TESTIMONY

OF

JANLORI GOLDMAN

STAFF ATTORNEY

ON BEHALF OF THE

AMERICAN CIVIL LIBERTIES UNION

ON

S. 496

THE COMPUTER MATCHING AND PRIVACY PROTECTION ACT OF 1987

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT INFORMATION, JUSTICE AND AGRICULTURE

HOUSE GOVERNMENT OPERATIONS COMMITTEE

JUNE 23, 1987

Mr. Chairman and Members of the Committee:

INTRODUCTION

I would like to thank you for the opportunity to appear before you today to testify on S.496, the "Computer Matching and Privacy Protection Act of 1987", which passed the Senate on May 21, 1987. I am a staff attorney on the American Civil Liberties Union's Project on Privacy and Technology, and appear today on behalf of the ACLU. The ACLU is a nationwide, nonpartisan organization with approximately 250,000 members dedicated to preserving citizens' constitutional rights.

Thirteen years ago Congress passed the Privacy Act. Those who worked long and hard to enact the legislation have been continually disappointed and frustrated by the Act's failure to give citizens' greater control over personal information held in federal agency record systems. As Chairman English remarked in his opening statement during the 1983 Privacy Act Oversight hearings:

> One of my chief concerns is that the bureaucracy, with the approval of OMB, has drained much of the substance out of the Act. As a result, the Privacy Act tends to be viewed as strictly a procedural statute. For example, agencies feel free to disclose personal information to anyone as long as the proper notices have been published in the Federal Register. No one seems to consider any more whether the Privacy Act prohibits a particular use of information."

As this Committee pointed out in its 1983 report entitled Who Cares About Privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and By the Congress, much of the failure of the the Privacy Act can be attributed to the

institutionalization of computer matching in government agencies despite the fair information principles originally embodied in the Act.

The perceived failure of the law to protect privacy is not a partisan issue. As stated in the 1980 Republican Party Platform:

> [g]overnment in recent years, particularly at the Federal level, has overwhelmed citizens with demands for personal information and has accumulated vast amounts of such data through the IRS, the Social Security Administration, the Bureau of Census, and other agencies. Under certain limited circumstances, such information can serve legitimate societal interests, but there must be protection against abuse . . . We are alarmed by Washington's growing collection and dissemination of such data. There must be protection against its misuse or disclosure.

If enacted, we believe the "Computer Matching and Privacy Protection Act of 1987" would represent the first step in what we hope will be a larger reform effort to make the Privacy Act work.

At some point in the near future, we look forward to legislative reform which is responsive to the fundamental civil liberties issue presented by matching and verification programs--the development of what the OTA recently termed the creation of a de facto national database containing personal information on most Americans. (See Electronic Record Systems and Individual Privacy, June 1986, hereinafter referred to as "OTA Study"). I will return to this overriding issue after discussing computer matching and the proposed legislation.

THE PRIVACY ACT OF 1974

To understand the need for the "Computer Matching and Privacy Protection Act," it is important to review the intended purpose of the Privacy Act and how it has been undermined by administrative interpretation.

Congress intended the Privacy Act to resolve the mounting tension between protecting personal information and the government's need to collect and use that information by prohibiting agencies from disclosing records containing personal information for purposes other than those for which they were collected without giving notice to and obtaining the prior consent of the individual. However, the Act contains a number of exemptions from this requirement, most notably the "routine use" exemption which authorizes the disclosure of records for a purpose which is compatible with the purpose for which the records were originally collected.

In 1977, the Carter Administration instituted "Project Match," a computer matching scheme to compare Health, Education and Welfare's (HEW) lists of welfare recipients with federal payroll files from the Civil Service Commission and the Defense Department (DOD) in eighteen states. The match sparked a heated debate between those who viewed matching as an important investigative tool and those who believed that matching records violated the Privacy Act and intruded upon individual liberties.

Proponents of computer matching claimed that matching was justified under the Privacy Act's "routine use" exemption. A number of agency officials argued that detecting fraud and abuse

in government programs was a legitimate government purpose, and thus compatible with the original purpose for which records were collected. It should also be noted that there were government officials who believed that Project Match was not a "routine use" of agency records and thus violated the Privacy Act.

At the time, the ACLU criticized computer matching principally as violative of Fourth Amendment principles and the Privacy Act. We still believe this is the case.

