Computer Matching: *Should It Be Banned?*

Since discovering the technique of computer matching several years ago, government managers have been invoking this computer tool in the attempt to root out waste and fraud in their programs. Is computer matching an indispensable tool for government administrators? Or a trampling on individual rights? In the following articles, two experts debate the pros and cons.

INTRODUCTION

On November 9, 1977, the Secretary of the Federal Department of Health, Education and Welfare (HEW), Joseph A. Califano, Jr., announced what he believed was a bold initiative to eliminate welfare abuse: *Project Match*. Califano's plan called for taking computerized files of federal employees and matching them against computerized files of state welfare rolls.

That proposal was met with a storm of criticism from some quarters on the grounds that such a project constituted a flagrant violation of individual privacy. HEW charged ahead anyway, marking that project as the first instance of computer matching in United States history.

Since then, computer matching has really taken off both at the federal and the state levels. According to Norma Rollins, director of the privacy project for the New York Civil Liberties Union, more than 10,000 computer matches have since been carried out by agencies of the federal and state governments and by the private sector.

Now, once again, the issue of computer matching is coming to a boil. One reason—as we have been reminded countless times—is that this is the Orwellian year of 1984. Another is that, during the past several years, computer technology has advanced at a breathless pace, making computer matches more cost effective than they once were.

But there is another, more ominous reason why the computer-matching issue is commanding attention. In the past, computer-matching projects were aimed mostly at poor people and others who were beneficiaries of government programs like welfare, food stamps, and unemployment compensation. But now, as Rollins and others point out, computer-matching projects are beginning to reach out and embrace the American middle class.

For instance, the Internal Revenue Service (IRS) is now matching census information and state motor vehicle records against federal income tax returns. Such computerized records reveal the type car, home, and community a person lives in. By matching that kind of information against a person's *reported* income, IRS can flag anomalies.

John Shattuck

Richard Kusserow

Also, in an effort to find out who has not registered, the Selective Service System is now planning to match their registrants' list against lists of male licensed drivers between the ages of 18 and 20.

In response to the growing concern, Congress, during the past 18 months, has conducted several hearings probing privacy issues, including the threat posed by computer matching. One proposal being studied now is to create a federal Privacy Commission to keep a permanent, watchful eye on government and private-sector activities that tread on individual privacy rights.

To prod discussion on this vital issue, *Communications* sought out as authors one of the leading opponents of computer matching—and one of the leading proponents. In the following article, John Shattuck, the executive director of the Washington office of the American Civil Liberties Union, argues that computer matching is a serious threat to individual liberty—and should be stopped. In the follow-on piece, the Inspector General for the federal Department of Health and Human Services, Richard Kusserow, insists that the federal government must make use of computer matching.

Gene Dallaire

COMPUTER MATCHING IS A SERIOUS THREAT TO INDIVIDUAL RIGHTS

JOHN SHATTUCK

More and more frequently, government agencies have been employing a new investigative technique: the matching of unrelated computerized files of individuals to identify suspected law violators. This technique—*computer matching*—provides a revolutionary method of conducting investigations of fraud, abuse, and waste of government funds. It permits the government to screen the records of whole categories of people, such as federal employees, to determine who among them also falls into separate, supposedly incompatible categories, such as welfare recipients.

Computer matching raises profound issues concerning individual privacy, due process of law, and the presumption of innocence. It also poses serious questions about cost effectiveness and the internal management of government programs.

COMPUTER MATCHING VERSUS INDIVIDUAL RIGHTS

To understand the impact of computer matching on individual rights, it is first necessary to grasp the difference between a computer-matching investigation and a traditional law enforcement investigation.

A traditional investigation is triggered by some evidence that a person is engaged in wrongdoing. This is true for cases of tax evasion, welfare fraud, bank robbery, or traffic speeding. The limited resources of law enforcement usually make it impracticable to conduct dragnet investigations. More importantly, our constitutional system bars the government from investigating persons it does not suspect of wrongdoing.

A computer match is not bound by these limitations. It is directed not at an individual, but at an entire category of persons. A computer match is initiated not because any person is suspected of misconduct, but because his or her category is of interest to the government. What makes computer matching fundamentally different from a traditional investigation is that its very purpose is to generate the evidence of wrongdoing required before an investigation can begin. That evidence is produced by "matching" two sets of personal records compiled for unrelated purposes.

