Gouvernement du Canada
Ministère des Communications

Government of Canada
Department of Communications

Le Centre canadien de recherche sur l'informatisation du travail

Canadian Workplace Automation Research Centre

LEGAL ISSUES ARISING OUT OF INTEGRATED INFORMATION SYSTEMS:

AN OVERVIEW OF PRACTICAL CONSIDERATIONS AND RECENT DEVELOPMENTS

by Dr. Jake V. Th. Knoppers
Senior Guest Researcher

LEGAL ISSUES ARISING OUT OF INTEGRATED INFORMATION SYSTEMS:

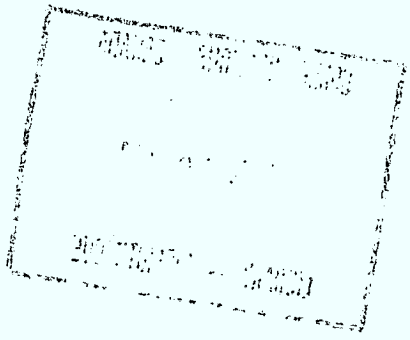
AN OVERVIEW OF PRACTICAL CONSIDERATIONS AND RECENT DEVELOPMENTS

by Dr. Jake V. Th. Knoppers
Senior Guest Researcher

Canadian Workplace Automation Research Centre

Prepared for the International Electronic Information Forum. Montreal, June, 1987. The opinions expressed in this report are those of the author.

DOC-CWARC-87-E-C04



Abstract

Formerly, and still to a large extent, recorded information was managed and used in hard-copy form. The introduction of new information technologies, the move towards their integration in recent years, and the striving for a paperless office, have brought to the fore a number of important legal issues. Information professionals would be well-advised to become aware of these issues and how to address them both from a professional point of view and from the need to integrate legal issues into their system development methodology. The area of office automation offers a particular challenge because it has only now reached the stage of integration, and because it has traditionally relied most heavily on paper.

Note to Readers:

The author welcomes comments, criticisms and suggestions on this research paper. Those wishing to be informed on further research in this area or who may wish to participate in this research program are also urged to contact the author.

TABLE OF CONTENTS

1.0 INTRODUCTION

Until recently the management and use of information basically has been the management and use of physical objects on which information was permanently recorded. That is, there existed a fixed one-to-one relationship between the recorded information and the physical carrier. This inseparable unit of recorded information and physical carrier was also not reusable. In reality, information management was, and remains to a large extent today, especially in the office, the management of physical objects (e.g. documents).

A whole range of laws and jurisprudence which developed over the centuries and which directly addresses various aspects of recorded information is technology dependent, i.e., they are directly linked to particular forms of recording information and to the means and methods for the distribution of information. The introduction of paperless information processing and communication technologies, coupled with their recent integration, has led to a situation where most of this traditional information law no longer applies. Even where it does, information processing professionals are not aware what these requirements are and if they are, how to integrate these legal requirements into their integrated information systems, i.e. both in management information systems and especially in the newly emerging integrated office systems.

This research paper is composed of three sections. The first section introduces and elaborates the concept of information law. The second identifies a number of key information laws, their relevancy and recent developments. The third section presents some practical considerations and identifies issues yet to be resolved.

The context of this research report is the legal, and thus management and operational, issues raised as a result of our increasing use of information technologies and what non-technical barriers may exist that prevent them from becoming the primary operational support systems for an organization.

That is, even if information technologies are available at the right price, with the appropriate functions, and management is willing to purchase and install such systems, what non-technical considerations and barriers must be addressed before one can move towards a "paperless" office?

2.0 INFORMATION LAW

2.1 Definitions

As information or data plays an increasingly important role in society and the economy at large, and in individual organizations in particular, it is not surprising that the last few years have seen a rapid increase in the laws, regulations, codes, guidelines, rules, etc., both nationally and internationaly, which govern what one can or cannot do or should do, with respect to recorded information. At the same time, existing laws or legal principles with which one had grown very comfortable, suddenly appear to have no relevance or application to the electronic digitized world. Those who had relied on these laws to provide a certain level of protection of guarantee of return on investment suddenly find themselves without recourse to law.

This problem is widespread. Hardly a statute or regulation is enacted or revised these days without consideration being given to how they are to address one aspect or another of the electronic and digitized world. In this paper the concept of information law is introduced to cover any law or pursuant statutes, or parts thereof, which deal with recorded information in one form or another.