First, we have claimed that the computerized scanning through thousands of personal record systems with no individualized suspicion of wrongdoing violates the Fourth Amendment. Unfortunatley, this consitutuional claim is not likely to prevail under current judicial precedents, particularly in light of the Supreme Court's refusal in U.S. v. Miller, (425 U.S. 435, 1976) to recognize a protectable privacy interest in personal information held by third parties.

Second, we argued that computer matching violates the basic principle that a citizen is innocent until proven guilty when benefits are denied on the basis of a mere "hit" without further investigation by the matching agency. Since the well-known 1982 bank match in Massachusetts in which the benefits of welfare recipients were wrongfully terminated on the basis of "hits" generated by comparing welfare records with state bank records, Congress has included in programs such as DEFRA the requirements that agencies independently verify "raw hits" before suspending or terminating benefits to avoid such unjustifiable results.

Third, we argued that computer matching of records collected for different purposes and disseminated without actual notice and

individual consent violates the due process and informational privacy rights incorporated in the Privacy Act of 1974.

The legislative history of the Privacy Act is clear on this final point. Congress did not intend the "routine use" exemption to shield most matching programs from the Act's scope. The legislative history of the Privacy Act reveals the intended application of the "routine use" exemption:

> This Act is not intended to impose undue burdens on the transfer of information to the Treasury Department to complete payroll checks, the receipt of information by the Social Security Administration to complete quarterly posting of accounts, or other such housekeeping measures and necessarily frequent interagency or inter-agency transfers of information. It is, however, intended to discourage the unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material." (Legis. History of Privacy Act, Source Book PP. 859-60, emphasis added)

Despite these criticisms, the computer matching proponents prevailed, touching off the beginning of widespread computer matching programs within the federal government. The Constitutional arguments were damaged by the Miller case and the difficult standards of proof in the Privacy Act precluded any meaningful litigation on the Act's meaning and application. Moreover, Congress has overridden the Privacy Act by subsequently authorizing computer matching and front-end verification in a number of government programs. In the Deficit Reduction Act of 1984, matches covering all need-based programs were essentially reauthorized, including new authority to match against heretofore confidential unearned income records of the IRS. Legislation to

establish matching and verification procedures for other grant programs (the Payment Integrity Act) may be introduced by the Administration in the near future.

Administrative limits or controls on computer matching have been watered down or hardly exist. Even the Carter Administration's requirement that computer matching must be cost-justified has been eliminated. Oversight of matching proposals or matching program results is nonexistent according to the OTA Privacy Study and the 1983 Report by this Subcommittee.

In this legal vacuum, the use of computer matching by government agencies to detect fraud and abuse in benefit programs and for law enforcement purposes has grown enormously. In its recent study, OTA reported that in 1984 eleven cabinet-level departments and four independent agencies conducted 110 separate matching programs, totaling nearly 700 matches. Over 2 billion separate records were used in the reported matching programs, and due to multiple matches of the same records, over seven billion records were matched. Since 1980, the number of computer matches has tripled.

The full scope of the government's matching activities is difficult to access. In a study published in August, 1986, the Government Accounting Office (GAO) found that agencies which conducted matching programs did not have complete, accurate data on the extent of their programs.

The government's enthusiasm for matching turns on the belief of government officials that it is an effective tool for detecting fraud and abuse in government programs although, as GAO has reported, the government does little if any systematic cost-

benefit analysis of matching programs. In sum, the concern for individual privacy and autonomy which existed thirteen years ago has given way to the Administration's single-minded quest to reduce the deficit, at any cost. Whatever technological hurdles existed when matching programs were initiated, sophisticated computer hardware and software have overcome them. Now, more complex matches may be performed at lower cost.

THE COMPUTER MATCHING AND PRIVACY PROTECTION ACT OF 1987

The ACLU recognizes that the "Computer Matching and Privacy Protection Act of 1987" represents the first step ever taken by Congress to regulate computer matching and bring it under the wing of the Privacy Act. Even though its reforms are modest, if enacted the legislation would:

--provide private citizens with actual notice that information supplied to the government will be matched or verified against other government data files;

--require matching agencies to independently verify "raw computer hits" before suspending or terminating benefits;

--give citizens due process hearing rights to challenge computer matching results before benefits are suspended or terminated;

--strenghten congressional and public oversight by requiring agencies to enter into a matching agreement which map out with specificity the purpose and plan for the match; and

--enhance internal administrative oversight by establishing Data Integrity Boards in each agency to review matching

agreements and oversee matching programs.

