THE IMPACT OF THE DIGITAL AGE ON MONEY LAUNDERING INVESTIGATIONS

Daniel P. Murphy *

I. INTRODUCTION

In the film Jerry Mcguire one of the main characters uttered a phrase that popularises the criminal's justification for most profit motivated crimes "SHOW ME THE MONEY". The volume of cash in many criminal activities creates a problem for the criminal and their advisors.

What is we look at currency as nothing more than pieces of paper? Nations stand behind the value represented by the paper but it remains paper. I am not intimately familiar with national or international finances. My knowledge of banking is minimal and personal, rather than professional. On the other hand, my experiences tell me that drug traffickers need to move their currency for a variety of reasons. This gives the State an investigative opportunity. It also provides an opportunity to forfeit a criminal's cash. These are two different issues.

The simple fact is that a dollar bill, or a $20 dollar bill, weighs a gram. The weight of currency in a drug transaction, at the higher levels, is greater than the weight of the drugs. This creates it own security risk. The cash has to be moved around the world. It has to be converted into other currency. Cash should be seen as a business inconvenience.

Cash is an important justification for every currency transaction reporting systems.[1] Canada recently revised and replaced its *Proceeds of Crime (Money Laundering) Act*.[2] That law will cover cash transactions, which occur in a variety of business sectors.[3] The Regulations contain the implementation provisions for this new anti-money regime. In the anti money laundering environment the regulation of the financial sector is more than a means to test a financial institution's institutional stability or its "know your customer" policies.

Canada's new law and its ancillary regulatory package will establish some cash transaction reporting requirements in Canada. Essentially, transaction reporting will be triggered by proscribed amounts of cash, deposited or involved in a transaction. In addition, Part 11 of the Act will establish a regime to gather information concerning the cross border movement of cash and monetary instruments.[4] The provisions in the regulatory package will eventually evolve beyond concerns on paper currency

* Senior Counsel, Strategic Prosecution, Policy Section, Justice Canada, Canada

1 FINCEN recently released *A Survey of Electronic Cash, Electronic Banking and Internet Gambling*, an excellent review of the field. http://www.ustreas.gov/fincen/e-cash.pdf

2 S.C. 2000, C. 17

3 Section 6 specifies that persons subject to the Act will keep and maintain records. The Act improves upon and replaces the previous *Proceeds of Crime (money laundering) Act* and *Regulations*. Statutes of Canada 1991,c.26, in R.S.C 1985, C. P-24.5 as amended. (see http://canada2.justice.gc.ca/en/laws/P-24.5/79312.html)

4 Section12 specifies that the part will deal with currency or monetary instruments greater than a proscribed amount.

and address the new world of digital cash.

This law depends upon currency transaction reporting and the ancillary financial institution record keeping requirements. It will include emerging issues as they impact on the money laundering issue. In fact, three emerging issues have developed and each connects to the emerging digital age. These are:

(i) The issue of personal information protection in the digital age.
(ii) The issue of an investigator's capacity to capture digital communications, and
(iii) The ability for individual's to move and conceal digital information.

Consider this last issue, for a minute. A letter or a fraudulent receipt can be used to acquire money. Good documentary evidence is the essence of a financial crime investigation. Investigators will look under the bed; search file cabinets and continually seize the paper. After all it is the best evidence. In the last decade the search for documents has been frustrated by the evolution of the digital age. You now need to search computers yet the Internet and data safe havens can easily convert a personal computer into an expensive paperweight. The State's ability to search the Internet and seize Internet communications is a common concern for all nations. It is also new territory.

Unfortunately, this territory ignores national borders yet national laws depend upon borders. In this paper I will attempt to raise some issues with respect to the three emerging issues set out above.

How does the digital revolution impact on the investigative imperatives of the modern world? That is a question everyone must ask since the entire world has jumped into a digital whirlpool. This is especially important in an era the individuals response is to demand that states enact laws to protect individual privacy.

II. PERSONAL PRIVACY PROTECTION

Hollywood movies suggest that nothing is secure from the intrepid Internet search engine and a sophisticated digital detective.[5] Canada's Constitution includes a *Charter of Rights and Freedoms*, which impacts upon the ability of the state to search and seize information which includes a reasonable expectation of privacy exists.