Present definitions in law of "record", "document", "to produce", "to keep", "to maintain" are technology-bound (e.g. hard-copy). New, more generic and technology independent definitions are needed. The following sections propose three basic definitions, namely:

- "recorded information"
- "information handling"
- "information law"

2.1.1 Recorded Information

It would be useful to note that in this paper, the terms "data", "information", "record", "document", etc. are used interchangeably. They all refer to "recorded information". Recorded information is defined as:

> "information or data which is recorded regardless of its physical storage medium and in possession of an organization (ownership) and/or under the control of an organization in terms of its access and use or disposal and/or can be readily compiled/retrieved from information systems in new forms or combinations, using tools and mechanisms available in the usual and ordinary course of business".

If integrated information systems and especially integrated office systems are ever to become the mainstay of support for all our activities, i.e. a "paperless world", it will be necessary to revise or amend the definition of record, document, etc. in all laws and regulations to one which is generic and technology independent, i.e. "recorded, information".

2.1.2 Information Handling

Similarly, the concept of information handling is introduced as a generic term to cover the many types of functions or activities that can take place with respect to recorded information, such as:

> "any function with respect to recorded information such as creation or collection, processing, storage, retrieval, communications or flow, dissemination and distribution, access and use, protection, i.e. security, confidentiality, privacy, etc., retention, disposal, archiving, etc."

Information handling is thus the generic term used to cover the whole range of recording and storage media and all functions that can be performed using information processing and communications technologies. It is also a term that is not readily associated with any technology.

2.1.3 Information Law

The level of concern and degree of "informatization" has reached the plateau where it has become useful to categorize a body of laws and regulations as "information law"[1]. Information law can be defined as:

> "any law, regulation, policy, or code (or any part thereof) that requires the creation, production, retrieval submission, retention, storage or destruction of recorded information; or that places conditions on the access and use, confidentiality, reproduction, distribution, transmission, sale, sharing, or handling of recorded information".

Basically, information law and associated requirements can be broken down into a number of categories: namely those which,

- require one to keep or retain certain data for specified periods of time, commonly known as records retention requirements;
- require one to have the ability to produce or retrieve data, (e.g. for inspectors in certain industries);
- require one to submit or file data to a government or regulatory agency (e.g. tax data, customs data, filings with security exchange regulatory commissions);
- require one to create data if one undertakes a particular activity, (e.g. data on exposure to radiation, data on emissions);
- require one to destroy data (e.g. classified material, or information on persons);
- require one to protect data (e.g. privacy, information collected under the Statistics or Income Tax Act);
- place conditions on the access, use or confidentiality of recorded information (e.g. access to information, official secrets, new Criminal Code sections on computer crime, and data abuse, client-solicitor confidences, etc.);

- place conditions on the way in which one processes information (e.g. Evidence Act, financial regulations and standards, etc.);
- place conditions on the production, distribution or sale of recorded information (e.g. copyright, trade marks, hate literature, pornography);
- place conditions on the sharing, linking or flow of information (e.g. protection of personal data, restrictions on technology transfer); and,
- place conditions on the location where data is handled (e.g. the Bank Act or "at the head office")

Most information law operates at the national and provincial levels. However, the body of information law at the international level is increasing. It should be noted that at the international level a substantial part of information law developments is the result of governments and businesses working closely together to develop standards and codes, mostly voluntary, which are mutually acceptable.

It should also be noted that the categories of information law described above are not necessarily mutually exclusive. As a matter of fact, any law affecting the handling of recorded information often involves several categories of information law at the same time. One should look at information law from the much wider perspective presented above rather than limiting it to just a few categories such as copyright, trademarks, patents, broadcasting or publishing. Information law elements are also found in the rights guaranteed by the Canadian Charter of Human Rights and Freedoms, such as the freedom of expression, the freedom of communication, and freedom of the press, etc.

Information professionals as well as decision-makers in an organization should not underestimate the present and growing importance of information law. Regardless of whether one manages or uses large or small computer systems, develops applications or designs systems, etc., one should know the information law requirements for the organization which one serves, and for the data being processed in such systems. Irrespective of the technology used to handle recorded information in one's organization, information law

requirements must still be either complied with, where they are mandatory, or taken into account, where they are voluntary.

2.2 Recent Developments in Canadian Information Law

While many information laws are activity or industry specific, there are a number of key information laws which every organization must take into account. These are the Canada Evidence Act, the recently enacted new sections in the Criminal Code on computer crime and data abuse, records retention requirements, copyright, and increasingly in the public sector and to some degree in the private sector as well, access to information and privacy legislation.

While the examples given below are based on the Canadian context, similar problems or challenges with respect to "information law" exist in most countries.

