Information
and Privacy
Commissioner/
Ontario

Privacy and Computer Matching
report for
the Standing Committee
on the Legislative Assembly

Tom Wright
Commissioner
January 1991

Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

This publication is also available on the IPC website.

Executive Summary

Computer matching is perceived by privacy advocates to be a potential threat to civil liberties and privacy. However, all Western European countries, the United States and the Canadian federal government use matching as an audit and investigative tool. While no study exists documenting the use of computer matching within Ontario, it may be reasonable to assume from the experience of other jurisdictions that computer matching is currently being practised within the Ontario government.

Computer matching, at its most basic, involves the computerized comparison of automated systems of records or databases. The process may be conducted within an institution or it may involve the matching of data obtained from more than one institution or external source.

As computer matching can detect persons or organizations that may be intentionally defrauding the government, it is used extensively for law enforcement purposes to identify suspects for investigation. Computer matching is also used for the purpose of front-end verification (i.e., verification of information before benefits or services are given). Another practice closely related to computer matching is that of computer profiling. This technique is used primarily for law enforcement purposes to locate potential violators when there is a general idea about the characteristics of offending behaviour, but no precise information. Profiling involves the correlation of information to determine how closely persons or events fit previously determined violation patterns.

Supporters of computer matching believe that all parties involved benefit from such activity. Benefits are considered to be both quantitative (e.g., monetary savings) and qualitative (e.g., improved law enforcement). The main benefits of computer matching, as argued by its supporters, are increased detection and deterrence of fraud, waste and abuse, and improved efficiency and effectiveness of government programs. Computer matching is also considered less intrusive than manual audit techniques and is reported to be very cost-effective (i.e., the savings resulting from the match outweigh the costs of the program). In addition, the use of this technique is thought to increase the public's confidence in government.

Critics of computer matching argue that the benefits are overstated and unsubstantiated as the lack of government oversight has meant a paucity of reliable information on computer matching. They also are critical of the exclusive use of information generated from computer matches to make decisions affecting the data subjects, and of the use of inaccurate information in matches.

The central issue in the debate about computer matching is whether there are adequate safeguards associated with the new technology to prevent violations of personal privacy. The main privacy implications resulting from this practice, as reported by various privacy advocates, are that the use of computer matching results in:

- the data subjects loss of control over their personal information,
- unlawful search and seizure,
- the presumption of innocence being turned into the presumption of guilt,
- lack of proper due process, and
- unequal protection of the law.

The general rule in regards to the regulation of computer matching in various jurisdictions surveyed, is that matching proposals must be submitted, in writing, to a data protection agency for review. Some of these agencies then have the authority to quash the proposals while others merely are permitted to make recommendations. These jurisdictions include most of the European nations, Australia, the United States, the Canadian federal government and the province of Quebec. All these jurisdictions have already performed studies on the subject or are in the process of commissioning studies on the subject.

There is a pressing need to determine the extent of computer matching within Ontario and bring a degree of public accountability to bear on this issue. The acceptability of computer matching depends, in part, on establishing a proper balance between the legitimate information needs of government and individuals' rights to privacy. It is evident that computer matching is an important and beneficial tool for government, however, it is also evident that the privacy concerns associated with matching are grave enough to merit some form of regulation.

The statutory authority of the Information and Privacy Commissioner/Ontario to review matching programs is limited. As a result, the Office of the Information and Privacy Commissioner is not able to regulate or monitor the majority of computer matches within the provincial government. The Commissioner is even unable to determine the existence of current or proposed matching programs. Due to the limitations of the *Freedom of Information and Protection of Privacy Act, 1987*, it is inappropriate to attempt to regulate computer matching within the existing statutory provisions.

Recommendation

To properly examine computer matching within the Ontario government, it is recommended that a Task Force be created to examine this issue and its associated privacy concerns, and to recommend an appropriate mechanism to control and monitor computer matching within the Ontario government.

The Task Force could perform a complete survey of computer matching and address the concerns on both sides of the matching issue. Additionally, the Task Force would be in a position to determine the extent of this practice in Ontario, and to consider if all types of computer matches within the Ontario government need to be regulated. This type of review would provide for public participation and would assist in continuing the concept of open government that is embodied in the *Act*.

It is suggested that the Task Force have a time limit of six months to complete its study. It is also recommended that the Task Force be composed of representatives from government institutions which may be involved with, or have concerns regarding the management of computer matching in Ontario. Privacy advocates and technology experts from the private sector could also be included on the Task Force.

Table of Contents

1. Introduction

Within Ontario, the *Freedom of Information and Protect of Privacy Act, 1987*, as amended, (the *Act*) provides individuals with the right to protection of privacy of their personal information.[1] This right embodies the basic principle of informational privacy (i.e., an individual's right to control the personal information held by others about him/herself).

Expanded use of computer and telecommunication technology, however, has made it increasingly difficult for individuals to exercise some measure of control over their personal information held by government. Computers have made it possible to collect, use, manipulate, exchange, disclose and erase information with astonishing ease and speed. Recent years have seen the development of increasingly sophisticated computer hardware and software. These technical advances have created the ability to electronically link separate and remote databases so that the information contained in each is available to users instantaneously.[2]

Concerns about the protection of privacy, particularly in the context of this new age of computers, have been raised throughout the western world at all levels of society — the general public, privacy advocates, law-makers, government officials and decision-makers.

Justice Gerard Vincent La Forest, in a recent decision of the Supreme Court of Canada, stated:

> … society has come to realize that privacy is at the heart of liberty in a modern state … Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection … The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state. … [Also] there is a privacy in relation to information. This too is based on the notion of the dignity and integrity of the individual.[3]

In the United States, President George Bush, in his greeting to the "Privacy in the 1990s" Conference, noted:

> As new technology has brought us the information age, it has underscored the fact that knowledge is often synonymous with power. Information itself has become a commodity — bought and sold in the marketplace and available at our fingertips through computer systems.
>
> The information age has made personal information about each of us far more accessible. … The ease with which information can be collected and disseminated has raised legitimate concerns about the best ways to protect the confidentiality of certain information.[4]

One of the practices which has been made possible through the advances in computer and telecommunication technology is computer matching. Many perceive computer matching as a potential threat to everyone's civil liberties and privacy, while others believe it to be a useful audit and investigative tool. Therefore, a potential conflict exists between the demand for efficient management of government programs, including effective law enforcement, and the privacy rights of individuals.

In its 1986 study of electronic record systems, the United States Office of Technology Assessment noted that all Western European countries and Canada are using computer matching, to an increasing degree, as a technique for detecting fraud, waste and abuse.[5]

At present, computer matching is widely practised in the Canadian Federal government. The matches are prevalent in agencies involved with broad social benefit programs, law enforcement, and investigations or intelligence work. The Privacy Commissioner of Canada has begun reviewing these matching programs under a policy established in Treasury Board of Canada guidelines.[6] In the United States, the use of computer matching by federal and state agencies is generally held to have developed in the late 1970s, and its use has steadily expanded since that time.[7]

The Information and Privacy Commissioner is not aware of any study documenting the use of computer matching within Ontario and, as a result, a history of matching by the government of Ontario cannot be presented here. However, it may be reasonable to assume from the experience of other jurisdictions that computer matching is currently being practised within the Ontario government.

The purpose of this paper is to explain the process of computer matching, to examine the benefits and problems associated with it, and to discuss the privacy implications of this practice. In addition, the manner in which other jurisdictions have dealt with matching is presented. Finally, as there is no specific provision in the *Act* which addresses the issue of computer matching, a recommendation is presented on how the government of Ontario should address the issue.

2. What is Computer Matching?

Computer matching, also referred to as data matching, record linkage, computer cross-checking, data searching, joint running, cross matching, and a variety of other terms, has been defined in all manner of ways by different jurisdictions. However, at its most basic, computer matching generally involves the computerized comparison of two or more automated systems of records or files. To achieve this comparison, the computer is instructed to search the database(s) and locate specific information or data elements (e.g., name, address, occupation, etc.). The computer then examines this data according to pre-determined selection criteria (i.e., is the information within the data element identical, similar or contradictory). The information which meets the criteria and is selected by the match is referred to as a "hit". If the information is unverified, it is known as a "raw hit."