There are four ways in which a computer match differs from a conventional law enforcement investigation in its impact on individual rights:

(1) Fourth Amendment

The Fourth Amendment protects against unreasonable searches and seizures, the most blatant of which have been "fishing expeditions" directed against large numbers of people. From the "writs of assistance" used in the eighteenth century by royal revenue agents, to door-to-door searches for violations of the British tariff laws in the American Colonies, to the municipal code inspections of the twentieth century to enforce health and safety standards, the principle that generalized fishing expeditions violate the right to be free from unreasonable searches has held firm in American law.

That principle is violated by computer matching. The technique of matching unrelated computer tapes is designed as a general search. It is not based on any preex-

isting evidence to direct suspicion of wrongdoing to any particular person. Although systematic searches of personal records are not as intrusive as door-to-door searches, the result is the same: a massive dragnet into the private affairs of many people.

(2) Presumption of Innocence

People in our society are not forced to bear a continuous burden of demonstrating to the government that they are innocent of wrongdoing. Although citizens are obliged to obey the law—and violate it at their peril—presumption of innocence is intended to protect people against having to prove that they are free from guilt whenever the government investigates them.

Computer matching can turn the presumption of innocence into a presumption of guilt. For instance, Massachusetts welfare recipients have been summarily removed from welfare rolls as the result of a computer match. These people fought for reinstatement based on information the state neglected to consider after their names appeared as "hits" in the match.

Another example of this "presumption of guilt" occurred three years ago in Florida. The state's attorney for a three-county area around Jacksonville obtained case files for all food stamp recipients in the area. He then launched fraud investigations against those receiving allotments of more than $125 a month. A federal court of appeals invalidated the file search and enjoined the investigation on the ground that the targeted food stamp recipients were put in the position of having to prove the allotment they had received was *not* based on fraud. Construing the Food Stamp Act, the Court held that "it did not allow the [state food stamp] agency to turn over files . . . for criminal investigation *without regard to whether a particular household has engaged in questionable behavior.*"

Once a computer match has taken place, any person whose name appears as a "raw hit" is presumed to be guilty. In part, this is because the technology of computer matching is so compelling and in part because its purpose—the detection of fraud and waste—is so commendable. The worst abuses of computer matching, such as summary termination of welfare benefits, have occurred when authorities have casually transformed this "presumption" into a conclusive proof of guilt.

(3) Privacy Act

The most important principle governing collection and use of personal information by the government is that the individual has a right to control information about himself and to prevent its use without his consent for purposes wholly unrelated to those for which it was collected. This principle is imperfectly embodied in the Privacy Act of 1974.

The Privacy Act restricts disclosure by federal agencies of personally identifiable information—*unless* the subject consents. There are two major exceptions. The first involves a "routine use," defined as "the use of (a) record for a purpose which is compatible with the purpose for which it was collected." The second involves a "law enforcement" disclosure, which enables an agency to be responsive to a request by another agency for information relevant to the investigation of a specific violation of law.

When computer matching was in its infancy, the Privacy Act was correctly perceived by several federal agencies to be a major stumbling block. The Civil Service Commission initially balked in 1977 at the plans of Health, Education and Welfare (HEW) Secretary Joseph Califano to institute a match of federal employee records and state welfare rolls, on the ground that the use of employee records for such a purpose would violate the Privacy Act. The Commission's General Counsel, Carl F. Goodman, stated that the proposed match could not be considered a "routine use" of employee records, since the Commission's "information on employees was not collected with a view toward detecting welfare abuses." Similarly, it could not be considered a "law enforcement" use, continued Goodman, since "at the 'matching' stage there is no indication whatsoever that a violation or potential violation of law has occurred."

This reasonable interpretation of the Privacy Act soon gave way to a succession of strained readings. Since enforcement of the Privacy Act is left entirely to the agencies it regulates, it is hardly surprising that the agencies have bent the Act to their own purposes. They have now miraculously established that computer matching is a "routine use" of personal records. All that is required, they say, is to publish each new computer matching "routine use" in the *Federal Register.*

The Privacy Act has now been so thoroughly circumvented by executive action that it can no longer be seen as an effective safeguard. Nevertheless, the principle underlying the Act—that individuals should be able to exercise control over information about themselves that they provide to the government—is a bedrock principle of individual privacy. That principle is at war with the practice of computer matching.