2.2.1 Criminal Code

In Februay 1983, the Canadian Information Processing Society (CIPS) organized, with the assistance of the federal Department of Justice, a "National Consultation on Amendments to the Criminal Code dealing with Computer Abuse". Representatives from a wide mix of organizations and individual experts participated. The purpose of this consulation was to discuss and find ways on how the Criminal Code could be amended to cover actions commonly known as "computer crime" and "data abuse" and to advise the Department of Justice accordingly. The results of litigation in the courts at that time had made it quite clear that the provisions in the Criminal Code related to theft of a telecommunication service as found in section 287(1) of the Criminal Code could not be applied to concepts such as "theft of computer time or a computer service" or "theft or misappropriation of data".

This caused great concern among industry and professional associations. The use of computer-related technologies had reached the stage in many industry sectors and individual businesses where one had not only expended vast resources in building computerized records-keeping systems but had become very dependent on them as an indispensable tool in support of day-to-day operations. There was a groundswell of widespread concern that as one took advantage of new information technologies to become more efficient and cost-effective in one's operations that one suddenly found oneself without recourse to the protection of law just because one had changed the media of an organizations's recorded information from hard-copy to electronic form.

The two-day "consultation" covered a wide variety of areas related to the technological impacts on law and legal concepts (e.g. is data property?). In summary, the results of that consultation were that:

- the misappropriation, copying or destruction of proprietory information, be it a computer program or machine-readable record, should be a crime regardless of the media or form in which such recorded information is stored;

- because of the unique and new characteristics of computer systems and computerized or electronic data, the Criminal Code should be amended to specifically address these issues;

- there should be a separate section for a "computer crime" analogous to a telecommunications crime; and,

- there should be a new section which specifically would address the problem of "data abuse" and that this should not be confused with intellectual property rights (e.g., copyright).

A year later, on 7 February 1984, an omnibus bill to amend the Criminal Code, Bill C-19, was tabled but died in the order paper. Later reintroduced as Bill C-18, it contained two specific amendments pertaining to computer crime and data abuse. These amendments were passed, with some changes, by the House of Commons on 24 April, 1985, and received Royal Assent, i.e., became law, on 5 December, 1985. Of particular interest are two new sections: namely,

- s.301.2 which deals with unauthorized use of a computer; and,
- s.387.1(1.1) which introduces the concept of mischief in relation to data.

Bill C-18 also introduced new definitions for a computer program, computer service, computer system, data, function, intercept, and an electromagnetic, acoustic, mechnical or other device.

The wording of the relevant section dealing with unauthorized use of a computer is as follows:

> "s.301.2 (1) Everyone who, fraudulently and without color of right,
>
> (a) obtains, directly or indirectly, any computer service,
>
> (b) by means of an electromagnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or
>
> (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 387 in relation to data or a computer system,
>
> is guilty of an indictable offence and is liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction."

This new section on computer crime not only introduces in law the concept of theft of a computing service (as already exists for a telecommunications service under Section 287 (1)), but also makes illegal any form of eavesdropping, interruption in a computer operation as well as programming a computer to systematically attempt to establish unauthorized access to a computer system. The latter is a favoured technique of the computer "hacker". From the perspective of law enforcement, there appears to be little or no difference between a telecommunications device and a computer as far as illegal usage is concerned. Given the fact that it is becoming increasingly difficult in many instances to distinguish between a computer with telecommunications capability, and a telecommunications device with

computing capacity, this is a very useful feature and makes this Canadian law much simpler to administer than similar statutes either in the United States or Europe.

Secondly, the wording of the new section on data abuse is as follows:

"s.386.1 (1.1) Every one commits mischief who willfully

(a) destroys or alters data;

(b) renders data meaningless, useless or ineffective;

(c) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

Several comments on the section on data abuse are in order:

(1) The wording is both precise and wide enough to cover any possible action that one could take in relation to data including the deletion of data.

(2) From the perspective of enforcement, the operative word here is "willfully". That is, it would appear that one would need to have a feature in one's system and in one's operating procedures and instructions whereby data could not be altered or deleted "accidentally".

(3) While this section does not specifically make the addition of data a crime, i.e., adding false data, it can be argued that such action would interfere with the "lawful use of data" and would include "altering" data (sets), and/or unauthorized use of a computer function.

(4) Since a computer program or software, by definition consists almost totally of data, this new section should also cover any "theft" of one's proprietary computer programs, since such a "theft" would of

necessity involve a "willful" and "unauthorized" action involving both the computer and data.

Some new definitions, as found in section 301.2 (2) are as follows:

"computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function.

"computer service" includes data processing and the storage or retrieval of data.

"computer system" means a device that, or a group of interconnected or related devices, one or more of which,

(a) contain computer programs or other data, and

(b) pursuant to computer programs,
(i) performs logic and control, and
(ii) may perform any other function.

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system.

"electromagnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing.

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system.

"intercept" includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof.