Matching is generally done by linking a single specific identifier (e.g., social insurance number) or a combination of several identifiers or unique data elements (e.g., sex, marital status, birth date, etc.).[8] Databases may be compared either by running the physical computer tapes together or by the direct electronic linkage of computers (e.g., via a modem). In the United States, the matching of tapes was the procedure most commonly used in the late 1980s. However, as systems become more compatible and costs drop, direct electronic linkage between systems is likely to increase.[9]

The nature of computer matching is very much case-specific. It may be either a one-time occurrence or a recurring process. The technique permits matching within a single file or database or, as noted, between two or more databases.[10] The process may be conducted within an institution or it may involve the matching of data obtained from more than one institution or external source.[11]

Matching is not a new concept. The use of a computer to match data is "a modern version of an old analytical technique."[12] However, computerization has made matching feasible on a more routine basis and on an extremely large scale. For example, in Canada, the Comptroller General has used computer matching, as authorized by the Federal Privacy Commissioner, to perform a research project involving the collection of defaulted student loans by deducting outstanding amounts from tax rebates.[13]

In the United States, the Office of Personnel Management recently began an 18 month project designed to ensure that civilian retirees who are rehired by the Defense Department receive the correct salary and benefit level. This project involves the matching of 1.5 million civilian retiree files with approximately one million files at the Defense Department.[14]

3. Discussion

Computer matching has been the subject of a heated debate since the 1970s. During this time there have been a number of significant developments which have fuelled the arguments on both sides.

One of these developments is that during the last decade, the amount of information which government holds on individual citizens has increased dramatically. In 1982, the Canadian federal government held, on average, 10 to 12 files on each Canadian. By 1989, that number was closer to 20.[15] Increased collection of personal information, responding to expanded government services and computer storage capacity, coincided, not surprisingly, with increased public awareness about privacy and concern about the applications of computer technology. This concern was succinctly expressed to a United States Senate Sub-Committee as follows:

> The computer, with its insatiable appetite for information, its image of infallibility, its inability to forget anything that has been put into it, may become the heart of a surveillance system that will turn society into a transparent world in which our home, our finances, our associations, our mental and physical condition are laid bare to the most casual observer.[16]

Recent surveys of the general public have echoed this sentiment. In 1984, the year of George Orwell's 'Big Brother', The Canadian Institute of Public Opinion determined that the majority of Canadians (68%) believed the government had invaded their privacy. This percentage was higher than the four other countries surveyed (Britain, Brazil, West Germany and Switzerland).[17] By 1987, the majority of Canadians (77%) believed that "as long as information is stored on computers, we can never be sure of our guarantee to privacy."[18] The results of a telephone survey conducted for the Office of the Information and Privacy Commissioner, in January 1988, showed a continued rise in the level of concern over privacy. At that time, the vast majority of Ontario residents surveyed (94%) thought that it was important to protect individual privacy.[19]

3.1 Purposes of Computer Matching

Traditionally, computer matching, regardless of the jurisdiction, has been used for both auditing and investigative purposes. As an audit tool, it is generally used to assess particular aspects of a program or to identify areas for audits. Computer matching is also viewed as a way for administrators to compensate for weak program controls by catching errors that have already been made. Follow-up matches may serve the additional objective of assessing the effectiveness of changes implemented as a result of an earlier match.[20]

However, as computer matching can detect persons or organizations who may be intentionally defrauding the government, it is also used extensively for law enforcement purposes to identify suspects for investigation. Such investigations are carried out by using matching to identify individuals who should not appear in two systems of records but do (e.g., government employees above a certain salary level and persons receiving welfare benefits). It is also used to locate individuals who should appear in two systems of records but do not (e.g., in the United States, males registered for the draft and males over the age of 18 with driver's licences).[21]

The objectives of computer matching have been very diverse in nature. This serves to illustrate the potential reach of this technique.[22] Examples of some of the purposes to which matching has been employed are:

- detection of fraud (e.g, fraudulent or multiple claims, unreported income or assets, impersonation, omissions, unauthorized use, improper conduct by beneficiaries, etc.)[23] and deter others from defrauding the program,
- reduction of duplication of benefits or billing,
- verification of continuing eligibility for a benefit program, or compliance with the requirements of a program,
- recouping incorrect payments or delinquent debts,
- monitoring grant and contract award processes,
- identification of corruption (e.g., improper conduct by employees, conflict of interest, misuse of position, questionable contracts, etc.),
- identification of program mismanagement (e.g., unusual payments, excessive withdrawals, multiple invoicing),
- monitoring of information (e.g., audits, verification, cost comparisons, etc.),[24]
- improvement of program policy, procedures, and controls,
- identification of those eligible for a benefit but not currently claiming,
- construction of comprehensive databases intended for research purposes.[25]

Matches may be undertaken to address only one objective, but in practice the results of a computer match may support several purposes to varying degrees,[26] including subsequent purposes not intended by the original match.

Front-end Verification

Computer matching is also used for the purpose of front-end verification (i.e., verification of information before benefits or services are given). In the past such verification was done manually on a random basis or when the accuracy of the information supplied was suspect. What computer technology has permitted is routine verification.[27]

Essentially, computer-assisted front-end verification differs from traditional or "back-end" computer matching in four ways:

- information is verified on an individual basis rather than for a category or class of people,
- information is verified before an individual receives government benefits or employment,
- its purpose is to prevent and deter rather than detect and punish,
- it is done most effectively at the time of the initial transaction.[28]

The accuracy of the information supplied is checked by comparing it against information held in various computerized databases, generally belonging to other institutions or third parties. These databases may also be searched to determine if there is any additional relevant information which the individual to whom the information relates (also known as data subject) omitted to provide.

Computer Profiling

Another practice closely related to computer matching is that of computer profiling. This technique is used primarily for law enforcement purposes to locate potential violators and violations when there is a general idea about the characteristics of offending behaviour, but no precise information on the violators.[29]

Profiling involves the searching for a specific combination of data elements (i.e., the profile). Statistical selection methods and inductive logic are used to determine indicators of characteristics and/or behaviour patterns related to the occurrence of a certain activity (e.g., persons most likely to under-report taxable income, persons most likely to engage in illegal drug activity, etc.).[30] In other words, profiling involves the correlation of information to determine how closely persons or events fit previously determined violation prototypes.[31]

Computer systems which identify records by a unique identifying number (e.g., social insurance number) permit profiles to be built across several databases. This enables inter-institutional profiling to take place, thereby allowing a composite picture of an individual to be constructed by the aggregation of several institutions' records.[32]

3.2 Benefits of Computer Matching

Regardless of the application, the key to any type of computer matching is that it permits the matching of independent pieces of information in order to draw conclusions which would not have been possible without the link being made.[33] By the joining of what had previously been considered "un-joinable,"[34] investigations which had previously been impossible or impractical may now be undertaken.

Supporters of computer matching argue that computer matching is "an efficient and effective technique for coping with today's expensive, complex, and error-prone government programs."[35] They believe that all parties involved benefit from such activity: the government institutions, the judicial system, the clients of government programs, and the general public. Benefits are considered to be both quantitative (e.g., monetary savings) and qualitative (e.g., improved law enforcement). The main benefits of computer matching, as argued by its supporters, are discussed below.

Detection of Fraud, Waste and Abuse

Perhaps the most frequently touted benefit is that computer matching is an effective method of identifying unlawful conduct within government programs. The detection of such activity results in significant savings as matching leads to:

- identification and cessation of incorrect payments,
- recovering of overpayments and debts, restitution of underpayment of tax,
- avoidance of future erroneous payments or overpayments, and underpayment of taxes,
- improved law enforcement activity.

An example of savings resulting from computer matching was reported by the American Internal Revenue Service. It indicated that auditing techniques, including computer matching, brought in $22 billion in outstanding debts.[36]

Deterrence of Fraud, Waste and Abuse

It is believed that if all participants in a government program are aware that computer matching is conducted on a regular basis for the purpose of detecting fraud, and those found to be defrauding the institution prosecuted, the incidents of fraud will decrease.[37]

Improved Efficiency and Effectiveness of Program

By using computer matching to identify those who are improperly receiving benefits and then eliminating them from the program, it is felt that the efficiency of the program will be increased as the institution will be able to concentrate its resources on eligible beneficiaries. This results in improved service delivery and eligibility determination, and correction of program deficiencies.[38]

It is also argued that computer matching enhances the administration of a program as it boosts staff morale, and increases the quantity of the information available for decision-making. In addition, supporters believe computer matching to be useful for identifying action needed to be taken to strengthen program controls or procedures.[39] Further, the quality and reliability of the information in a database may be improved by the correction of errors or outdated data.[40]

Greater Public Confidence and Support

Public perceptions of waste and abuse are seen to erode public support for the government and, therefore, institutions conducting computer matching are thought to benefit from increased program support by the public. By taking proactive steps to detect and deter fraud and other abuses in publicly funded programs, the credibility of the government is perceived to be enhanced.

