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