In an improvement over the legislation as originally introduced, the Senate-passed measure covers all federal employee matches as well as matching programs involving federal matches with state or private record systems.

Thus, while it does not impose any substantive limits on matching programs, the Act would set in place regulations and procedures for agencies to follow which enhance privacy and due process rights of citizens who are the subject of matching and verification programs. The ACLU supports this measure. We make the following recommendations to further strengthen and clarify certain sections of the bill:

MATCHING AGREEMENTS

Under this legislation, oversight of matching programs would be improved by requiring agencies to enter into matching agreements to articulate their reasons, both legal and programmatic, for establishing a matching or verification program and to set forth how they plan to protect due process and privacy rights. The Act would require agencies to provide a detailed account of a proposed match, including the number of data elements and records involved, notice and destruction procedures, and other security safeguards.

Oversight would be further improved if the legislation also required that the matching agreements be published in the Federal Register before they are approved. This would permit greater congressional and public oversight by supplying information sufficient to judge the intrusiveness of particular matches and

what steps are being implemented to protect privacy, data security, and due process.

JUSTIFICATION

The proposed matching agreement section does require agencies to justify the need for matching programs. We believe that the justification provision should be clarified to include an anticipated cost-benefit analysis if it is a new program and documentation of past results (e.g. fraud detected) if it is a recurring program. The matching agency should perform a cost/benefit analysis prior to conducting a match, projecting qualitative as well as quantitative costs and benefits. In this way, the Data Integrity Boards of each agency and the Congress may compare the initial projections with the post-match analysis. This process will provide a basis for determining whether a match is "justified" and cost-effective.

Under the Carter Administration, agencies were required by OMB to cost-justify computer matches, a requirement withdrawn by OMB under the present Administration. In view of GAO's report indicating that cost-benefit analyses are feasible, Congress should restore this requirement as part of the "justification" provision and as a benchmark for evaluating matches after they are conducted.

Additionally, this Section of the legislation should specify that heightened scrutiny of cost-benefit should be applied in recurring matches since data will be available to evaluate with more precision projected costs and benefits of continuing matches.

NOTICE AND CONSENT

One of the major reforms in the Act is its notice provisions requiring actual and periodic notice to individuals that their records held by government agencies may be subject to matching and verification. Today, notice is satisfied by publication in the Federal Register which most citizens don't read. Congress should make clear that notice under the proposed Act will be printed boldly on the application form and spelled out in plain language. Congress should clarify that the requirement cannot be met by a boilerplate statement that information may be verified against other data but should list other data files which may be checked (e.g. IRS unearned income, SSI unemployment conpensation, state wage data, bank records).

Today, even when notice does appear on an application form, it is often unintelligible. For example, here is a recent notice on a Veterans Administration form:

> The information submitted may be disclosed outside the Veterans Administration (VA) only as permitted by law, including the routine uses identified in VA system of records 58VA 21/22/28, Compensation, Pension, Education and Rehabilitation Records--VA published in the Federal Register."

In addition, some agencies disclose that collateral sources will be contacted. Others do not. Uniform disclosure by all agencies should be a part of the notice requirement.

Also, we would require actual consent to any exchange of information. Consent can be achieved by providing a space for an applicant's signature at the end of the notice provision. Actual notice, coupled with consent to record exchange or verification, makes due process a meaningful reality

when a citizen applies for and accepts a government benefit.

Although these due process requirements may temporarily burden matching agencies, they should be supported by Congress and the Administration. Explicit notice that information will be verified will deter citizens from supplying inaccurate or false information knowing that it will be detected, and is thus consistent with the government's goal of reducing fraud and abuse in government benefit programs. Moreover, notice and consent will remove the element of surprise which a citizen often experiences upon learning that personal information which they have voluntarily given to one agency has been disseminated to another agency without their knowledge.

The notice requirements can be further improved. Notice should advise citizens that the Privacy Act provides them the right to correct information and that benefits may not be denied or terminated unless independently verified and subject to a citizen's right to a hearing. Citizens are rarely informed by government agencies of their right to see and correct records. Also, the legislative history of the Act should suggest that agencies consider the possibility of developing means by which citizens can see and correct their records by computerized means.

VERIFICATION

The ACLU recognizes that the Act's verification procedures are intended to avoid another Massachusetts bank match case in which hundreds of people were wrongfully thrown off the welfare rolls on the basis of unverified "raw hits." While we support

this measure, Congress must be clear that the Act requires human verification of all data which may adversely affect benefit rights.