A traditional investigation is triggered by some evidence that a person has engaged in wrongdoing. What makes computer matching fundamentally different is that its very purpose is to generate the evidence of wrongdoing required before an investigation can begin.

Under the Privacy Act of 1974, the individual has a right to control information about himself and to prevent its use without his consent for purposes wholly unrelated to those for which it was collected. That principle is at war with the practice of computer matching.

(4) Due Process of Law

Once a computer match has taken place, it will result in a series of hits. All those identified are in jeopardy of being found guilty of wrongdoing. To the extent that they are not given notice of their situation and an adequate opportunity to contest the results of the match, they are denied due process of law.

This is precisely what has happened in several matching programs. For example, the results of Secretary Califano's Operation Match were kept secret from federal employees whose records were matched with welfare rolls, because the Justice Department viewed the investigation "as a law enforcement program designed to detect suspected violations of various criminal statutes." The Justice Department ordered the Civil Service Commission not to notify any of the federal employees whose names showed up as hits, since "[t]he premature discussion of a specific criminal matter with a tentative defendant is in our view inimical to the building of a solid prosecutorial case." In Massachusetts, welfare authorities have terminated benefits of persons showing up as hits without even conducting an *internal* investigation.

This approach makes a mockery of due process. Due process is the right to confront one's accuser and introduce evidence to show that the accuser is wrong. When the accuser is a computer tape, the possibility of error is substantial. Keeping the subject of a raw hit in the dark increases the likelihood of an error's going undetected.

SOME COMMENTS ON THE OFFICE OF MANAGEMENT AND BUDGET'S (OMB's) GUIDELINES

Since 1979 computer matching at the federal level has been regulated by guidelines issued by the OMB. These guidelines, which were considerably looser in May 1982, are intended to "help agencies relate the procedural requirements of the Privacy Act to the operational requirements of computerized matching." Although Kusserow cites the guidelines as evidence of the federal government's concern about privacy protection, in fact, they constitute an effort to paper over the profound conflict between (1) the Privacy Act principle that personal records are to be used by federal agencies only for purposes compatible with those for which they were compiled and (2) the computer matching practice of joining personal records compiled for wholly unrelated purposes.

OMB's matching guidelines have rendered meaningless the central principle of the Privacy Act. In 1980, for instance, the Office of Personnel Management (OPM) published a notice in the *Federal Register* concerning its proposed use of personnel records for a matching program to help the Veterans' Administration (VA) verify the credentials of its hospital employees. The notice dutifully stated that the proposed match of OPM and VA records was a "routine use," which it explained as follows:

> "An integral part of the reason that these records are maintained is *to protect the legitimate interests of the government* and, therefore, such a disclosure is compatible with the purposes for maintaining these records."

Under that broad justification any disclosure or matching of personal records would be permissible, since all federal records are purportedly maintained for the "legitimate interests of the government."

The guidelines, on which Kusserow so heavily relies, contain no requirements or limitations on the conduct of computer matching in these critical areas:

(1) **The nature of the record systems to be matched**—There are no personal records, no matter how sensitive (e.g., medical files, security clearance records, intelligence records), that are beyond the reach of computer matching for any investigative purpose.

(2) **The procedures to be followed in determining the validity of hits**—No particular procedures are required to insure that the subjects of hits are afforded due process of law.

(3) **The standards and procedures to be followed for securing OMB approval of a proposed match**—Since the first guidelines were promulgated in 1979, OMB has not disapproved a single computer match.

(4) **The projected costs and benefits of a proposed match**—The 1982 guidelines have deleted all reference to cost-benefit analyses or reports on computer matches. It is entirely at an agency's discretion whether to undertake a proposed match or to report the costs and benefits of the match.

It is impossible not to conclude that computer matching at the federal level is a huge unregulated business,

the only clear effect of which to date has been the undermining of individual privacy.

SOME EXAMPLES OF COMPUTER MATCHING

In the seven years since the technique was first used, over 200 computer matches have been carried out. At the federal level there have been matches for a wide variety of investigative purposes, using a broad range of personal record systems of varying degrees of sensitivity.