In a 1993 case, *R. v. Plant*,[6] the Supreme Court of Canada held that Canada's s. 8 *Charter* protected a biographical core of personal information maintained by a commercial enterprise, in certain scenarios. In *Plant* the police obtained hydro consumption records from a city utility company without a search warrant. Justice Sopinka, for the majority, opined that the Charter protected a biographical core of personal information from the State. He opined as follows:

> "The United States Supreme Court has limited application of the Fourth Amendment (the right against unreasonable search and seizure)

[5] Coincidentally, as I was finishing this brief paper my local newspaper arrived with an insert magazine called *Backbone*-Premier issue. It contained a short article by Sheldon Gordon, *Diary of a Digital Detective*. The article described a fictional denial of service attack against a Canadian on-line grocery service business. I suspect that a future article could be on how a person can access personal information from any computer. The issue is that computers make our lives easier while they risk our privacy.

[6] http://www.canlii.org/ca/cas/scc/1993/1993scc96.htm

protection afforded by the United States Constitution to situations in which the information sought by state authorities is personal and confidential in nature: *United States v. Miller*, 425 U.S. 435 (1976). That case determined that the accused's cheques, subpoenaed for evidence from a commercial bank, were not subject to Fourth Amendment protection. While I do not wish to be taken as adopting the position that commercial records such as cancelled cheques are not subject to s. 8 protection, I do agree with that aspect of the *Miller* decision which would suggest that in order for constitutional protection to be extended, the information seized must be of a "personal and confidential" nature. In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual. The computer records investigated in the case at bar while revealing the pattern of electricity consumption in the residence cannot reasonably be said to reveal intimate details of the appellant's life since electricity consumption reveals very little about the personal lifestyle or private decisions of the occupant of the residence. "

Commercial businesses, including financial institutions, collect a significant amount of personal information on their customers. Traditional businesses obtained personal information, via paper transaction or otherwise. They obtained that information for their credit files: customer preference files: and other reasons. E Business obtains the same information electronically. They could also capture essential information the moment that an individual accessed the business's web site. Frequently, an Internet business includes a specific privacy policy. Individuals had an opportunity to acknowledge that they have read and agreed to the site's privacy policy. I often wonder who takes the time to read those privacy statements and policies.

The result is that individuals have grown concerned with the Wild West type of privacy infringement, which they perceive exists in the commercial world. Nations have responded to this perception. Type in Information Privacy on an Internet search engine and you access thousands of hits.[7] You could also immediately access the Council of Europe's Directive 95/46.[8] You will quickly note a significant movement to protect the "data subject's" (i.e. a Counsel of Europe expression) privacy. Their Directive specifically requires that third countries receiving data adopt an adequate level of protection for personal information.

III. CANADA'S LEGISLATED RESPONSE TO PERSONAL INFORMATION

Canada recently enacted its *Personal Information Protection and Electronic Documents Act*.[9] Part 1 of this law (which I will describe as the PIPED Act) establishes a right of protection for personal information collected, used or

[7] One interesting site I discovered was Privacy and the Information Highway, by Ian Lawson at http://strategis.ic.gc.ca/SSG/ca01021e.html

[8] http://www.privacy.org/pi/intl_orgs/ec/eudp.html and save a lot of time.

disclosed in the course of commercial activities. It establishes principles to govern the collection, use and disclosure of personal information. The accuracy of any records holding personal information is a significant issue of concern in the *PIPED Act*. It also requires businesses to provide adequate security for records containing personal information. It requires business to make information management policies readily available. In addition, business was required to provide individuals with access to information about themselves. It further provides that a Privacy Commissioner could receive complaints concerning contraventions of the Act's principles; conduct investigations; and attempt to resolve such complaints. Unresolved disputes relating to certain matters can be taken to the Federal Court for resolution.

A. Some Details on the Act

The *PIPED Act* came into force on January 1, 2001. It specifically covers banks; other federally regulated financial institutions; and other federal business organizations. Transitional provisions provide that all other Canadian businesses will become subject to that law within three years. This law controls the business collection of personal information and the subsequent use and disclosure of such information. The *PIPED Act* will have a significant impact on how a business uses the personal information it collects. It will also have an impact upon investigations since it applies the concept of personal information protection and access, in a manner that is similar Canada's *Privacy Act*.[10]

B. Business Records Impact

The *PIPED Act* establishes two results that have yet to be fully appreciated. The first impacts upon businesses. Every business must convert their record keeping systems into a personal information retrieval system. Their customers have a right to access all their personal information held by the business.[11] That business must assist the individual in preparing the access request, if necessary. In addition, the "organization"[12] must respond to an individuals access request with due diligence and in any case not later than thirty days after receipt of the request.[13]

The business must insure that their records are accessible. In addition, they had better insure that the personal information they collect, use and disclose is accurate; used in the manner intended; and properly disclosed.[14] The individual, in addition to their right to access their personal information, has a right to complain to the Privacy Commissioner. The Commissioner has the statutory right

[9] S.C. 2000 c. 5, http://canada.justice.gc.ca/en/laws/ann_stat.html

[10] R.S.C. 1985, c. P.21, as amended.