We note that in issuing regulations for DEFRA, some affected agencies read the verification requirements only to mean that they had to verify IRS unearned income data. To avoid similar confusion, Congress should clarify that all information upon which adverse action could be taken should be independently verified, not just "wage, asset and income information."

Independent human verification of computer matches is essential to protect due process and the presumption of innocence. No benefit should be suspended or terminated without such verification. However, the Act should contain a clear definition of "independent verification." Verification procedures must not be overly intrusive. The statutory language authorizing verification from "third party sources" is subject to broad interpretation (e.g. employee or neighbor interviews) and should be limited to collateral sources.

The need for thorough verification is clear. Many of the agencies' computer databases are replete with incomplete, false, and inaccurate data. For example, under DEFRA, benefit applications are to be checked against IRS unearned income records. In recent testimony before the House, John Finch of the General Accounting Office revealed that faulty software used by a number of banks to report unearned income to the IRS led to inaccurate IRS reporting "affecting approximately one million taxpayers." According to some state officials we have talked

with, significant error rates can also occur in other wage and income data.

Also, we suggest that matching agreements include reasonable time limits for verifying information. Long delays may adversely affect citizens if they must wait for verification to receive benefits. If verification time limits are exceeded through no fault of an applicant, he or she should be presumed qualified and receive benefits pending a final determination.

These requirements, together with actual notice and consent, constitute the core due process protections afforded by the proposed legislation and institutionalize due process as a matter of fundamental fairness.

DATA INTEGRITY BOARDS

According to the OTA Study, numerous hearings, and the 1983 Report by this Subcommittee Who Cares About Privacy?, oversight of matching and verification programs is almost non-existent. The 1983 Committee report concluded that "OMB does not actively supervise, review, or monitor agency compliance with Privacy Act guidelines."

The statutory creation of Data Integrity Boards in every matching agency is a step towards rectifying this problem by requiring in-house systematic oversight over matching programs. Without agency oversight, this Act may never be enforced in an effective way. The failure of the 1974 Privacy Act is due in large measure to the fact that provisions which would have established an overall privacy oversight board were eliminated before final passage.

We would like to see the Boards given stronger, clearer oversight authority, particularly at the "front-end" of the process. For instance, the term "approve" should be interpreted to give the Boards power to also "disapprove" proposed matching programs. Also, in performing the cost/benefit analysis after a match, the Board should consider any disparity between "raw hits" and the final verification of information. This will enable the Board to evaluate the accuracy and completeness of the agency's record systems and whether the matches are cost-effective.

The Boards should be expanded to include the Privacy Officers which have been established by the Administration in each agency. This would ensure that the Boards would not only be concerned with efficiency, but also privacy and security by including a person or persons responsible to evaluate matching agreements and programs from a citizen privacy perspective.

Overall, the Boards should be vested with the authority to monitor compliance of the matching agreements and be required to report any unauthorized use of information to OMB and Congress. These reports should ultimately be made available to the public.

SANCTIONS

There are no real sanctions in this legislation. If Congress wants to be serious about enforcing this bill, Congress must revisit and reform the civil remedies section of the Privacy Act. As the proposed legislation provides, agencies may not disclose records if there is "reason to believe" that the matching agreement and other requirements are not being followed. A

similar sanction governs the FBI's National Crime Information Center which bars federal exchange of records with police agencies who fail to maintain accurate and complete records. It is never used because of overriding law enforcement interests in continuing to exchange records. We doubt whether it will prove to be an effective sanction in the context of matching and verification programs for similar reasons.

We recommend the inclusion of a statutory tort remedy that would allow citizens to recover statutory damages if records are exchanged or disclosed in willful disregard of requirements set forth in matching agreements or in violation of the disclosure provision. Statutory damages are necessary when intangible harms such as invasion of privacy occur. Such a remedy is already incorporated in federal wiretap statutes and would put "teeth" in this legislation.

A DE FACTO NATIONAL DATA BASE ON CITIZENS

Earlier, I indicated that the ACLU supports the "Computer Matching and Privacy Protection Act" because it would enhance privacy and due process protections in computer matching and front-end verification programs. However, the Act does not address the more fundamental civil liberties problem of the creation of a "de facto national data file" on each citizen. This legislation will not ban but only regulate computer matching and front-end verification programs. It would give citizens basic due process and privacy safeguards while authorizing the continued expansion of computer matching and verification programs.

