13 *Use of Internal Revenue Service Resources and Taxpayer Information for Draft Registration and Welfare Restriction Purposes: Hearings Before the Subcomm. on Commerce, Consumer and Monetary Affairs of the House Committee on Government Operations,* 97th Cong., 2d Sess. 58-59 (1982) (statement of Thomas K. Turnage, Director of Selective Service System). *See also Computer Matching Hearings, infra* note 8, at 83, 115-116.

14 48 Fed. Reg. 6786 (1983); *See also Privacy Act Hearings, supra* note 4, at 276.

15 *Computer Matching Hearings, supra* note 3, at 112 (prepared statement of John H. Shattuck, National Legislative Director, American Civil Liberties Union).

16 *Private Computers' Income Data to Aid I.R.S. in Hunt for Evaders,* N.Y. Times, August 29, 1983, at A1; U.S. News and World Report, October 24, 1983, at 41.

17 *Income List Tested in Tax Evasion Hunt,* The Baltimore Sun, December 25, 1983 at A21; *See also IRS Pilot Program Taps County Computers,* The Baltimore Sun, March 18, 1984 at G4.

18 5 U.S.C. 552a(b) (1982).

19 Office of Management and Budget Revised Computer Matching Guidelines, 47 Fed. Reg. 21656 (1982).

20 Kirchner, *supra* note 1, at 3.

21 *Computer Matching Hearings, supra* note 3, at 113 (prepared statement of John H. Shattuck, National Legislative Director, American Civil Liberties Union).

22 *See* Office of Management and Budget Revised Computer Matching Guidelines, *supra* note 19 (definition of "hit").

23 *Computer Matching Hearings, supra* note 3, at 114 (prepared statement of John H. Shattuck, National Legislative Director, American Civil Liberties Union).

24 *Id.*

25 Hendricks, *How Not to Catch Welfare Cheaters,* The Washington Post, July 1, 1979, at C8, *quoted in Computer Matching Hearings, supra* note 3, at 114.

26 *Computer Matching Hearings, supra* note 8, at 142-43 (statement of Robert Ellis Smith, Publisher of PRIVACY JOURNAL).

27 *Computer Matching Hearings, supra* note 3, at 223 (testimony of William T. Hogan, Secretary, Executive Office of Human Services, State of Massachusetts).

28 *Id.* at 106-107.

29 *Id.* at 107.

30 Lessard v. Spirito, Civil Action No. 82-3389-MA (D. Mass. filed November 5, 1982).

31 *Computer Matching Hearings, supra* note 3, at 12.

32 *See, e.g., id.* at 99-107.
Although no court has yet ruled on the constitutionality of computer matching, Supreme Court decisions interpreting the scope of permissible government intrusions into privacy indicate that computer matching is constitutional. *See* Miller v. U.S., 425 U.S. 435 (1976) (bank customer had no legitimate expectation of privacy under the fourth amendment in bank

records disclosed by his bank in compliance with a government subpoena because the records were the bank's own property); *But, cf.* Katz v. U.S., 389 U.S. 347 (1967) (the fourth amendment "protects people not places"); Whalen v. Roe, 429 U.S. 589 (1977) (upholding a New York law requiring prescribing physicians to submit to the state, for its centralized computer bank, copies of every prescription written for certain lawful drugs having an illegal market); and Paul v. Davis, 424 U.S. 693 (1976), *reh'g denied* 425 U.S. 985 (1976) (sheriff did not violate plaintiff's right of due process by disclosing plaintiff's name to local merchants in a list of "active shoplifters" that resulted in damage to plaintiff's reputation).

[33] *See, e.g.*, 18 WEEKLY COMP. PRES. DOC. 335 (March 18, 1982). In his remarks at the Annual Washington Policy Meeting of the National Association of Manufacturers, President Reagan referred to computer matching as "one of the most innovative techniques" yet developed by Inspectors General in the "campaign against waste and fraud" in government programs. Later, in the same address, President Reagan remarked, "This administration wants to achieve economic growth by reducing government intrusions in order to expand human freedom, value individual excellence, and make the American dream a reality for our citizens." *Id.* at 341. The President was apparently unaware of the ironic inconsistency of these two statements.

[34] *See infra* notes 67 and 68, and accompanying text.

[35] Kirchner, *supra* note 1, at 11.

[36] A. MILLER, THE ASSAULT ON PRIVACY 55 (1971).