[11] *PIPED Act*, Section 8 allows individuals to submit written requests for access to a business

[12] *PIPED Act*, Subsection 2 defines an "organization" to include an association, a partnership, a person and a trade union. Section 4 then provides that the Act applies to any "organizations" that collects personal information. Section 2 defines personal information to mean "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization". Finally, since personal information is contained in records, section 2 defines records, in an expansive definition, to include any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of any of those things.

[13] *PIPED Act*, subsection 8(3).

[14] *PIPED Act*, section 7 controls the collection use and disclosure of personal information.

to investigate the individuals complaint and take the matter to Court.[15] Finally, the court has the power to remedy the complaint Section 16 of the *PIPED Act* allows the court to:

(a) order an organization to correct its practices in order to comply with sections 5 to 10;
(b) order an organization to publish a notice of any action taken or proposed to be taken to correct its practices, whether or not ordered to correct them under paragraph (a); and
(c) award damages to the complainant, including damages for any humiliation that the complainant has suffered.

There have not been any decisions, to date, since the Act came into force at the beginning of 2001.

Current reality, vis-à-vis business records, is that individuals have a very difficult challenge obtaining access. Law enforcement has a similar challenge. In light of the *Charier*, and the courts ability to determine that personal information accessed from a commercial enterprise goes to the biographical core of information deserving of protection, the police are always well advised to access business information under the authority of a warrant. The problem is that the records are not readily available. Frequently the police wait, in sufferance, while the required record is retrieved. The law will, over time, compel organizations to shift their record-keeping paradigm toward accessibility. Accessibility by law enforcement will be improved.

[15] Sections 12 to 15.

C. Impact on the Police

I indicated that there were two unexpected impacts as a result of the *PIPED Act*. The Act controls how business discloses personal information they retained. If law enforcement obtains access to personal information held by a business, they may have to disclose that fact if the person asks for instances where their information is used. This will have an unexpected impact upon law enforcement. The essence of the *PIPED Act* is that individuals should have the right to know the use and disclosure activities of any business that retained their information. Organizations are required, under the *PIPED Act*, to advise their customers, upon a request from the customer, with respect to any business use of personal information. Subsection 7 (c); (c.1); (d); and (e) authorise disclosure without consent.[16] The individual, however, retains the right to access their personal information record in the organization and determine if the organization has made any disclosures under the authority of subsections7 (3)(c) to (e).

This means that a police investigative interest, even if the police used a warrant that authorised a surreptitious disclosure,

[16] The relevant sections read as follows:

(c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;

(c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that

(i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,

(ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an

should be disclosed to a requesting individual. Indeed, any competent criminal or criminal organization, might, as a matter of routine, file *PIPED Act* section 8 requests to determine if the organization has disclosed to authorities. This can be equated to an early warning mechanism for interested individuals.

The *PIPED Act* responded to this possibility by allowing the organization to notify the authorities about an access request and delay access pending a decision, by the authorities to object.[17] I will not set out the specific provisions but the result is that law enforcement must create some type of system to respond to a business's notification about access requests. If the deadline to object passes without an objection from the relevant authority the business must tell the person who made the request about the earlier disclosure to law enforcement.

D. Suspicious Transaction Reporting

There is one other aspect to the *PIPED Act*. It contemplates consent disclosure, informed consent and a confirmation of the fact of a disclosure to law enforcement. Recall however, that Canada's new *Proceeds of Crime (Money Laundering) Act* create a suspicious transaction reporting requirement and a new tipping off offence.[18] Section 97 of that *Proceeds of Crime (Money laundering) Act* includes conditional and consequential amendment to the *PIPED Act*. It adds a subsection 7(3) and 9(2.1)(a)(I), (2.3) and (2.4)(c)(I) to specifically cover suspicious transaction reporting.