These include matches of federal employee records maintained by the Civil Service Commission with files of persons receiving federal Aid to Families with Dependent Children, to investigate "fraud"; federal personnel records maintained by OPM with the files of VA hospital employees, to check "accreditation"; federal personnel records of Agriculture Department employees in Illinois with Illinois state files on licensed real estate brokers, to "ascertain potential conflicts of interest"; Internal Revenue Service (IRS) records of taxpayer addresses with lists of individuals born in 1963 supplied by the Selective Service System, to locate suspected violators of the draft registration law; and Labor Department files of persons entitled to receive Black Lung benefits with Health and Human Services (HHS) records of Medicare billings, to investigate double-billing medical fraud.

These matches are only a handful of the total conducted. Even with these, very little hard data are available, thanks to the extraordinarily weak oversight and reporting requirements of the OMB guidelines and to the lack of attention to this subject by Congress.

CONCLUSION

Computer matching is an attractive investigative technique. It appears to permit law enforcement officials to instantaneously root out all instances of a particular kind of wrongdoing in a particular segment of the population. It constitutes a general surveillance system that supposedly can detect and deter misconduct wherever it is used. It appeals to the view that "if you haven't done anything wrong, you don't have anything to worry about."

But there are heavy costs associated with computer matching, both in terms of individual rights and in terms of law enforcement expenditure. It is not at all clear that the benefits of the technique outweigh the costs.

The comparison of unrelated record systems is fraught with difficulty. Data on the computer tapes may be inaccurate or inaccurately recorded. It may present an incomplete picture. It is unlikely to be sufficient to "answer" difficult questions, such as whether a person is entitled to receive welfare or is engaged in a conflict of interest.

On the other hand, computer matching erodes individual rights: the Fourth Amendment right to be free from unreasonable search, the right to the presumption of innocence, the right to due process of law, and the right to limit the government's use of personal information to the purposes for which it was collected.

Moreover, the rapid and unchecked growth of computer matching leads inexorably to the creation of a de facto National Data System in which personal data are widely and routinely shared at all levels of government and in the private sector.

RECOMMENDATIONS

As a general framework for safeguarding individual rights, I propose the following:

(1) The Privacy Act should be amended to clarify that computer matches are not ipso facto "routine uses" of personal record systems.

(2) No further federal computer matches should be permitted without express congressional authorization.

(3) Congress should not authorize computer matches of sensitive personal records systems (the confidentiality of which is otherwise protected by statute) such as taxpayer records maintained by the IRS, census records maintained by the Census Bureau, or bank records maintained by federally insured banking institutions.

(4) No computer match should be authorized unless and until an analysis has been made of its projected costs and projected savings in the recoupment of funds owed to the government. The match should not be authorized unless the public benefit will far outweigh the cost—and unless individual rights will be protected. The results and full costs of any match should be published.

(5) Procedural due process protections for the persons whose records are to be matched should be specified by statute, including the right to counsel, the right to a full hearing, and the right to confidentiality of the results of a match.

The thrust of my comments has been to raise some basic questions about computer matching. I recommend a moratorium on all further matching so Congress and the public can study the results of all computer-matching programs conducted to date and assess the long-term consequences.

In closing, I second the view of Justice William O. Douglas, when he said, "I am not ready to agree that America is so possessed with evil that we must level all constitutional barriers to give our civil authorities the tools to catch criminals."

Author's Present Address: John Shattuck, American Civil Liberties Union, 600 Pennsylvania Avenue, S.E., Suite 301, Washington, D.C. 20003.

THE GOVERNMENT NEEDS COMPUTER MATCHING TO ROOT OUT WASTE AND FRAUD

RICHARD P. KUSSEROW

More information will be collected, stored, and retrieved in our lifetime than in all other generations combined. This information explosion, however, is creating new problems for the government manager.

Crucial issues revolve around the use of computer technology to insure that taxpayers' money is being safeguarded and to manage personal data without sacrificing individuals' rights to privacy. Predictions about the dehumanizing effects of technology heat the issues.

Unfortunately, *computer matching*, charged with myth and misconception, has become fuel for this emotional debate. Critics depict mere man against massive computers and evoke the specter of the Orwellian 1984 and "Big Brother."

In reality, computer matching covers many processes used to detect payment errors, increase debt collection, and identify abusive grant or procurement practices. The Department of Education, for instance, uses computer matches to identify federal workers who default on student loans. The National Science Foundation screens research fund applicants against its employee and consultant lists to prevent any conflict of interest in grant awards.