[37] *Privacy and Efficient Government: Proposals for a National Data Center*, 82 HARV. L. REV. 400, 401 (1968); A. MILLER *supra* note 36, at 55.

[38] D. BURNHAM, *supra* note 12, at 189.

[39] A. MILLER, *supra* note 36, at 57.

[40] *Id.*

[41] *Id.*

[42] A. MILLER, *supra* note 36, at 25; *See also* Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y. U. L. REV. 962 (1964); Bloustein, *Privacy is Dear At Any Price, A Response to Professor Posner's Economic Theory*, 12 GA. L. REV. 429, 447 (1978).

[43] J. O'REILLY, FEDERAL INFORMATION DISCLOSURE: PROCEDURES, FORMS AND THE LAW § 20.01, at 20-3 (1977) [hereinafter cited as J. O'REILLY]; Today, the federal government operates "over 18,000 main frame computerized systems... with additional ones being added almost daily." *Computer Security in the Federal Government and the Private Sector: Hearings Before the Subcomm. on Oversight Management of the Senate Committee on Government Affairs*, 98th Cong., 1st Sess. 78 (1983) (prepared statement of Richard P. Kusserow, Inspector General, Dept. of Health and Human Services).

[44] 1974 U.S. CODE CONG. & AD. NEWS 6916.

[45] 5 U.S.C. § 552a(d) (1982).

[46] 5 U.S.C. § 552a(e) (1982).

[47] 5 U.S.C. § 552a(4) (1982).

[48] 5 U.S.C. § 552a(5) (1982).

[49] 447 F. Supp. 221 (D.D.C. 1978), *remanded on other grounds*, 604 F.2d 698 (D.C. Cir. 1979).

[50] *Id.* at 228.

[51] 479 F. Supp. 304 (N.D.Ga. 1979), *aff'd*, 620 F.2d 298 (11th Cir. 1981), *cert. denied*, 449 U.S. 1078 (1981).

[52] *Id.* at 308.

[53] 709 F.2d 621 (8th Cir. 1983).

[54] 5 U.S.C. § 552a(b)(1)-(12) (1982).

[55] 5 U.S.C. § 552a(b)(3) (1982).

[56] 5 U.S.C. § 552a(7) (1982).

[57] 5 U.S.C. § 552a(e)(4)(D) (1982).

[58] *Privacy Act Hearings*, *supra* note 4, at 260 (testimony of Ronald Plesser, Esquire, of the Washington, D.C. law firm of Blum & Nash and former Counsel to the Privacy Protection Study Commission).

[59] 618 F.2d 677 (10th Cir. 1980).

[60] *See, e.g., Privacy Act Hearings*, *supra* note 4, at 276 (prepared statement of John H. Shattuck, National Legislative Director, American Civil Liberties Union).

[61] *Id.*

[62] 5 U.S.C. § 552a(b) (1982).

[63] *Computer Matching Hearings*, *supra* note 3, at 5 (testimony of Richard P. Kusserow, Inspector General of the Department of Health and Human Services).

[64] 47 Fed. Reg. 21656 (1982).

[65] *Id.* at 21657, § 5(d).

[66] *Computer Matching Hearings*, *supra* note 3, at 24.

[67] *Privacy Act Hearings*, *supra* note 4, at 92.

[68] *Id.* at 113.

[69] 5 U.S.C. § 552a(g)(4) (1982).

[70] 5 U.S.C. § 552a(g)(1)(D) (1982).

[71] Albright v. U.S., 631 F.2d 915 (D.C. Cir. 1980).

[72] *Privacy Act Hearings*, *supra* note 4, at 282.

[73] *See supra* note 7.

[74] Anderson, *Social Security Turns to Raw Big Brotherism*, The Washington Post, June 11, 1982. *See also* D. BURNHAM, *supra* note 12, at 212: "Mr. Reagan and his advisors appear to live in a world where the desire for orderliness dominates other considerations. Perhaps, because most of the members of the Reagan administration have so long held positions of corporate or political power, they find it hard to conjure up situations where the institutions they are associated with might some day turn on them. The implicit assumptions of the Privacy Act... have not been the hallmark of the Reagan team or the permanent cadre of the federal government."

[75] *Privacy Act Hearings*, *supra* note 4, at 259 (testimony of John H. Shattuck, National Legislative Director, American Civil Liberties Union).