The current government trend is to increase front-end verification of applicant information for all government benefit programs. Front-end verification reduces benefit payment "errors" by detecting non-eligibility before rather than after a citizen receives benefits. Although some argue that it also constitutes a lesser intrusion on citizen privacy because the procedure involves a search through a particular citizen's file rather than a "general search" through all files, the ACLU believes that the unchecked growth of verification systems linking various data bases of personal information on every citizen poses a serious danger to individual autonomy and privacy.

The goal of front-end verification is to achieve quick and accurate benefit determinations. While such determinations may save taxpayers money and serve a citizen's interest in obtaining benefits as soon as possible, they require systems which permit rapid access to more complete and accurate information.

In establishing the Income Eligibility Verification System (IEVS) in the Deficit Reduction Act of 1984, Congress authorized the use of social security numbers for all need-based programs to make accurate identification of applicants and to permit computer retrieval of data on applicants from various agencies' program databases containing information on applicants and from databases containing wage, pension, unemployment insurance, and other income data, including unearned income from IRS files.

Congress also called for the development of standard formats for databases for a number of programs to facilitate

rapid exchange of information. DEFRA regulations make a critical leap from "encouragement" to requiring that agencies administering IEVS-covered programs adhere to standardized formats and procedures in using information which will enable the states to create files specifically for matching and verification programs. Although the regulations state that it is a "logical process and not a physical or automated system" which is intended, the regulations do require a number of agencies to automate their systems. The newly-created State Wage Information Collection Agencies (SWICA) must maintain their data in "machine readable" form, as must state agencies which administer AFDC.

DEFRA regulations state that agencies should only create an "automated front-end eligibility system" if it is cost-effective for them to do so. They note that "SSA and IRS have not yet found it cost-effective to make wage and self-employment and unearned income information accessible on-line for their own agency purposes. Therefore, it would not be feasible to allow States on-line access to these files." I submit to you that it is only a matter of time before SSA and IRS will find it cost-effective to provide on-line access to their files. In the end, the result will be the "de facto national database" foreseen by the OTA.

In the 1960's, the Johnson Administration proposed the creation of a central databank on every citizen containing social security, income, census, and other sensitive personal information to serve the needs of the welfare state. The idea of such a central data file on every citizen was overwhelmingly condemned as "Big Brother" government and a threat to privacy and citizen autonomy. The plan was abandoned.

IEVS and proposed legislation to extend IEVS to other government programs makes a national databank on most citizens a reality. Now, however, the information does not have to be stored in one mainframe at a central agency. With the social security number as a uniform identifier, common formats, and on-line access, enormous amounts of data may be assembled instantly on any citizen by computer from "decentralized" files. A decentralized system may look less ominous than a centralized file, but the effect is the same.

The "Computer Matching and Privacy Protection Act" recognizes this problem by providing for the destruction of records used in a match but it should also begin to address the data linkage issue by:

1) prohibiting the creation of third files on individuals from matching or verification programs;

2) stating that nothing in this Act is intended to authorize or establish a national data base; and

3) clarifying that the Act recognizes ongoing matches but requires Congressional authorization for all future matches. Such requirements would help to focus Congressional attention on the privacy issues involved in data linkage and hopefully move it in the direction of weighing privacy as an interest as important as government efficiency and effective law enforcement.

Furthermore, we believe there should be substantive limits placed on what files or data may be linked together. Along with the American Bar Association, we recommend an express prohibition on use of 1040 information, political affiliation, race, and

other sensitive information in matching and verification programs. Otherwise, data linkages will expand to files of greater sensitivity and involve more information collected pursuant to compulsory process.

For example, the IEVS system will grow. Eventually the system will feature on-line access by federal and state agencies. In the future, it is not hard to imagine that INS will want access to IEVS to detect illegal aliens. IRS will want to verify income tax returns through IEVS and pressure will mount to add more IRS data to the system for verification purposes. The FBI will want access to IEVS for law enforcement and intelligence purposes. In fact, the FBI's Advisory Committee recently proposed expanding its NCIC system to provide 64,000 criminal justice agencies with on-line access to SSI, IRS and INS records.

This government use of technology for fraud detection and law enforcement has serious social and civil liberties costs--increasing power in the hands of large government bureaucracies, diminishing sense or "expectation" of privacy, and pressure on citizens to conform.

While we urge passage of the "Computer Matching and Privacy Protection Act of 1987", we must all begin to address this more fundamental long term trend towards a de facto (if not de jure) national data base on every citizen. We must find ways to limit and control this threat to privacy.

pc# 2
496test