Less Intrusive than Manual Auditing Techniques

The use of computer matching allows institutions to be more efficient by improving their audit methods.[41] A manual examination would involve the search of all records in a file. A computer, however, is able to pick out only those records that meet the selection criteria and ignore all the others. As a result, the use of computer matching to verify information is purported to be less intrusive than manual reviews.[42]

Client Benefits

It is argued that computer matching results in improved client relations because underpayments are identified, service delivery is improved, and there is a reduction of the stigma of participating in the program.[43] The latter point is felt to result from the fact that if the use of computer matching is widely known, a welfare recipient, for example, will be perceived by the public as someone who legitimately needs the benefit and not someone who is attempting to defraud the government. Another benefit is that matching reduces the need to repeatedly collect information from program clients.

Public Benefits

Supporters also think that computer matching assists in the attainment of more abstract objectives such as the achievement of greater social equity in the distribution of government benefits, and of the tax burden.[44] Another less tangible benefit for the public is the improvement in the operation and administration of government programs and law enforcement activities. Some think that government has a responsibility to employ whatever techniques are available to manage its resources correctly[45] and that computer matching is just one means of fulfilling that obligation to the public.

Cost-Effectiveness

Computer matching is presented as a cost-effective practice as the savings resulting from the match are reported to outweigh the costs of the program. The professed cost-benefit from matching is one of the reasons it is seen to have broad public support in the United States.

Many argue that computer-assisted front-end verification achieves the same benefits as "back-end" computer matching but is much less expensive to operate. The costs of traditional computer matching (e.g., verifying large numbers of hits, holding follow-up hearings, and prosecuting wrongdoers) are not incurred with front-end verification.[46] In addition, such a process avoids unnecessary or erroneous payments.

Technological Improvements

Computer matching results in an increase in the amount of information available to institutions, which is considered a benefit as it fosters "the continuing development of improved computer technology to process that information."[47]

It is also argued that the use of computers for storing and processing personal information offers greater opportunities for the protection of that information than paper-based systems. Such techniques as passwords, encryption and audit trails are used to protect the confidentiality and security of information in an electronic environment.[48]

3.3 Problems with Computer Matching

Critics of computer matching argue that these benefits are overstated and unsubstantiated. Leaving aside the privacy implications of computer matching (to be discussed later in this paper), they maintain that there are a number of problems associated with the process of computer matching (discussed below).

Lack of Government Oversight

In the past, opponents have been critical of the lack of government regulation of computer matching. Today, although many jurisdictions have introduced some measure of control, criticism centres on the narrow focus of the regulations and/or guidelines and the fact that computer-assisted front-end verification and computer profiling have yet to be specifically studied and regulated.

Lack of government oversight has meant there is a paucity of reliable information on computer matching. In 1986, the United States Office of Technology Assessment conducted an extensive assessment of electronic record systems and found there was little or no information on:

- the scope and magnitude of computer matching, front-end verification and computer profiling activities,
- the quality and appropriateness of personal information that is being used in these applications, and
- the results and cost-effectiveness of these applications.[49]

Cost-Effectiveness

Without reliable documentation and consistent cost-benefit analysis, critics think that all claims regarding the cost-effectiveness of computer matching are without basis. They also argue that when all the associated costs (e.g., software cost, computer and staff time, etc.) are included and the financial savings realistically tallied, the costs of matches may be greater than the savings.[50]

The claims that computer-assisted front-end verification results in a greater saving than traditional computer matching have also been challenged. The practice does not eliminate the need for later matching as client circumstances change over the course of time.[51] This means that institutions using front-end verification may also employ computer matching at a later date for the purpose of detecting fraud, thereby, incurring twice the costs.

Quality and Accuracy of Information

There is considerable concern over the ability of computer matches to produce accurate and reliable results due to the type and frequency of errors which are seen to be inherent in the matching process. Errors result from erroneously reported or inaccurately entered data, time lags, hardware and software problems, and the abstract nature of the decision process.[52]

Critics want government institutions conducting matches to understand that a database is not "a perfect reflection of reality"[53] and that information created by computer matching should not be used for decision-making purposes without proper verification. Opponents do not believe that matching is reliable as this process can never identify all hits.[54] Matching may also identify infractions where none exist.[55]

Some critics maintain that often insufficient or inaccurate information is compared in matches, leading to information being taken out of context or misapplied. Faulty or inappropriate selection criteria are thought to distort the results of the match. Additionally, computer matching is considered to only work effectively where the databases are similar.[56]

An additional problem relating to the accuracy of information used in matches stems from the fact that computers tend to "freeze dry" information. Data which is accurate for a moment in time may be preserved by a computer and then that moment extended temporally and spatially through a match, often to the detriment of the data subject.[57]

Appropriateness of Computer Matching

It is thought that with sufficient experience, checking, and updating, technical errors such as hardware and software problems, can be reduced to an acceptable minimum. However, errors created by substituting "technical for human judgement and profiles based on samples for which the true parameters are unknown"[58] are felt to be far more difficult to correct. When used as a decision guide, rather than as an aid, matching is thought to be misused. The machine should not be a substitute for human discretion and judgment.[59]

Problems with Computer Profiling

Certain problems are considered to be inherent in the process of computer profiling and the use of statistical reasoning and group comparisons. The database used for constructing a profile may be reasonably accurate, but it may not be representative of reality as important information may never have been entered into the system. For example, it is sometimes argued that our knowledge of criminals is distorted because it is based primarily on those who have been caught and they may be less competent than those who manage to avoid apprehension.[60] In addition, there is also concern about the accuracy of the selection criteria, the relevancy of the data used, and the appropriateness of using profiling for certain decisions.[61]

Changing Computer Environment

Rapid changes in computer technology, the pervasiveness of that technology within the government, coupled with a perceived lag in the government's responsiveness to that technology, have all raised a number of additional concerns regarding computer matching.

Everywhere in government, the percentage of records stored on computers has increased significantly over the past decade. These records differ from paper files in a fundamental way. Privacy advocates believe a paper file cannot easily be altered since any tampering with the written or printed word can, in most cases, be detected. Electronic data, on the other hand, may be readily corrupted.[62] There is also concern about the fact that technology enables rapid exchange of entire record systems, often without leaving an audit trail.[63]

In addition, since the late 1970s when the use of computer matching first came to the fore in the United States, the entire face of computer technology has changed dramatically. In the past, there was a centralized mainframe computer or host connected to terminals with fixed functions, that is, they could not be programmed. These terminals communicated through a network that was usually implemented and controlled by a data processing department.

This environment provided a relatively easy structure to control because all the functions of the terminals were fixed and known, all the network controls and the data in the network were designed around, and in the context of, a single host computer.

In today's environment, terminals are programmable which enables users to extract data from the host computer, manipulate it, and store it in mini- or personal computers (also known as microcomputers). This changes the very nature of data integrity and control.[64]

Privacy advocates think the type of computing environment described above lowers the accuracy and reliability of information because of the multiplicity of copies and change(s) in custodianship.[65] This means that extensive manipulation of a database threatens the integrity of the information. Should such information be used in a match, that lack of integrity jeopardizes the validity of the match. Critics of computer matching advise extreme caution because of this and note that verification and follow-up investigation are even more important in this new computer environment. An additional problem relating to matching is that electronic record systems make it difficult to determine who has custody and control of the information.[66]

Security

Privacy advocates argue that as more sensitive personal information is accumulated and linked together, "privacy rights are threatened by inadequate attention to data security issues."[67]

In a report by the United States National Research Council (released December 5, 1990), it was noted that computer systems are open to "safety and security catastrophes." The report warns that the prevalence of computers, the use of networks to link computers and the increase in computer literacy could lead to an explosion of accidents and security breaches. The report also notes that without adequate safeguards, there is a risk of "intrusions into personal privacy and potential disasters that could cause economic and even human losses."[68] These security concerns may be amplified by computer matching.

Another potential problem is that there is an increased use of portable computers, also known as briefcase, laptop or notebook computers. Such transportable computers aggravate the problems of data integrity and security, especially since information may be transported out of government offices into areas that are neither controlled nor secure.[69]

In addition, there is concern about the retention and security of the information created by the match. If, for example, the "hit list" is retained and then later used for another purpose, the mere presence on the list could lead to erroneous, and potentially harmful, assumptions in the future.[70] The dissemination of information through matching also increases the number of places where inadequate security may lead to unauthorized disclosure.