Of particular interest is the possibility that these amendments to the Criminal Code may go a long way in addressing the problem of "illegal" copying of software. One could make such an argument in a number of ways. For example one, could argue that this involves the initiation of a computer function without colour or right, or that such copying could be construed as unlawful use of data since the definition of data includes instructions. While the question of copyright is addressed below in greater detail, it may well be that "creative" use of these Criminal Code amendments could be of assistance in arresting the widespread habit of "illegal" copying of software programs. This was the case recently where trade mark law was successfully used to prosecute for what was in effect a violation of copyright with respect to software.

It should also be noted that the amendment on data abuse stayed clear of the question of whether data is property by adding section 387(4) which sets penalties for mischief in relation to data quite apart and distinct from those for property in general. In addition, there is no $1,000 minimum value attached to data mischief as there is for mischief against property.

The penalty for a computer crime can range from summary conviction to ten years imprisonment while that for data mischief ranges from summary conviction to two years imprisonment.

Finally, it might be useful to draw the attention of information professionals and managers to a new section, 387(5.1), which reads as follows:

> "Every one who wilfully does an act or wilfully omits to do an act that it is his duty to do, if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or data,
>
> (a) is guilty of an indictable offence and is liable to imprisonment for a term not exceeding five years; or
>
> (b) is guilty of an offence punishable on summary conviction".

This clause appears to place a responsibility on managers of computerized information systems to exercise good stewardship and ensure that adequate security and confidentiality provisions are in place for their systems and the data they contain. For example, it can be argued that managers of computer systems which support vital functions in a hospital such as monitoring and controlling life support systems, who fail to install security measures that adequately protect such operations against unauthorized access and possible interference, i.e., by hackers or disgruntled employees, might expose themselves to possible charges under the Criminal Code.

As a matter of fact, to this author it appears perverse that managers of information systems are rarely fired when their systems are "broken into" or compromised by the so-called hackers, especially since the latter owe their ability to penetrate computer systems more on the basis of persistence or luck and, especially, on the lack of basic computer/communications security features in many systems than on the basis of their advanced knowledge of computer/communications technologies.

In this context, the "Code of Ethics and Standards of Conduct" [2] issued by CIPS in January, 1985 takes on added importance and it might be useful for CIPS, other associations of individuals or industry to seriously consider whether it would be both useful and appropriate to develop a code interpreting the obligation of good stewardship of information professionals in relation to data (including instructions on software) as found in section 387(5.1).

2.2.2 Evidence Act

While the new amendements to the Criminal Code on computer crime and data abuse clearly recognize the importance and value of computerized systems and data by providing protection for such resources, one other major legal issue in integrated information systems remains. This is the question of the admissibility of computer-generated records (CGR) as evidence in court. The need to amend the Canada Evidence Act was recognized over a decade ago, but

it was not until the spring of 1985 that a concerted effort was made to try to resolve the question of "admissibility of recorded evidence". At that time the Department of Justice asked the Association of Records Managers and Administrators (ARMA) to organize a national consultation focusing in the question of admissibility of recorded evidence (or NCARE). [3] A large and representative number of professional, industry, labor and other organizations participated in the NCARE consultation.

In one of the documents prepared for NCARE, it was noted that "in the absence of clear guidelines on the admissibility and weight given to computer-generated output and electronically produced signatures and authorizations, a significant bulk of paper documents are retained by each organization to record transactions and reduce potential litigation costs. Retaining this paper duplicates information already held in computerized form, adds to overhead and reduces competitiveness". [4] The study went on to report that paper in an office is growing at a rate of 20% per year, and that on the average 19 copies are made over the lifetime of a document. Not only are nearly all filed, but are never looked at again. The report concluded that "harmonizing admissibility criteria to the computerized information management systems that business uses, and would like to use, will increase the use of technology. This will provide new economies of scale, improve return on investment from information systems and improve decision support and productivity. The existence of admissibility criteria will also ensure a continuing focus on preserving the integrity of the organization's information resource... Additional benefits with the admissibility of computer-generated records will be a reduction in the dependence on paper decision support systems, leading to the reduction or possible elimination of paper records".