My office in the federal Department of Health and Human Services (HHS) uses matches to unearth doctors who are double-billing Medicare and Medicaid for the same service. Over 230 problem health providers were removed from participation in the Medicare program in the last fiscal year—a 253 percent increase over the previous year. We have also matched the Social Security benefit rolls against Medicare's record of deceased patients and discovered thousands of cases of administrative error and fraud. This project alone resulted in savings of over $25 million.

Without the computer, government could not fulfill many mandated missions. Forty million Social Security checks are issued each month—an impossible feat without automated data processing.

Computers are here to stay and will become even more pervasive. We are witnessing the virtual disappearance of hardcopy, a development of special importance to the government manager, auditor, and investigator. Without a paper trail, government workers must use innovative techniques to meet this new challenge.

Computer matching is an efficient and effective technique for coping with today's expensive, complex, and error-prone government programs. For instance, computer matching and other innovative techniques helped my office identify $1.4 billion in savings—about a 300 percent increase over the previous year.

THE HIGH COST OF ERRORS AND FRAUD

Over $350 billion is paid out every year through government entitlement programs to millions of recipients. Ineligibility and payment errors cost the taxpayers billions of dollars annually. Add to this the dollars lost through loan delinquencies, excessive procurement

costs, and other abuses, and the losses become even more staggering. Perceptions of waste and cheating in government programs erode public support for the programs and respect for government itself.

Government managers cannot simply rely on chance discovery, voluntary compliance, or outdated manual procedures to detect errors. They have a responsibility to use innovative techniques to monitor the expenditures of program dollars, to detect fraud, to determine who is ineligible or being paid incorrectly, etc.

COMPUTER MATCHING: NOT A NEW TECHNIQUE

Computer matching is not a new technique. The basic approach of matching one set of records to another has been used by both public and private sectors for years. Although matching predates the computer, the computer has made it quick and cost effective.

In 1977, Congress, recognizing the effectiveness of computer matching, passed Public Law 95-216. This law mandated that state welfare agencies use state wage information in determining eligibility for Aid to Families with Dependent Children (AFDC). Subsequent legislation also required similar wage matching for the Food Stamp program.

Computer matching can serve many objectives:

- assuring that ineligible applicants are not given costly program benefits;
- reducing or terminating benefits for recipients who are being paid erroneously;
- detecting fraudulent claims and deterring others from defrauding the program;
- collecting overpayments or defaulted loans more effectively;
- monitoring grant and contract award processes;
- improving program policy, procedures, and controls.

Simply defined, computer matching is a technique whereby information within two or more records or files is compared to identify situations that *could* indicate program ineligibility or payment errors.

The process, however, should not and does not stop there. The computer does *not* decide who is getting erroneous payments and does *not* automatically decide who should be terminated from the payment rolls. The computer merely provides a list of items that *could* indicate an erroneous or aberrant situation. The matched items must be investigated by program staff. Only then can an agency determine whether a payment should be adjusted or stopped, or the file record corrected.

Early computer matching efforts, which acted upon "raw hits" without proper follow-up, were justifiably criticized. Today, computer matching is far more effective, efficient, and less intrusive. A manual examiner had to search through *all* records in a file. A computer, however, picks out only those records that match and ignores all the others: it only scans for aberrations. In this sense, computer matching is far less of an invasion than 100 percent manual review.

PRESIDENT'S COUNCIL ON INTEGRITY AND EFFICIENCY

In 1981, President Reagan formed the President's Council on Integrity and Efficiency (PCIE) to coordinate efforts to attack fraud and waste in expensive, government programs. One of its major activities is the Long-Term Computer Matching Project, which I cochair with the Inspector General of the Department of Labor.

Our overall objective is to expand the cost-effective use of computer matching techniques that prevent and detect fraud, abuse, and erroneous payments and, at the same time, to protect the rights and privacy of individuals. The Project does not run computer matches. Rather, through its membership of federal and state program administrators, the Project

- gathers and shares information about federal and state matching activities,
- analyzes and removes technical and administrative obstacles to computer matching, and
- fosters increased federal and state cooperation in computer-matching activities.

So far, the Project has inventoried federal and state matches, established a clearinghouse and a newsletter, and launched an effort with eight states to test standardized data extraction formats for computer matching. The standardized formats will make matching "hits" more reliable, thereby reducing the need for manual review of client files.