Merging of Regulatory Roles

Another perceived problem with the wide-spread use of computer matching is that it will result in the blurring of regulatory roles both within and between institutions.[71] Welfare workers will become bill collectors or police officers, thus combining wholly separate functions. Such an occurrence would, it is argued, undermine the traditional checks and balances in government.[72]

3.4 Privacy Implications

Computer matching has been criticized by a great many sources throughout the western world. Much of that criticism has focused on the perceived threat computer matching poses to individuals' civil liberties and right to informational privacy. Since the mid-1980s the Privacy Commissioner of Canada has been one of the most vocal opponents of unregulated computer matching. In the 1987–88 Annual Report he stated:

> … it is a technique which, unbridled, would present an Orwellian threat which even Orwell could not have imagined. The invasive, indiscriminate use of the computer in gathering, storing and comparing personal information for purposes either benign or malign, reduces individuals to commodities, subjugates human values to mere efficiency.[73]

This sentiment is echoed by many privacy advocates. However, computer matching, in and of itself, does not create the privacy problems, it is the use to which it has been put and the action resulting from the process which has raised the concern. The potential benefits of computer matching are generally acknowledged but, as the Canadian Privacy Commissioner has also noted: "It is precisely the goodness of the cause which makes matching both so attractive and so hard to stop."[74]

The central issue in the debate about computer matching and related practices is whether there are adequate safeguards associated with the new technology to prevent violations of personal privacy.[75]

As the Supreme Court of Canada has yet to make an explicit and definitive ruling as to the constitutional right to informational privacy, the arguments presented below are those which have been raised by privacy advocates in other jurisdictions, primarily in the United States.

Loss of Control of Personal Information

Much of the criticism directed at computer matching centres around the fact that, in the past, matches have been undertaken without the data subject's knowledge or consent. In addition, information used in a match may be obtained from other institutions or third parties, and not from the individual to whom the information relates.[76] This practice is seen to be in direct violation of fair information practices.

A further concern created by computer matching is that personal information is collected for one purpose (e.g., filing an income tax return) and then used in a match for another purpose (e.g., determining whether welfare recipients are correctly reporting their income when they apply for benefits). This is considered an invasion of privacy as the individual to whom the information relates cannot control the use of his/her personal information.

Increased exchanges and manipulation of information held by computers also makes it difficult for an individual to know what personal information is maintained by an institution. The use of computer matching and the "extension of bureaucratic surveillance power through computerization" is seen to shift the balance between the rights of individuals and the informational needs of the government, away from the individual. It also creates the unusual situation where the computer becomes an informant, making avenues of redress and the ability to face one's accuser difficult.[77]

Search and Seizure

Privacy advocates think that computer matching equates to a general electronic search, a "fishing expedition" or "dragnet," because it is performed without any pre-existing evidence or suspicion of wrongdoing.[78] As the Australian Privacy Commissioner stated:

> [Computer matching] is like investigators entering a home without any warrant or prior suspicion, taking away some or all of the contents, looking at them, keeping what is of interest and returning the rest, all without the knowledge of the occupier.[79]

To fully understand this allegation and why computer matching is viewed as a violation of individual privacy rights, it is necessary to grasp the differences between a computer matching investigation and a traditional law enforcement investigation. A traditional investigation is generally triggered by some evidence that a person is possibly engaged in wrongdoing. A computer match is not bound by this limitation. It is directed not at an individual, but at an entire category of persons. It is random in nature as it is not initiated because any person is suspected of misconduct, but because a category (e.g., welfare recipients) is of interest to the government. What makes computer matching fundamentally different from a traditional investigation is, therefore, that its very purpose is to generate the evidence of wrongdoing required before an investigation can begin.[80] The Canadian Privacy Commissioner has noted:

> Thus do old-fashioned "fishing expeditions" pose as high technology. What is wrong about "fishing expeditions" is wrong about unrestrained computer-matching: it changes the way a government looks at its citizens.[81]

Participating in a government program or being a government employee should not inherently give rise to any suspicion. It is a status, not a crime. To subject a whole class of citizens to a search for possible violations is thought to be akin to a "general warrant," a practice in England that permitted the Crown to search without specifically naming the target.[82]

American supporters of computer matching have argued that harm to individuals is minimal and that most individuals are not even aware of the match. They also hold the view that "if you haven't done anything wrong, you don't have anything to worry about."[83] Opponents, on the other hand, view matching as nothing more than "sanitized search and seizure,"[84] making palatable what would never be tolerated under different circumstances. What many have also found objectionable is that because the underlying payoff to society, such as improved efficiency in government, is deemed to be positive, all sorts of abuses are tolerated, i.e., the end justifies the means.[85]

American privacy advocates have argued that computer matching, as a general electronic search, is in violation of the Fourth Amendment to the United States Constitution.[86] Others, however, consider such an argument false and note that there are many similar searches (e.g., airport scanning of luggage) which are accepted as a necessary evil. Some supporters also think that it may be persuasively argued that a computer match program does not search through records but only scans and ignores records unless pre-selected data elements contain relevant discrepancies. In other words, only records where there are "hits" are searched.[87]

Although the issue of computer matching has not been addressed by the Canadian courts, this practice may raise a comparable debate in Canada as section 8 of the *Charter of Rights and Freedoms* states: "Everyone has the right to be secure against unreasonable search or seizure."[88]

Presumption of Innocence

The principle of the presumption of innocence (i.e., everyone is presumed to be innocent until proven guilty) is embodied in subsection 11(d) of the Canadian *Charter of Rights and Freedoms*.[89] There is a concern that computer matching tends to turn this presumption of innocence into the presumption of guilt. Matching is seen to shift the burden of proof from the institution having to prove wrongdoing to the data subject having to prove innocence.

Critics noted that even when there is no indication of wrongdoing, there is the presumption that anyone who appears as a "raw hit" is guilty.[90] In the past, 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.[91]

Supporters of computer matching maintain that the presumption of innocence is not an issue if the "hits" resulting from computer matching are treated as evidence of possible wrongdoing and subjected to further investigation and verification.

Computer profiling is seen as the worst offender vis-a-vis this change in presumption of innocence. Individuals who fit the profile are treated differently from those who do not. Guilt is inferred from the probability that an event will or has occurred. A judgment is made about a particular individual based on the past behaviour of other individuals who appear statistically similar, that is, who have similar demographic, socioeconomic, physical or other characteristics.[92]

Due Process

The issue of due process is one of the most contentious in the ongoing debate about the lawfulness of computer matching. By due process it is meant the right to challenge and refute the government's information before a decision is made.

In the United States, decisions adversely affecting data subjects have been made based solely on the "raw hits" produced by a match. To the extent that the data subjects 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, according to the American Civil Liberties Union.[93]

This issue may arise under section 7 of the Canadian Charter of Rights and Freedoms which states:

> Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.[94]

Dealing specifically with computer-assisted front-end verification, in many of these programs performed in the United States before 1986, the data subjects were not informed of the verification, or were only informed indirectly, i.e., that the information would be verified but not how or when.[95]

With front-end verification it is generally a simple process to notify applicants that information they provide will be verified before benefits/services are granted. However, critics question whether notice is useful for the individual under these circumstances. The purpose of notice is to give individuals the time and information they need to act. In the case of front-end verification, notice generally leaves the individual only one recourse if he/she does not want the information verified, and that is to withdraw the application.[96] Even in cases where consent for verification has been given, there is concern that such consent may result from duress and coercion. The belief that a badly needed benefit may be cut if consent is not given is not seen as a real choice.[97]

Those who support computer matching maintain that the argument regarding due process is misleading. They note that the right to confront an accuser has never applied to the purely investigative stages of a law enforcement activity.[98] In addition, they maintain that due process is not an issue if after the match has been done and the investigation completed, the data subjects are informed of what information was used, how the conclusions were arrived at and that they have an opportunity to refute the evidence.

Equal Protection

Privacy advocates also maintain that computer matching conflicts with the right of equal protection under the law as matches are inherently mass or class investigations, conducted on a category of people rather than on individual suspects.[99]

Another criticism of computer matching in the United States is that it has been targeted towards certain racial and income groups. However, those who feel computer matching is a viable audit tool have noted that: "Computer matching is racially, sexually, and ethnically blind."[100]

This concern regarding equal protection and computer matching may also arise in Canada as a result of subsection 15(1) of the *Charter of Rights*, which states:

> Every individual is equal before and under the law and has the right to equal protection and equal benefit of the law without discrimination and, in particular, without discrimination based on race, national or ethnic origin, colour, religion, sex, age or mental or physical disability.[101]

Creation of New Information and Databases

The public's fear of a single omnipotent government database may not be as extreme as it first sounds. In many countries where computer matching is used, computerized databanks have been created solely for matching purposes.[102] This means that information collected for one purpose has been copied or transferred so that it can permanently be used for unrelated purposes on an ongoing basis.