In a similar vein, ARMA in its brief to NCARE argued that "for most organizations and especially business, the prevalence of the use of computerized information/records-keeping systems is essential to their corporate survival and ability to reduce costs so that they can remain competitive in their field. For Canadian business to stay competitive, both domestically and internationally, it has no choice but to adopt and use the most cost-

effective technologies available... ARMA members have become very concerned about the fact that they cannot take full advantage of the new technologies to provide more efficient and cost-effective services to their organizations. If they do, they may jeopardize their potential for successful litigation, as either defendant or plaintiff." [5]

A court can only act on evidence properly before it. "The issue of 'admissibility' is therefore central to the law of evidence. In determining whether evidence is admissible, a judge must first decide whether it is 'relevant' to the case... Irrelevant evidence is therefore always inadmissible. However, relevant evidence may still be inadmissible because it offends one of the exclusionary rules". [6] On the whole, the Courts prefer to receive evidence from a witness having first-hand knowledge of the facts in question and being able to cross-examine the witness. Basically, the courts do not allow for hearsay. However, over the centuries, practices have been developed whereby exceptions to the hearsay rule, such as the admissibility of government, banking, business and medical records made in the "usual and ordinary course of business". Such exceptions to the hearsay rule are based on the justification that the inherent likelihood that such records would be erroneous is very small since business or government itself is relying on these records to make decisions and run their operations.

Another major exclusion of the hearsay rule is the best-evidence rule. Basically, it requires that where an original of the record exists, the original must be produced in court. However practices over the years have developed where, under certain conditions, copies and duplicates can be admitted (e.g. of banking records).

At present the status of the admissibility of CGRs is not clear. The jurisprudence in Canada is very limited and inconsistent. At the National Consultation, i.e., NCARE, the major questions raised were:

- the relevancy of concepts such as "original", "duplicate", and "copy" to CGRs;
- the interpretation of the phrase "in the usual and ordinary course of business" when one is increasingly using interactive online real-time

decision-support systems where the "record" is generated only at the request of the user, often in a unique and customized fashion;

- the role of data processing standards and whether standards were possible; and,
- whether the same rules of admissibility of CGRs should apply to all regardless of whether one is a bank, a government, a business or a medical institution.

In this context it must be noted that at present banking records have special status with respect to admissibility. "The argument is sometimes made that a less stringent standard of admissibility should apply to records and CGRs of banks and financial institutions as they have to balance their books everyday, and they are subject to continual scrutiny not only to their auditors but also by their customers. However, government and non-financial businesses would maintain that their records are also carefully kept and subject to audit... Indeed some government and non-financial businesses may be more sophisticated in their record keeping than some financial institutions". [7]

A new Uniform Evidence Act, applicable at both the federal and provincial levels, has been drafted but not yet tabled at the time of writing of this research paper. However, it is useful to note NCARE's recommendations. In summary form then, the suggestions of NCARE are that the Canada Evidence Act be amended to allow for the admissibility of CGRs by:

- adding new definitions in relation to computers and computer produced records such as:
  - computer systems (as in the Criminal Code)
  - data (as in the Criminal Code); and,
  - original (a separate clause to cover CGRs where each CGR would be considered as "original").
- adding to the current section on authentication by:
  - adding a subsection for establishing authenticity of a CGR via a witness orally or by affidavit,
  - adding a subsection to allow for authentication via affidavit(s) with the possibility of model forms, i.e. one for the data user

and one for the data processor where there are seperate persons, being specified in regulations pursuant to a new Canada Evidence Act;

- with respect to the business records of financial institutions, the addition of a subsection to accept a busines record in a proceeding to which the institution is not a party as evidence unless there is proof to the contrary; and,

- that the same rules should apply for any CGR whether they are business, financial, medical or government.

It was also suggested that in order to ensure an acceptable level of data integrity and trustworthiness, an organization could expand the internal and external audit function to include information as well as financial management. This is in line with the concept of "comprehensive audit". Institutions which are audited in this manner would have little or no difficulty in introducing extracts from computerized databases in court as evidence. Further, it was recommended that there be two types of affidavits; one for the person creating or using the data in question, i.e. data user, and one for the person in charge of the computerized information system, i.e. data processor. [8] Finally, it was agreed that a single data processing standard was an impossibility. However, it might be possible and useful to develop standards for specific and well-defined applications with their own documentable transaction and audit trails. Basically, the most promising area for standards for data appear to be in the area of output devices, especially those for permanent data storage, i.e. updatable but non-erasable optical disk. In this context it is useful to draw attention to the fact that in 1979 a processing standard for microforms technology was developed and approved. Titled "Microform as Documentary Evidence/Microfilm Preuve Litterale", it is a National Standard of Canada (CAN2-72.11-79) and was approved by the Standards Council of Canada.

2.2.3 Access to Information and Privacy Law

Both the Criminal Code and Evidence Acts are examples of laws of general applicability affecting all types of information systems. There are also specific information laws which introduce new legal requirements for

recorded information and information handling. They also tend and try to be technology independent in their application. At present, access to information and privacy legislation in Canada applies only to specified public sector institutions in the federal sector and in certain provinces. Canada, however, has committed itself to encourage the private sector to adhere, on a voluntary basis, to the OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data.