One of the Project's first tasks was to revise the Office of Management and Budget's (OMB's) "Guidelines for Conducting Computer Matching Programs." The Guidelines were originally set forth in 1979 to implement the Privacy Act of 1974, in the context of federal computer matching efforts. The 1982 revision streamlined paper-work requirements and reiterated requirements for privacy and security of records.

The Guidelines call for public notice of proposed matches and strict safeguards concerning use, storage, and disclosure of information from matches. In his December 1982 testimony before Senator William S. Cohen's Subcommittee on Oversight of Government Management, David F. Linowes, former chairman of the Privacy Protection Study Commission, stated that the 1982 Guidelines make "sound provisions for protecting the privacy of the individual."

FEARS OF A NATIONAL DATABASE ON INDIVIDUALS UNGROUNDED

A major concern is that computer matching will ultimately result in the creation of a national database of computerized information on every individual. OMB Guidelines insure that such would be impossible. Once a match is completed, Guidelines require that the files be returned to the custodian agency or destroyed.

To be effective, computer matching must be built into the administration of a government program—not just run as an ad hoc investigation. Also, matching should be performed *before* payments are made, as well

as used in an ongoing monitoring effort. In this way, matching stops payment errors before they occur.

Prepayment screens using computer matching techniques not only detect errors, they also deter fraud and abuse in government programs. California, for instance, routinely checks public assistance claims against wage records, saving an estimated $1 million per month in overpayments.

Computer matching is racially, sexually, and ethnically blind. No person or group is targeted.

SOME EXISTING PRIVACY SAFEGUARDS

A number of privacy safeguards have already been institutionalized. "The Computer Matching Reference Paper," published by the PCIE, sets forth "purpose" standards. An agency considering a match must first conduct a study to determine the match's scope and purpose, identify agencies and records involved, and ascertain the information and follow-up actions needed. A key aspect is the assessment of the estimated costs and benefits of a match.

Another safeguard is OMB's "Model Control System." This document suggests that government officials carefully analyze the hits from a computer match to verify the data with the source agency and determine whether the hit is the result of error or abuse. For large matches, officials would have to analyze only a sample of the hits to verify the matching process. After doing this, officials should take corrective measures, proceeding cautiously against any individual where doubt exists.

A third privacy safeguard is provided by a memorandum sent by the deputy director of OMB, Joseph A. Wright, Jr., to the heads of all government agencies on December 29, 1983.

That memorandum provides instructions for preparing a Computer Match Checklist, to be completed by each government agency involved in matching federal data records. This checklist and the Model Control System help agencies to comply with the Privacy Act of 1974 and the OMB Computer Matching Guidelines of May 11, 1982.

Relevant government agencies must complete this checklist immediately following their announced intent (as indicated by publication in the *Federal Register*) to conduct a computer match. This checklist must be on file for review by OMB, Government Accounting Office (GAO), and others interested in insuring that safeguards are being followed to protect personal data.

Still another privacy safeguard, the PCIE reference paper, calls upon government managers to do a cost-benefit analysis both before and after a computer-matching project. In some cases it will make sense to do a pilot match based on a sample. The results of this pilot study would provide a better idea of what could be achieved from a full-scale matching project. In any event, pilot matches are subject to Privacy Act safeguards.

Finally, the OMB Matching Guidelines require government managers to prepare a matching report at least 30 days prior to the start of the match project. It would be published in the *Federal Register* to give relevant parties an opportunity to comment.

CONCLUSION

Any computer match that does not consider privacy, fairness, and due process as among its major goals is not a good project. Well-designed computer matches are cost effective.

The government's need to insure a program's integrity need not be incompatible with the individual's right to privacy and freedom from government intrusion. The point is to *balance* these competing interests. Government managers have a responsibility to insure that program funds are spent as intended by Congress. At the same time, these managers must carry out those responsibilities within the requirements and spirit of the Privacy Act. Such a balance is both possible and essential.

Additional Comments

In addressing the concerns raised by John Shattuck, I must first put federal computer-matching projects into perspective. A common misconception is that computer matching is primarily an investigative tool. In reality, matches are used primarily to assist in government audits to identify inappropriate data (e.g., mistakes or errors) in the records under review. Most of our computer-assisted audits use computer screens rather than tape-to-tape matches, which are usually performed on a one-time basis.