In the United States, for example, the technology requisite for front-end verification has lead to the establishment of individual databases for verification purposes and to the connection of these databases through on-line telecommunication linkages. This process is seen to have lead to the creation of a *de facto* national database covering nearly all Americans.[103]

4. Comparative Jurisdictions

As noted earlier, there is no specific provision in the *Freedom of Information and Protection of Privacy Act, 1987*, as amended, which explicitly addresses the issue of data or computer matching. Outlined below are summaries of how some other jurisdictions have dealt with the issue.

Quebec

Unlike Ontario, Quebec has a specific provision in its privacy statute[104] which addresses this issue:

> **68.1.** A public body may, without the consent of the person concerned, release a personal information file for the purposes of comparing, pairing or matching it with a file held by a person or body, if the release is necessary for the carrying out of an Act in Quebec.
>
> Any operation under this section shall be carried out under the terms of a written agreement.

Articles 69 and 70 discuss some of the terms of the written agreement contemplated in Article 68.1 and the role of the Commission d'acces a l'information:

> **69.** The release of nominative information contemplated in sections 67, 67.1, 67.2, 68 and 68.1 shall be made in such a manner as to ensure the confidentiality of the nominative information. In cases where a written agreement is required, the agreement shall provide for the means to ensure confidentiality.
>
> **70.** Every agreement under section 68 or 68.1 must be submitted to the Commission for an opinion. The agreement comes into force on government approval.
>
> The agreement and the Commission's opinion are tabled in the National Assembly within fifteen days approval, if the Assembly is in session, or, if it is not sitting, within fifteen days after the opening of the next session, or of resumption.
>
> The Government may, after obtaining the opinion of the Commission, revoke the agreement at any time.

The Quebec Commission is in the process of studying the development of computer matching within Quebec. According to the Quebec Commission, a more proactive approach is currently being taken with regards to the approval of computer matches. The match applications are being analyzed systematically and on-site technical reviews are being performed.[105]

Federal Government of Canada

As in the case of Ontario, there is no specific provision in the federal *Privacy Act* which addresses the issue of data or computer matching. However, the Treasury Board of Canada, the body which advises the federal government on how to administer the federal *Privacy Act*, issued a policy on *Data Matching and Control of the Social Insurance Number* on June 26, 1979.

The federal policy is based on the United States government's 1979 computer matching guidelines. The basic principles underlying both these guidelines are as follows:

- **Public Notification:** A matching program should only be established after the public has been notified and given the opportunity to identify privacy problems.
- **Data Security:** Such a program should only be conducted with safeguards on access to the data and on disclosure of the names of suspects identified by matching.
- **Exhaust Alternatives:** Such a program should only be established when there are no alternative, cost-effective means of identifying violators.

The Canadian federal policy, which applies to all government institutions listed in the schedule to the *Privacy Act*, requires institutions to do the following:

- prior to the initiating of matching programs, institutions must assess the feasibility of the proposed programs by doing a cost benefit analysis of the impact of the matching,
- the institutions must notify the Privacy Commissioner of new matching programs by providing him with copies of their assessments 60 days prior to when the programs are scheduled to begin,
- the Privacy Commissioner may make recommendations to the heads of institutions concerning the matching programs; only the heads of institutions or officials specifically delegated authority by the heads may approve matching programs,
- institutions must account publicly for the matching programs in the Index of Personal Information, and
- institutions must subject information generated by matching programs to a verification process prior to using the information for administrative purposes.

Australia

Like the Quebec Act, Australia's *Privacy Act 1988* specifically addresses the issue of data matching. Subsection 27(1)(k) of the Australian Act provides as follows:

> **27.**(1) Subject to this Part, the Commissioner has the following functions:
>
> (k) on request of a Minister or agency, to examine a proposal for data matching or data linkage that may involve an interference with the privacy of individuals.

The Australian Privacy Commission has recently released draft guidelines on the subject of computer matching in a discussion paper entitled *Data Matching in Commonwealth Administration, October 1990*. The guidelines require that if a matching proposal is to proceed, the agencies responsible must prepare a program protocol dealing with such matters as the purposes of the program, the legal authority and its costs and benefits. Prior to the commencement of the program, draft technical standards must be in place, which then must be finalized after the program has been running for an initial period of time. These arrangements are subject to monitoring by the Privacy Commissioner. The Privacy Commissioner is required to report to the Attorney General and through him to Parliament.[106]

The objectives of the guidelines are listed as follows:

- to ensure that data matching programs are only undertaken where there are substantial social benefits which outweigh the privacy of individuals in relation to their personal information;
- to ensure that data matching programs are conducted in a manner which avoids any further and unnecessary intrusion into privacy and avoids unfairness;
- to ensure that data matching programs are regularly monitored as to their compliance with these guidelines and their continued justification.[107]

The United States

The federal government of the United States has implemented comprehensive legislation, the *Computer Matching and Privacy Protection Act of 1988*, dealing with this issue. The legislation amends the *Privacy Act* of 1974. The purposes of this legislation are seen to be two-fold:

- the establishment of uniform procedures under which agencies would perform matches so that the subjects of the matches are afforded due process,
- the establishment of a number of oversight mechanisms to ensure that agencies implement the bill procedures.[108]

The legislation expands the scope of the *Privacy Act* to include any non-federal matching entity. A "non-federal entity" is defined to include any state or local government, or agency of such government, and any public or private organization participating in a matching program. It excludes any computerized comparison devised to produce anonymous statistical or research data and matches of tax information conducted pursuant to the tax code. The legislation also provides an exemption for any match performed subsequent to the initiation of a specific criminal investigation designed to gather evidence for a prospective law enforcement proceeding against named individuals.

To ensure the protection of individual privacy, the legislation requires that before exchanging information, a recipient or a source agency must publish, in the Federal Register, notice of the establishment of the matching program.

In addition, all agencies involved must enter into a written agreement which details specific aspects of the matching program. The agreement must state the justification, purpose and authority for conducting the match, and describe the records that will be utilized. Procedures for notifying applicants, both upon initial application and periodically thereafter, that any information provided may be subject to verification through matching programs must also be provided in the matching agreement.

Likewise, the method for conducting such verification, and the measures implemented to ensure physical security of the records, matched and created by the program, must be particularized in the written agreement. The agreement must also include any information regarding assessments that have been made on the accuracy of the records that will be used in the matching program. Copies of the agreement must then be provided to the appropriate Congressional and Senate Committees and be made available to the public.

In addition to detailing the requisite elements of a matching agreement, the legislation addresses the need for information verification. The legislation requires that an agency independently verify information produced by a matching program before it may deny, terminate, suspend or reduce any federal financial assistance. The legislation contains a provision regarding notice and the opportunity to contest the agency's findings.

Finally, the legislation requires every agency to establish a Data Integrity Board to oversee and coordinate the agency's implementation of this legislation. The Board is to be comprised of senior agency officials. It is the duty of each Data Integrity Board to review, approve and maintain all written agreements to ensure compliance with the legislation. This last aspect creates quality assurance problems as agencies are given the task of approving their own matching programs.

The European Community

The European Community has adopted a program that involves the creation of a single European Community Information Market. Part of this program involves addressing the concerns surrounding data or computer matching. The approach to be taken to these concerns on the part of the European Community is currently in the process of being studied and formalized. The Secretary to the European Community's Legal Advisory Board, responsible for Telecommunications, Information Industries and Innovation, expressed the need to address this issue as follows:

> The fears expressed by citizens at the advent of large informatics systems, fears that had been tempered down by national data protection legislations, could be revived by the prospect of interconnecting information services networks at the Community level.[109]

France

France has had legislation dealing with this topic since 1978. In that year the *Law No. 78-17 Relating Data-Processing, Card Files and Freedom* was passed. That legislation enunciated several privacy protection principles including the following:

> **Article 1:** The data processing must be at the service of each citizen. Its development must operate within the realm of international cooperation. It must not infringe either on human identity, or on human rights, or on private life, or on freedom whether individual or public.
>
> **Article 2:** No legal decision involving an appreciation on human behaviour may have its foundation on an automatic processing of information giving a definition of the profile or the personality of the interested party.
>
> No administrative or private decision involving an appreciation on human behaviour may have for sole foundation an automatic processing of information giving a definition of the profile or the personality of the interested party.

The legislation also created the National Commission on Informatics and Freedom. "Informatics" is an expression that describes the organization, processing and transmission of personal information, normally by computers, but also includes a concern for the implications of information systems for society.[110]

The National Commission on Informatics and Freedom has to authorize record linkages through controlling applications of data processing for the handling of nominative information.[111] In general, the Commission is opposed to linkages because of the principle that data should be used only for the purposes for which it was collected.[112]

United Kingdom

In England, it is the duty of the Data Protection Registrar to uphold the principles of the *Data Protection Act 1984*. Any person who holds personal information must register as a data user with the Protection Registrar. This leaves that office with great leeway in determining the data protection issues that are to be examined.