To date, privacy legislation is often regarded by the information professional as an unwarranted intrusion, a negative element, in information systems. This is a misconception. In essence, privacy legislation requires that one keep timely, accurate and relevant personal information only. That this information not be misused, and that it be collected for a specific or defined purpose only and then directly from the individuals concerned who in turn must be given the opportunity to see the same and request correction or deletion where appropriate.

Freedom of information legislation in providing access rights at the same time identifies specific categories of sensitive (or valuable) information which must be protected from unathorized disclosure. Both types of legislation introduce the concept of public accountability for information management by requiring the production of annual indexes and the ability to identify and retrieve specific information quickly. Both acts thus promote good information practices.

2.2.4 Records Retention Requirements

An analysis of all federal records retention requirements on business in Canada in 1982 indicated that of the 76 laws and 111 regulations existing at that time, the vast majority did not allow for such information to be maintained in machine-readable form. This is because the definition of record is basically still one of a hard-copy record. Information professionals in designing integrated information systems to replace paper-based operations especially those in the office would do well to

examine the legal aspects of records retention requirements before undertaking such conversions.

2.2.5 Copyright

One area of information law which has caused considerable debate is the question of copyright as applied to software and, increasingly, data (bases). The debate has suffered from the failure to make a clear distinction between data abuse, i.e., theft of data including sets of instructions, and inadequacies in copyright legislation. The need to protect corporate assets in the form of recorded information (whether data or software) from unauthorized disclosure or theft, i.e., data abuse, should not be confused with the desire to obtain a fair return on investment (real or intellectual). Copyright basically concerns the control of distribution of recorded information, however packaged, which in most cases is already public information. This is the opposite of the concern of the information resources manager who wishes to protect corporate assets or resources in the form of recorded information against any unauthorized disclosure (e.g. by copying) and is not at all interested in distribution or sale of the same.

With respect to copyright, it might therefore be useful to distinguish between proprietary software and data of an organization which it considers to be part of its assets (or "property") and never intends to distribute and software (or data) which is intended for distribution and sale. The former could be covered by the new provisions in the Criminal Code. From an economic perspective, copyright law is a mechanism used to ensure a fair return on investment for those who have invested resources in order to be able to distribute and sell something of value to others. In this context, the Criminal Code protects "property" in the form of "data" and "software" from being misappropriated from its owner who is not interested in its distribution or sale, i.e. does not wish it to be "public". As a matter of fact, the data and software in question may well form the core of the business and provide a competitive advantage (e.g. financial services).

A "data" or "software" publisher is by definition someone who does wish to distribute but needs to be assured of a return on the investment. As such the drafting of new Copyright legislation should take into account remedies which are now already available under the new sections of the Criminal Code on computer crime and data abuse.

3.0 PRACTICAL CONSIDERATIONS

Having introduced and explained the concept of information law and its importance to integrated information systems and identified some key legal issues and recent developments in information law in Canada, this third and last section presents some practical considerations and identifies legal issues yet to be resolved. Their resolution is considered a necessary precondition to the full informatization of the workplace.

3.1 Definition of Record: From Object to Information

The classic definition of recorded information in law is that of a record with records generally being defined as a physical object or artifact on which information is recorded; and, where a unique one-to-one relation exists between the recorded information and the information carrier, which is not reusable, is fixed in time, space and form and is based on concepts such as "original", "duplicate", and "copy".

The major impact of the new information technologies on information law is to shift the emphasis from the physical artifact or information carrier to the information or data itself, i.e., from record to recorded information. From an information handling perspective, it represents a shift from the management of physical objects, or records, to the management of information or data where there is no longer a one-to-one relation between the storage medium and the storage media is even reusable. New legislation such as the amendments to the Criminal Code, proposed amendments to the Anti-Combines Investigation Act, the Bankrupty Act, federal and provincial access to information and privacy legislation, etc. all contain definitions of records, information, and/or data which are technology independent. At the same time, a very large body of law continues to exist where the definition of record is obsolete or irrelevant from the perspective of the new information technologies. The result is that if one moves from a paper-based operation to an integrated information system, one may find that a particular

law no longer applies or that there is confusion on how a law would apply or which laws apply. It could well be that a strict intepretation of a law or regulation prevents one from introducing new, more efficient or cost-effective information technologies. The latter is true especially for existing records retention requirements.

A practical consideration for those with a stake in the information technology area would be to advocate that existing information laws, at whatever level of jurisdiction, be amended so that the definition of "record" or "recorded information" or "data" is made technology independent and uniform. The basic definition could simply be that of "recorded information". If a uniform definition of "recorded information" is not possible, one should ensure that variations in definition are, at the least, compatible with each other. This is of special importance where one integrates several information systems which currently run as separate applications. This could easily result in several information laws applying at the same time to such an integrated information system.