IV. THE GROWTH OF INTERNET COMMUNICATIONS AND CYBERCRIME

There is a phenomenal amount of literature on the Web concerning the growth of cybercrime. The United States' National Information Infrastructure Protection Act of 1996[19] illustrates how significant a problem this is for one jurisdiction. At the 10th United Nations Conference on Prevention of Crime and Treatment of Offenders' Computer Crime Workshop, last April, the Attorney General of Canada summarised the problem created by the Internet and the personal computer in a few words. The Attorney General advised the group that:

Computer networks, and the Internet, in particular, have managed to shrink our

investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or

(iii) the disclosure is requested for the purpose of administering any law of Canada or a province;

(d) made on the initiative of the organization to an investigative body, a government institution or a part of a government institution and the organization

(i) has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or

(ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;

(e) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure;

[17] *PIPED Act*, subsection 9(21.) to 9 (2.4).

[18] S.C., 2000, C. 17. Section 8 creates an offence to disclosure that a suspicious transaction report has been made.

[19] 18 U.S.C. 1830 http://www.cybercrime.gov/1030_new.html

vast world. Today's technology allows us to share information with people in other countries, and on other continents with minimal expense.

With the internet the possibility now exists for people all over the world to have access to the stores of knowledge and products and services that were once only accessible by a very few. This possibility has provided new opportunities to draw the world together. The emergence of e-commerce is allowing small businesses around the world to compete with their larger competitors.

But, the Internet has also created corresponding opportunities for criminals. Like everyone else, criminals have embraced high technology to further their goals. We are becoming increasingly aware of the threats posed by the Internet. Hate literature and child pornography can be disseminated easily. Even traditional crimes such as fraud and forgery can now be committed with the Internet.

In October 1999, the G8 Ministers of Justice and the Interior adopted a set of principles on transborder access to stored computer data. The principles cover many issues relevant to computer evidence; including, the secure rapid preservation of data, and transborder access to data through expedited mutual assistance, and in some cases direct transborder access in cases of public internet sites or with consent of an authorized user.

On March 28, 2000 F.B.I. Director Louis Freeh made a statement on the Record before the United States' Senate Committee on Judiciary.[20] The Director analysed the problems created by the cybercrime phenomenon. I can not improve upon his excellent overview and recommend the statement for anyone seeking a general description of the issues. I can only add that nations must consider this problem or recognize the reality that their borders and sovereign interests are completely artificial.

Concomitantly to the 10th United nations Convention; the work of the Ministers of Justice and Interior and the efforts in the United States, the Council of Europe, over the last three years, has been negotiating a draft Convention on Cyber-crime, which will be open to signature to all of its members and to non-member states.

The purpose of the Convention is "to deter actions directed against the confidentiality, integrity and availability of computer systems, networks and computer data, as well as the misuse of such systems, networks and data, by providing for the criminalisation of such conduct, as described in the Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating the detection, investigation and prosecution of such criminal offences at both the domestic and international level, and by providing arrangements for fast and reliable international co-operation."[21]

In particular, the Convention has four major components:

(1.) Requiring State Parties to criminalise certain forms of abuse against computer systems (i.e., illegal access, illegal interception of communications, data interference, system interference and misuses of hacking and virus

[20] http://www.fbi.gov/pressrm/congress/congress00/cyber032800.htm

[21] The most recent public draft of this convention, i.e. version 25, can be accessed at: http://conventions.coe.int/treaty/EN/projets/cybercrime25.htm

programs and devices) and certain forms of crimes committed through the use of computer systems (i.e., forgery, fraud, production/distribution/possession of child pornography, and infringement of copyright as defined under national law pursuant to fulfilling obligations under a number of specific copyright treaties).

(2.) Requiring State Parties to enact, or take such other measures as are necessary, to ensure that various enforcement powers can be exercised by law enforcement authorities for the purpose of criminal investigations or proceedings (i.e., orders for the preservation of specific computer data pending its acquisition by legal measures, search and seizure of computer data, orders for the production of computer data, collection of traffic data, interception of communications) in relation to Convention offences, any other criminal offence committed by means of a computer system and evidence in electronic form of any criminal offence.

(3.) Requiring State Parties to adopt legislative and other measures to establish jurisdiction over the Convention offences when the offence is committed: in its territory; on board a ship or airline registered under the law of that Party; or by one of its nationals if the conduct is a criminal offence where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

(4.) Requiring State Parties to provide, to the widest extent possible, each other co-operation in the investigation and prosecution of Convention offences and any offence in respect of which evidence is in electronic form (e.g., mutual legal assistance, extradition). State Parties are entitled to use the Convention to supplement any existing treaties among them or where there are no existing treaties or other arrangements.