In the *Sixth Report of the Data Protection Registrar June 1990*, the subject of matching was listed as being a significant issue. The Data Protection Registrar recommended that a study is needed of "the situations in which [computer matching] is occurring, of possible future developments and of policies to control the use of this method of drawing together information on individuals…" and that more work is required to assess the implications of profiling.[113]

Sweden

Under the Swedish *Data Act*, the Swedish Data Inspection Board controls most of the matching that occurs in that country. Specific permission is required from the Data Inspection Board to perform linkages of files that contain personal data procured from any other personal file, unless the data is recorded or disseminated by virtue of a statute, a decision of the Data Inspection Board or by permission of the person registered.

The Data Inspection Board evaluates all the proposals for data linkages. It has approved an estimated 80 to 90 percent of the proposals thus far. The Data Inspection Board primarily reviews the purpose and the quality of the match. Some of the elements reviewed include timeliness, accuracy and completeness of the matching scheme. In general, the Board is opposed to linkages of sensitive personal information (e.g., drug addiction and alcoholism records) and matching where the users do not know why personal information was originally collected.[114]

The concerns regarding the existence of easy matching schemes is evidenced in the comments of one of the members of the Data Inspection Board who stated: "A society that could develop a workable scheme to end all tax frauds would be an impossible place for persons to live." Another member of the Board has stated that a complex system of linkages will not work because it is impossible to assure the quality of the data and to inform Swedish citizens of their rights.[115]

Federal Republic of Germany

The German *Federal Data Protection Act* contains a general prohibition against the dissemination of personal data from one public body to another. An exception to this rule allows competent recipients to receive personal data for the purpose of accomplishing legitimate tasks. Computer linkages or matches are common among social services and do not have to be reported to the Data Protection Commissioners. However, most linkages of social service data outside the social service administrations are prohibited by the Social Code unless the information is necessary to prevent premeditated crimes, to protect public health under certain circumstances, to implement specific stages of the taxation process and to assist the registered alien authorities.[116]

Comparative Jurisdictions Summary

The general rule in regards to the regulation of computer matching in these various jurisdictions is that the matching proposals must be submitted, in writing, to a data protection agency for review. Some of these agencies then have the authority to quash the proposals while others merely are permitted to make recommendations.

The strongest legislative schemes regulating data matching exist in the European countries. While there is evidence that those nations recognized from early on the dangers of matching, the strength of the legislative decrees can also be explained by the fact that these nations are mostly civil law jurisdictions as opposed to the British and North American common law jurisdictions.

Contrary to the common law where legal rules are established through precedents, born of judicial decisions on a case-by-case basis, the civil law exists through a written code of conduct. This code establishes how the citizens of that country are to go about leading their lives. The rules are very general and are not necessarily subsequently litigated. As a result, even if strong general language has been passed regarding information and privacy, such action may speak more to a general intention than to a regulated legislative scheme. However, computer matching concerns have also been addressed by common law jurisdictions such as Australia, the United States, and the Canadian federal government.

The jurisdictions mentioned herein have recognized that data or computer matching is a significant problem that is to be regulated by some form of government. All the jurisdictions discussed above have already performed studies on the subject or are in the process of commissioning studies on the subject.

5. Conclusion and Recommendation

Computer matching is a technically and ethically complicated subject, with far-reaching administrative, law enforcement and privacy implications. It is also one which has become more common-place over the last decade. As noted by the Privacy Commissioner of Canada in 1983:

> The pressure is mounting to make computer-matching a standard investigatory technique. It is inevitable that government will want to put the full potential of the computer to use not only in the name of efficiency but for apprehending, for example, tax evaders or welfare cheats. No one will quarrel with that objective. Computer-matching to detect what is called economic crime is in fact now being carried out routinely in many foreign jurisdictions.[117]

The pressure to implement computer matching and related techniques for law enforcement and administrative purposes will likely increase in the future. Ontario will not be immune to such pressure. Accordingly, if the government wants to guard against the outpacing of ethical and legal standards by technological developments,[118] consideration must be given to regulating the use of computer matching within Ontario.

Justice La Forest, of the Supreme Court of Canada, has noted that:

> … if privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated. … Invasions of privacy must be prevented, and where privacy is outweighed by other societal claims, there must be clear rules setting forth the conditions in which it can be violated.[119]

Additionally, the Canadian Privacy Commissioner has noted, if there are no safeguards placed on computer matching, there is a danger that computers will "function mindlessly and without discrimination, as mere machines must do."[120]

There is a pressing need to determine the extent of computer matching within Ontario and, as noted recently by the Australian Privacy Commissioner, to "bring a degree of public accountability and discipline to bear on data-matching."[121] The acceptability of computer matching depends, in part, on establishing a proper balance between the legitimate information needs of government and individuals' rights to privacy. It is evident that computer matching is an important and beneficial tool for government, however, it is also evident that the privacy concerns associated with matching are grave enough to merit some form of regulation.

The statutory authority of the Information and Privacy Commissioner/Ontario to review matching programs is limited. As a result, the Office of the Information and Privacy Commissioner is not able to regulate or monitor the majority of computer matches within the provincial government. The Commissioner is even unable to determine the existence of current or proposed matching programs.

Due to the limitations of the *Freedom of Information and Protection of Privacy Act, 1987*, it is inappropriate to attempt to regulate computer matching within the existing statutory framework. Therefore, it is suggested that the following recommendation be adopted by the Standing Committee on the Legislative Assembly.

Recommendation: Establishment of A Task Force

Computer matching is so complex and has such far-reaching privacy implications that in order to properly understand and assess this issue, various jurisdictions, as discussed above, have undertaken studies on this topic. As Ontario has established a scheme of privacy protection, keeping up to date with world developments in privacy matters, computer matching should also be examined and dealt with in this jurisdiction.

To properly examine computer matching within the Ontario government, it is recommended that a Task Force be created to examine this issue and its associated privacy concerns, and to recommend an appropriate mechanism to control and monitor computer matching.

As this paper represents only a partial examination of this issue, the Task Force could perform a complete survey of computer matching and address the concerns on both sides of the matching issue. Additionally, the Task Force would be in a position to determine the extent of this practice in Ontario, and to consider if all types of computer matches within the Ontario government need to be regulated. This type of review would provide for public participation and would assist in continuing the concept of open government that is embodied in the *Act*. Another benefit to establishing a Task Force is that its final report will greatly assist those institutions eventually assigned the responsibility of monitoring the problem of data matching.

To avoid undue delay in the introduction of a regulatory scheme for computer matching, it is suggested that the Task Force have a time limit of six months to complete its study. It is also recommended that the Task Force be composed of representatives from government institutions which may be involved with, or have concerns regarding the management of computer matching in Ontario (e.g., Management Board of Cabinet, Human Resources Secretariat, Ministry of Health, Ministry of the Attorney General, Ministry of Community and Social Services, Ministry of Government Services, Ministry of Transportation, and the Ministry of Revenue). Privacy advocates and technology experts from the privacy sector could also be included on the Task Force.

Endnotes

1. Subsection 2(1) of the *Act* defines personal information as:

   2.-(1) "personal information" means recorded information about an identifiable individual, including,

   (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

   (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

   (c) any identifying number, symbol or other particular assigned to the individual,

   (d) the address, telephone number, fingerprints or blood type of the individual,

   (e) the personal opinions or views of the individual except where they relate to another individual,

   (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

   (g) the views or opinions of another individual about the individual, and

   (h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

2. United States Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy* (Washington, D.C.: U.S. Government Printing Office, June 1986), p. 73.

3. *R.* v. *Dyment* (1988), 89 NR 249 (SCC), pp. 260 and 263.

4. Statement by President George Bush, June 22, 1990, as cited in *Privacy Times*, July 5, 1990, p. 2.

5. Office of Technology Assessment, *Electronic Record Systems*, p. 38.

6. Letter to the Office of the Information and Privacy Commissioner/Ontario from Mr. Brian J. Foran, Head, Systemic Investigations and Data Matching, Office of the Privacy Commissioner of Canada, December 24, 1990.

7. Anne R. Field, Robert Neff, Frances Seghers, and Kathleen Deveny, "'Big Brother Inc.' May Be Closer Than You Thought," *Business Week*, February 9, 1987, pp. 84–85.

8. Arthur J. Cordell, *The Uneasy Eighties: The Transition to an Information Society* (Ottawa: Ministry of Supply and Services Canada, 1985), p. 75.