Information law should also allow one to convert between various storage media and information handling technologies with the information law remaining equally applicable. (The current Bank Act has such a provision.)

However, it may well be that when it comes to the application sections in an information law, regulation or code it will be more appropriate and effective to create a special sub-section to address particular aspects of "recorded information" and "information handling" to address a particular type of information technology. The recent amendments to the Criminal Code for "data abuse" provide a good example of this approach.

3.2 Protection of Recorded Information

The increased use of information technologies and the increased recognition of information or data as an asset of value or resource go hand in hand. The acceptance and recognition of information as a resource of value is

reflected in the increasingly widespread use in the public and private sectors alike of concepts such as information resource management (IRM), Information Resources Manager or Information Resources Centre (IRC).

Similarly, the amendments to the Criminal Code on computer crime and data abuse were introduced and enacted because of a strong consensus among the private sector, government and individuals alike that information or data is a valuable resource which requires the same level of protection under law as that for property.

A (very) practical consideration for the information professionals in charge of information systems is that they would be well-advised to develop a clear statement or set of rules of what constitutes authorized and/or unauthorized action with respect to data (and software) and use of their computer systems. While this may be a relatively trivial task for stand-alone applications, developing such an access and use code for integrated information systems is not a trivial task and becomes even more challenging in the emerging area of integrated office information systems.

It is important for an organization and for information professionals to develop such an access and use code with appropriate levels of security protection for integrated information systems (or any EDP application). This is because if an organization finds itself the victim of an alleged computer crime or data abuse and wishes to maximize the possibility of successful prosecution, it has to be able to demonstrate that the activity in question was clearly unauthorized. The information manager, therefore, must ensure that every employee in the organization with access to a computer system or data, or any user, knows exactly which uses of the computer systems and data are authorized, and which are not. In the same vein, those in charge of the acutal information systems must ensure that security features exist for such systems at a level sufficient enough so that there can be no doubt that the computer crime or data abuse was not "accidental".

3.3 Data Integrity

One of the main reasons why many organization are hesitant to fully convert to integrated information systems or the "paperless" office is because key information laws, such as those on evidence, have not been amended to allow for the admissibility of CGRs as evidence. Nor have the numerous records retention requirements been amended to allow businesses to keep such records in electronic form.

The discussions at NCARE made it quite clear, however, that should the Canada Evidence Act be amended to allow for the admissibility of CGRs, there would be a concomitant responsibility on information professionals to be able to demonstrate the trustworthiness and integrity of the data in their systems. As a matter of fact, questions about data integrity and system trustworthiness dominated the NCARE discussion. As such one of the key challenges for the information professional, the information (technology) industry as well as the users, is the establishment of "standards" or practices whereby one can demonstrate data integrity and systems trustworthiness at a level sufficient to allow for the admissibility of CGRs of such systems. In this context, expanding the roles and responsibilities of both internal and external auditors to include auditing for information law compliance might be a practicable and workable solution. Such an audit would include trustworthines, accuracy and reliability of data in systems, security measures, etc. and would be a logical component of the emerging trend towards "comprehensive audits".

A key legal issue which has to be resolved is the role of signatures and authentication in integrated information systems. To date, many of the major systems requiring such features are transaction processing systems. In this area various checks and validation control steps have been developed at a level of detail and rigorous application sufficient to ensure both data integrity and authentication (e.g., the use of an ATM, where the use of the magnetic stripe card and the entry of one's personal identity number (PIN) coupled with contractual obligations effectively serve as an electronic signature).

A key challenge, as well as a legal issue, is that of electronic signature verification for "document"-based information systems. A major factor inhibiting the advent of the paperless office is the need for signatures, which together with other data elements, serve as proof of acceptance or authorization for such documents or specific actions. Even if the evidential question is resolved, this still leaves the problem of signature verification. [9] Recent advances in cryptography and personal identification systems (e.g. fingerprint, retina or voice recognition, PINs, magnetic stripe or holograph cards, etc.) have now made it technically possible and feasible, together with time and date stamping, to establish the authenticity of a paperless or "electronic document". How this is to be implemented in an operational sense and what changes to information law are required to make this a reality especially in "open" systems (as differentiated from "closed" systems such as SWIFT or those involving the use of ATMs) requires more research and work. An added urgency is added here due to the recent rapid rise of Electronic Data Interchange (EDI), i.e. firm-to-firm electronic (or paperless) documentation exchange for purchases, invoices, bills of lading, remittances, etc.