The goals of these matches are twofold: (1) to purify the databases, and (2) to build in routine front-end prevention procedures. ("Front-end matches" match data to an existing database before payments are made.) Shattuck's premise seems to be that computer-matching programs have enlarged the number of individuals subjected to government inquiry. This is not true. The criteria for identifying a "hit" are no different than the criteria for evaluating the need for further information

Early computer matching efforts, which acted upon "raw hits" without proper follow-up, were justifiably criticized. Today, computer matching is far more effective, efficient, and less intrusive.

Our overall objective is to expand the cost-effective use of computer matching techniques that prevent and detect fraud, abuse, and erroneous payments and, at the same time, to protect the rights and privacy of individuals.

received by other means. Computer matches have not created new areas of audit or investigation, but they have allowed agencies to improve their methods.

I fail to see the merit of requiring agencies to limit themselves to less effective audit activities. That argument is based on the unfounded belief that sophisticated proactive audit techniques are per se violative of individual rights.

Shattuck's comments demonstrate a lack of understanding of the procedures followed in federal computer matchings. The individuals whose records are included in a match are not really under investigation. The only records that can result in an inquiry are those that produce a hit. Such indicates a mistake, error, or possible fraud or abuse. In an Aid to Families with Dependent Children (AFDC) state-to-state match, for instance, records indicating a recipient receives AFDC benefits in several jurisdictions would be identified for further review. Since this clearly raises a question of eligibility, an eligibility review can hardly be characterized as a "fishing expedition."

The only real change from computer matches is the increased number of cases identified. Much of the alleged impact on individual rights discussed by Shattuck are issues separate and distinct from computer matching. Once hits are identified for further review, the reviews should be evaluated as any other reviews based on information from any source.

Examples cited by Shattuck of actions taken as a result of matches reflect his disagreement with the evidentiary criteria used by some agencies in pursuing an adverse action. They are in no way an indictment of computer matching for identifying cases for review. The two issues are separate.

The information produced by a matching program is no different from that produced by any other audit or law enforcement inquiry. Once that is recognized, the constitutional concerns raised by Shattuck can be put into perspective. I am unaware of any court decision even remotely indicating that computer-assisted audits of government records run afoul of the fourth amendment protections against unlawful search and seizure.

I also fail to see how a law enforcement inquiry based on a computer-matching hit has any impact on the presumption of innocence in a criminal proceeding. This presumption places the burden on the government to prove guilt in a criminal case. None of the examples cited by Shattuck have any bearing on this principle.

It is equally misleading to imply that computer matching has resulted in any weakening of due process. The right to confront an accuser has never applied to the purely investigative stages of a law enforcement inquiry. Shattuck apparently believes that individuals identified in a computer match should be afforded rights never afforded any investigative subject. Law enforcement inquiries can often be closed without a subject interview. This is equally true for inquiries triggered by a computer match. This in no way violates any legally recognized due process standards.

Criticisms made against computer matching are generally unfounded. I strongly oppose Shattuck's recommendations as being unnecessary and inappropriate. His intent is to greatly restrict, if not totally eliminate, the use of computer-matching projects by the federal government.

Requiring congressional authorization for each match and affording persons whose records are being matched rights far in excess of those available to the actual subjects of a law enforcement inquiry would not improve—but end—the use of matching. This is far too vital an audit technique to lose—especially in view of the fact that Shattuck has failed to provide even a *single* example of a federal computer match that violated an individual's legal rights.

The rights of individuals in federal criminal, civil, or administrative proceeding are already protected by constitutional and other legal constraints. I agree with Shattuck that matches should not be conducted prior to an analysis of their cost effectiveness. In fact, no federal agency has the resources to conduct such matches without careful consideration of costs versus benefits. Further restrictions are, therefore, unnecessary.

Author's Present Address: Richard P. Kusserow, U.S. Dept. of Health and Human Services, 330 Independence Avenue, S.W., Washington, D.C. 20201.

CR Categories and Subject Descriptors: J.1 [**Administrative Data Processing**]: *government*; J.1 [**Administrative Data Processing**]: *law*; K.2 [**History of Computing**]: *people*; K.4.1 [**Computers and Society**]: Public Policy Issues—*privacy*; K.4.2 [**Computers and Society**]: Social Issues—*abuse and crime involving computers*

General Terms: Human Factors, Legal Aspects, Security

Additional Key Words and Phrases: computer-assisted audits, computer matching, fraud and waste in government programs, individual rights, invasion of privacy