9. Office of Technology Assessment, *Electronic Record Systems*, p. 41.

10. Jim Durnil, "Detecting Fraud, Waste and Abuse Through Computer Matching," *Government Accountants Journal*, Summer 1983, p. 24.

11. Privacy Commissioner, *Data-matching in Commonwealth Administration: Discussion Paper and Draft Guidelines* (Sydney: Human Rights and Equal Opportunity Commission, October 1990), p. 4.

12. Testimony of Richard P. Kusserow, Inspector General, Department of Health and Human Services, *Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs: Hearings before the Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, United States Senate, Ninety-Seventh Congress, Second Session, December 15 and 16, 1982* (Washington, D.C.: U.S. Government Printing Office, 1983), p. 6.

13. Letter to the Office of the Information and Privacy Commissioner/Ontario from Mr. Brian J. Foran, Head, Systemic Investigations and Data Matching, Office of the Privacy Commissioner of Canada, December 24, 1990.

14. Mick Rood, 1990 States News Service, October 22, 1990.

15. Privacy Commissioner, *Annual Report Privacy Commissioner 1989-90* (Ottawa: Minister of Supply and Services Canada, 1990), p. 4.

16. Arthur Miller, "Statement to Sub-Committee of U.S. Senate on Administrative Practice and Procedure" (Washington, D.C: 14 March 1967), as cited in Cordell, *The Uneasy Eighties*, p. 74.

17. The Gallup Poll of Canada, The Canadian Institute of Public Opinion Press Release, "The Gallup Report," January 2, 1984.

18. *The Decima Quarterly Report*, March 1987, as cited in a memorandum to the Office of the Information and Privacy Commissioner from Decima Research, January 25, 1988. p. 4.

19. Memorandum to the Office of the Information and Privacy Commissioner from Decima Research, January 25, 1988, p. 1.

20. Field, *et al*, "Big Brother," pp. 84–85.

21. Office of Technology Assessment, *Electronic Record Systems*, p. 38.

22. Nancy Reichman, "Computer Matching: Toward Computerized Systems of Regulations," *Law and Policy*, p. 391.

23. Ibid., p. 412.

24. Ibid.

25. Daniel B. Radner, "Inter-agency Data Matching Projects for Research Purposes," *Social Security Bulletin*, July 1988, p. 22.

26. United States General Accounting Office, *Computer Matching: Assessing Its Costs and Benefits* (Washington, D.C.: United States General Accounting Office, November 1986), p. 17.

27. Ibid., p. 67.

28. Priscilla M. Reagan, "Privacy, Government Information, and Technology," *Public Administration Review*, November/December 1986, p. 632.

29. Nancy Reichman, "Toward Computerized Systems of Regulation," p. 390.

30. Office of Technology Assessment, *Electronic Records Systems*, p. 86.

31. Gary T. Marx, and Nancy Reichman, "Routinizing the Discovery of Secrets: Computers as Informants," *American Behavioral Scientist*, March/April 1984, p. 429.

32. Privacy Committee, *Privacy Issues and the Proposed National Identification Scheme — A Special Report* (Sydney: Privacy Committee, March 1986), p. 56.

33. Marx and Reichman, "Computers as Informants," p. 425.

34. Reichman, "Toward Computerized Systems of Regulations," p. 387.

35. Richard P. Kusserow, "The Government Needs Computer Matching to Root out Waste and Fraud," *Communications of the ACM*, June 1984, p. 542.

36. Jim Luther, The Associated Press, April 20, 1990.

37. Statement of Eleanor Chelimsky, Director Program Evaluation and Methodology Division, as cited in *Computer Matching and Privacy Protection Act of 1987: Hearing before a Subcommittee of the Committee on Government Operations, House of Representatives, One Hundredth Congress, First Session on S. 496, June 23, 1987* (Washington, D.C.: U.S. Government Printing Office, 1987), p. 84.

38. General Accounting Office, *Computer Matching*, p. 10.

39. Testimony of Wilbur D. Campbell, Director, Accounting and Financial Management Division, General Accounting Office, as cited in *Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs*, p. 176.

40. General Accounting Office, *Computer Matching*, pp. 17–18.

41. Kusserow, "Government Needs Computer Matching," p. 545.

42. Ibid., p. 543.

43. General Accounting Office, *Computer Matching*, pp. 69–70.

44. Privacy Commissioner, *Data-Matching*, p. 7.

45. Kusserow, "Government Needs Computer Matching," p. 543.

46. Office of Technology Assessment, *Electronic Record Systems*, p. 80.

47. Privacy Commissioner, *Data-matching*, p. 7.

48. Office of Technology Assessment, *Electronic Record Systems*, p. 13.

49. Ibid., p. 5.

50. General Accounting Office, *Computer Matching*, p. 10.

51. United States General Accounting Office, *Eligibility Verification and Privacy in Federal Benefit Programs: A Delicate Balance* (Washington, D.C.: United States General Accounting Office, March 1, 1985), p. 14.

52. Marx and Reichman, "Computers as Informants," pp. 434–435.

53. Ibid., p. 435.

54. Durnil, "Determining Fraud, Waste and Abuse," p. 25.

55. Marx and Reichman, "Computers as Informants," p. 438.

56. The Law Reform Commission of Australia, *Privacy*, Vol. 2 (Canberra: Australian Government Publishing Services, 1983), pp. 152–153.

57. Reichman, "Toward Computerized Systems of Regulations," p. 404.

58. Marx and Reichman, "Computers as Informants," p. 436.

59. Ibid.

60. Ibid., p. 437.

61. Office of Technology Assessment, *Electronic Record Systems*, p. 87.

62. Cordell, *The Uneasy Eighties*, pp. 75–76.

63. Office of Technology Assessment, *Electronic Record Systems*, p. 23.

64. David R. Wilson, "Trends in Information Security," *Computer Security Journal*, Vol.IV No.2, pp. 30–31.

65. Ibid., p. 31.

66. Office of Technology Assessment, *Electronic Record Systems*, pp. 103–104.

67. Statement of Ronald L. Plesser, American Bar Association, *Computer Matching and Privacy Protection Act of 1987*, p. 124.

68. Mary Gooderham, "Computer-system safeguards urged," *The Globe and Mail*, December 6, 1990, p. A12.

69. Office of Technology Assessment, *Electronic Record Systems*, p. 25.

70. Willis H. Ware, *Emerging Privacy Issues* (Santa Monica: The Rand Corporation, October 1985), p. 16.

71. Reichman, "Toward Computerized Systems of Regulations," p. 400.

72. Ibid., p. 406.

73. Privacy Commissioner, *Annual Report Privacy Commissioner 1987–88* (Ottawa: Minister of Supply and Services Canada, 1988), p. 4.

74. Ibid., p. 6.

75. Ibid., p. 5.

76. Office of Technology Assessment, *Electronic Record Systems*, p. 58.

77. Reichman, "Toward Computerized Systems of Regulations," p. 403.

78. John Shattuck, "Computer Matching is a Serious Threat to Individual Rights," *Communications of the ACM*, June 1984, pp. 538–539.

79. Privacy Commissioner, *Data-matching*, p. vi.

80. Shattuck, "Serious Threat," p. 538.

81. Privacy Commissioner, *Annual Report Privacy Commissioner 1984–85* (Ottawa: Minister of Supply and Services Canada, 1985), p. 4.

82. Statement of Robert Ellis Smith, Publisher, *Privacy Journal*, as cited in *Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs*, p. 145.

83. Shattuck, "Serious Threat," p. 541.

84. Testimony of Ronald L. Plesser, Former General Counsel of the U.S. Privacy Protection Study Commission, *Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs*, p. 155.

85. Ware, *Emerging Privacy Issues*, p. 15.

86. Fourth Amendment of the United States Constitution:

    The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

87. Statement of Ronald L. Plesser, *Computer Matching and Privacy Protection Act of 1987*, p. 122.

88. *Constitution Act, 1982* [en. by the Canada Act 1982 (U.K.), 1982, c. 11 Schedule B], as amended.

89. Section 11 of the *Charter of Rights and Freedoms*:

    Any person charged with an offence has the right …

    (d) to be presumed innocent until proven guilty according to law in a fair and public hearing by an independent and impartial tribunal.

    Constitution Act, 1982 [en. by the Canada Act 1982 (U.K.), 1982, c. 11 Schedule B], as amended.

90. Shattuck, "Serious Threat," p. 539.

91. Ibid.

92. Office of Technology Assessment, *Electronic Record Systems*, p. 88.

93. Testimony of John H. Shattuck, National Legislative Director, American Civil Liberties Union, *Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs*, p. 80.

94. *Constitution Act, 1982* [en. by the Canada Act 1982 (U.K.), 1982, c. 11 Schedule B] as amended.

