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.