3.4 Electronic Data and Document Storage

One final practical consideration is the question of "permanent" data storage for evidentiary and other legal, operational and archival purposes. For both evidentiary and other legal reasons, private and public sector organizations alike maintain vast volumes of hard-copy records at considerable expense. Microfilm technologies can offer up to 98% savings in physical storage space of recorded information and if done according to the microfilming standard, cited above, will be admissible as evidence. However, microfilm, as a permanent storage device has some basic drawbacks. First of all, the ability to search and retrieve data interactively is lost. Secondly, data on microfilm is not easily reusable without having to be re-entered into a computer system using special processes with the database structure also having to be reconstituted.

One promising technology for permanent data storage is the optical disk whose immense capacity for data storage appears to increase almost daily as new technologies are developed. Updatable but non-erasable optical disk technology coupled with proper authentication and transaction logging techniques appears to be a solution for storing (and retrieving if necessary) the tens of thousands of paperless "documents" of integrated office system (e.g. Write-Once-Read-Many or WORM).

However, here, as in other areas of information technology application, there remain legal issues to be overcome (e.g. the need for a new Evidence Act).

4.0 CONCLUSIONS

Technological and managerial solutions now exist to allow us to move towards integrated information systems and the paperless office. One of the main obstacles to overcome is the need to amend those information laws at the local, national and international levels, which currently inhibit the move to a paperless world yet at the same time maintain the spirit and purpose of such information law.

At the individual level, information professionals would be well-advised to become aware of the requirements of information laws and assess their impact on information systems. Information professionals who fail to take these information law requirements into account in designing and operating integrated information systems do so at their own peril. Not only may they and their organizations find themselves faced with costly retrofits but failure to comply with information law requirements can result in the loss of right, money, adverse consequences in litigation and even criminal penalties and fines.

On a more positive, note a close examination of the functional requirements for integrated information systems arising from compliance with information law are, on the whole, those of good information management practices. It can even be argued that information law compliance will encourage the development of efficient and cost-effective information systems. But that is another story.

FOOTNOTES

1. For an earlier article where the concept of "information law" was introduced consult, Knoppers, Jake V.Th. "Information law and information management". Information Management Review. Vol. 1, no.3 (Winter, 1986) p.63-73.

2. Canadian Information Processing Society (CIPS). Code of Ethics and Standards of Conduct. Toronto: CIPS, January, 1985, 9p.

3. Association of Records Managers and Administrators, Inc. (ARMA). Proceedings and Papers Presented at the National Consultation on Admissibility of Recorded Evidence (NCARE)/Consultation nationale sur la validité de la preuve informatisée (CNVPI). Ottawa, Canada: 28-29 March, 1985. (Hereafter cited as NCARE)

4. Taylor, R.C. "Trends in Data Integrity, Security and Use of Technology". NCARE Background Paper. NCARE, March, 1985, p.13.

5. Brief on Bill S-33, The Canada Evidence Act, 1982. Submitted by the Canadian Legislative and Regulatory Affairs Committee (CLARA) of the Association of Records Managers and Administrators (ARMA) to the Senate Committee on Legal and Constitutional Affairs. Ottawa: 23 June, 1983, pp. 2-3

6. Tollefson, E.A. "Admissibility of Computer-Produced Records: Principles and Problems". NCARE Background Paper. March, 1985, p.4.

7. Tollefson, p.8.

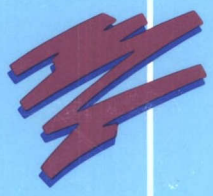
8. Knoppers, Jake V.Th. "Final Follow-Up". NCARE Memo to Participants. 3 July, 1985.

9 Knoppers, Jake V. Th "International Trade: The Information-Intensive Commercial Trends of the Future". Paper presented at the First International Records Management Congress, Manila: 18-22 November, 1985, pp.18-21, Published in International Records Management Journal 3(1) (January, 1987): 21-27 and subsequent three numbers.

7. Tollefson, p.8.

8. Knoppers, Jake V.Th. "Final Follow-Up". NCARE Memo to Participants. 3 July, 1985.

9 Knoppers, Jake V. Th "International Trade: The Information-Intesive Commercial Trends of the Future". Paper presented at the First International Records Management Congress, Manila: 18-22 November, 1985, pp.18-21, Published in International Records Management Journal 3(1) (January, 1987): 21-27 and subsequent three numbers.



Pour plus de détails, veuillez communiquer avec :

Le Centre canadien de recherche sur l'informatisation du travail
1575, boulevard Chomedey
Laval (Québec)
H7V 2X2
(514) 682-3400

For more information, please contact:

Canadian Workplace Automation Research Centre
1575 Chomedey Blvd.
Laval, Quebec
H7V 2X2
(514) 682-3400