95. Office of Technology Assessment, *Electronic Record Systems*, p. 78.

96. Ibid., p. 80.

97. Marx and Reichman, "Computers as Informants," p. 440.

98. Kusserow, "Government Needs Computer Matching," p. 545.

99. Office of Technology Assessment, *Electronic Record Systems*, p. 57.

100. Kusserow, "Government Needs Computer Matching," p. 544.

101. *Constitution Act, 1982* [en. by the Canada Act 1982 (U.K.), 1982, c. 11 Schedule B] as amended.

102. Office of Technology Assessment, *Electronic Record Systems*, p. 39.

103. Ibid., p. 67.

104. *An Act respecting Access to documents held by public bodies and the Protection of personal information*, R.S.Q., chapter A-2.1.

105. Conversation between John Eichmanis and Denyse Roussel of the Quebec Commission d'acces a l'information on October 5, 1990.

106. Privacy Commissioner, *Data-Matching*, p. viii.

107. Ibid, p. 12.

108. Mark W. Iannotta, "Protecting Individual Privacy in the Shadow of a National Data Base: The Need for Data Protection Legislation," *Capital University Law Review*, Fall 1987, p. 128.

109. George Papapavlou, *Privacy Laws and Business*, December 1989, p. 8.

110. David H. Flaherty, *Protecting Privacy in Surveillance Societies* (Chapel Hill: The University of North Carolina Press, 1989) p. 176.

111. Article 6, *Law No. 78-17 Relating Data-Processing, Card Files and Freedom*.

112. Office of Technology Assessment, *Electronic Record Systems*, p. 61.

113. Data Protection Registrar, *Sixth Report of the Data Protection Registrar* (London: HMSO), p. 10.

114. Office of Technology Assessment, *Electronic Record Systems*, p. 61.

115. Flaherty, *Protecting Privacy*, p. 120.

116. Office of Technology Assessment, *Electronic Record Systems*, p. 61.

117. Privacy Commissioner, *Annual Report, Privacy Commissioner, 1983-84* (Ottawa: Minister of Supply and Services Canada, 1984), p. 4.

118. Marx and Reichman, "Computers as Informant," p. 441.

119. *R.* v. *Dyment* (1988), 89 NR 249 (SCC) p. 263.

120. Privacy Commissioner, *Annual Report 1983–84*, p. 4.

121. Privacy Commissioner, *Data-matching*, p. viii.

Bibliography

Computer Matching and Privacy Protection Act of 1987: Hearing before a Subcommittee of the Committee on Government Operations, House of Representatives, One Hundredth Congress, First Session on S. 496, June 23, 1987. Washington, D.C.: U.S. Government Printing Office, 1987.

Cordell, Arthur J. *The Uneasy Eighties: The Transition to an Information Society*. Ottawa: Ministry of Supply and Services Canada, 1985.

Data Protection Registrar. *Sixth Report of the Data Protection Registrar*. London: HMSO, June 1990.

Durnil, Jim. "Determining Fraud, Waste and Abuse Through Computer Matching." *Government Accountants Journal*, Summer 1983, pp. 24–27.

Field, Anne R.; Neff, Robert; Seghers, Frances; and Deveny, Kathleen. "'Big Brother Inc.' May be Closer Than You Thought." *Business Week*, February 9, 1997, pp. 84–86.

Flaherty, David H. *Protecting Privacy in Surveillance Societies*. Chapel Hill: The University of North Carolina Press, 1989.

Freedman, Warren. *The Right of Privacy in the Computer Age*. New York: Quorum Books, 1987.

Government of Canada. *Access and Privacy: The Steps Ahead*. Ottawa: Minister of Supply and Services Canada, 1987.

Iannotta, Mark. W. "Protecting Individual Privacy in the Shadow of a National Data Base: The Need for Data Protection Legislation." *Capital University Law Review*, Fall 1987, pp. 117–135.

Kusserow, Richard R. "The Government Needs Computer Matching to Root out Waste and Fraud." *Communications of the ACM*, June 1984, pp. 542–545.

Langan, Kenneth James. "Computer Matching Programs: A Threat to Privacy." *Columbia Journal of Law and Social Problems*, Vol.15 No.2, 1979, pp. 143–180.

Laudon, Kenneth C. *Dossier Society: Value Choices in the Design of National Information Systems*. New York: Columbia University Press, 1986.

The Law Reform Commission of Australia. *Privacy*. Report No. 22, Volumes 1 and 2. Canberra: Australian Government Publishing Service, 1983.

Leadbeater, Alan. "Computer Matching and Individual Rights: A Canadian Perspective." *Government Information Quarterly*, 1988, pp. 191–194.

Linowes, David F. *Privacy in America: Is Your Private Life in the Public Eye?*. Chicago: University of Illinois Press, 1989.

Louis Harris and Associates and Westin, Dr. Alan F. *The Equifax Report on Consumers in the Information Age*. Atlanta: Equifax Inc., 1990.

Marx, Gary T. and Reichman, Nancy. "Routinizing the Discovery of Secrets: Computers as Informants." *American Behavioral Scientist*, March/April 1984, pp. 423–452.

Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs: Hearings before the Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, United States Senate, Ninety-Seventh Congress, Second Session, December 15 and 16, 1982. Washington, D.C.: U.S. Government Printing Office, 1983.

Oversight of the Privacy Act of 1974: Hearings Before a Subcommittee of the Committee on Government Operations, House of Representatives, Ninety-Eighth Congress, First Session, June 7 and 8, 1983. Washington, D.C.: U.S. Government Printing Office, 1983.

Papapavlou, George. *Privacy Laws and Business*. Middlesex: Stewart H. Dresner, Publisher, December 1989.

President's Council on Integrity and Efficiency. *Model Control System and Resource Document for Conducting Computer Matching Projects Involving Individual Privacy Data*. Washington, D.C.: Office of Management and Budget, 1983.

Privacy Commissioner. *Annual Report, Privacy Commissioner, 1983–84*. Ottawa: Minister of Supply and Services Canada, 1984.

Privacy Commissioner. *Annual Report Privacy Commissioner 1984–85*. Ottawa: Minister of Supply and Services Canada, 1985.

Privacy Commissioner. *Annual Report Privacy Commissioner 1985–86*. Ottawa: Minister of Supply and Services Canada, 1986.

Privacy Commissioner. *Annual Report Privacy Commissioner 1987–88*. Ottawa: Minister of Supply and Services Canada, 1988.

Privacy Commissioner. *Annual Report Privacy Commissioner 1989–90*. Ottawa: Minister of Supply and Services Canada, 1990.

Privacy Commissioner. *Data-matching in Commonwealth Administration: Discussion Paper and Draft Guidelines*. Sydney: Human Rights and Equal Opportunity Commission, October 1990.

Privacy Committee. *Privacy Issues and the Proposed National Identification Scheme — A Special Report*. Sydney: Privacy Committee, March 1986.

Radner, Daniel B. "Inter-agency Data Matching Projects for Research Purposes." *Social Security Bulletin*, July 1988, pp. 22, 56–57.

Rankin, Murray. "Privacy and Technology: A Canadian Perspective." *Journal of Media Law and Practices*, April 1984, pp. 21–49.

Reagan, Priscilla M. "Privacy, Government Information, and Technology." *Public Administration Review*, November/December 1986, pp. 629–634.

Reichman, Nancy. "Computer Matching: Toward Computerized Systems of Regulations." *Law and Policy*, October 1987, pp. 387–415.

Shattuck, John. "Computer Matching is a Serious Threat to Individual Rights." *Communications of the ACM*, June 1984, pp. 538–541.

The Standing Committee on Justice and Solicitor General. *Open and Shut: Enhancing the Right to Know and the Right to Privacy*. Ottawa: Supply and Services Canada, March 1987.

Surveillance, Dataveillance and Personal Freedoms: Use and Abuse of Information Technology. Fair Lawn: R.E. Burdick, Inc., 1973.

United States Congress, Office of Technology Assessment. *Federal Government Information Technology: Electronic Record Systems and Individual Privacy*. Washington, D.C.: U.S. Government Printing Office, June 1986.

United States General Accounting Office. *Computer Matching: Assessing Its Costs and Benefits*. Washington, D.C.: United States General Accounting Office, November 1986.

United States General Accounting Office. *Eligibility Verification and Privacy In Federal Benefit Programs: A Delicate Balance*. Washington, D.C.: United States General Accounting Office, March 1, 1985.

Ware, Willis H. *Emerging Privacy Issues*. Santa Monica: The Rand Corporation, October 1985.

Wilson, David R. "Trends in Information Security." *Computer Security Journal*, Vol. IV No. 2, pp. 29–38.