The cybercrime issue can become overly focused on how Internet communications occur. The environment changes faster than the law. This means that it is difficult to stay in front of the communications. Essentially this becomes an interception issue.

V. INTERCEPTION ISSUES

The interception of private communications, as an investigative technique, varies around the world. Some countries do not have any specific laws controlling this technique. Others have a law that permits investigators to use wiretaps provided they do so for intelligence purposes.[22] Canada, and other countries, legislated specific laws and use wiretaps to gather evidence that is used in prosecutions.[23] The Canadian interception law was found to be an acceptable procedure under Canada's *Charter of Rights and Freedoms*. From the Canadian perspective, the parties involved in a targeted communication have a reasonable expectation of privacy and a judicial authorization is required before the interception occurs if the State intends to use the interception as evidence.

[22] The United Kingdom's Regulation of Investigatory Powers Act.

[23] In Canada Part VI of the Criminal Code, for criminal evidence purposes and the Canadian Security Intelligence Services Act, for national security purposes.

Considering the person's expectation of privacy, there is minimal difference between phone communications and communications involving the Internet. Part VI authorizations are obtained by the police to intercept e-mail and other Internet communications while they are in transit. In the United States Title III was influenced by *Berger v. New York*[24] and *Katz v. U.S.*[25] Canadian wiretap law should apply the same analysis. They are as concerned with the need to control the threat posed to individual privacy by indiscriminate police use of wiretapping.

The American and Canadian wiretap legislation were drafted very broadly in order to regulate and control the technological invasive of privacy. Legislative amendments have also been made to keep pace with new police investigative techniques and technology that were not contemplated by the initial enactments. In Canada warrants in relation to videotaping, digital number recorders, tracking devices and cell phones were added to the *Criminal Code.*

The United States Supreme Court has described and outlined the history of the formation of the Internet:[26]

> [para25] The Internet is an international network of interconnected computers. It is the outgrowth of what began in 1969 as a military programme called "ARPANET," which was designed to enable computers operated by the military, defense contractors, and universities conducting defense-related research to communicate with one another by redundant channels even if some portions of the network were damaged in a war. While the ARPANET no longer exists, it provided an example for the development of a number of civilian networks that, eventually linking with each other, now enable tens of millions of people to communicate with one another and to access vast amounts of information from around the world. The Internet is "a unique and wholly new medium of world-wide human communication."
>
> [para26] The Internet has experienced "extraordinary growth." The number of "host" computers - those that store information and relay communications-increased from about 300 in 1981 to approximately 9,400,000 by the time of the trial in 1996. Roughly 60% of these hosts are located in the United States. About 40 million people used the Internet at the time of trial, a number that is expected to mushroom to 200 million by 1999.

The Reno court opined on the extra territorial nature of the Internet as a medium of communications:

> [para28] Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categorize precisely. But, as presently constituted, those most relevant to this case are electronic mail ("e-mail"), automatic mailing list services ("mail exploders," sometimes referred to as "listservs"), "newsgroups," "chat rooms," and the "World Wide Web." All of these

[24] Berger v. New York 388 U.S. 41 (1967)

[25] Katz v. U.S. 389 U.S. 347 (1967)

[26] Reno, Attorney General O v. American Civil Liberties Union (06/26/1997), From *Wiretapping and Other Electronic Surveillance*, By Hubbard, Brauti and Fenton, Canada law Book

methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium-known to its users as "cyberspace" - located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet. (Emphasis added)

[para29] E-mail enables an individual to send an electronic message-generally akin to a note or letter to another individual or to a group of addressees. The message is generally stored electronically, sometimes waiting for the recipient to check her "mailbox" and sometimes making its receipt known through some type of prompt. A mail exploder is a sort of e-mail group. Subscribers can send messages to a common e-mail address, which then forwards the message to the group's other subscribers. Newsgroups also serve groups of regular participants, but these postings may be read by others as well. There are thousands of such groups, each serving to foster an exchange of information or opinion on a particular topic running the gamut from, say, the music of Wagner to Balkan politics to AIDS prevention to the Chicago Bulls. About 100,000 new messages are posted every day. In most newsgroups, postings are automatically purged at regular intervals. In addition to posting a message that can be read later, two or more individuals wishing to communicate more immediately can enter a chat room to engage in real-time dialogue-in other words, by typing messages to one another that appear almost immediately on the others' computer screens. ... It is "no exaggeration to conclude that the content on the Internet is as diverse as human thought."

[para30] The best known category of communication over the Internet is the World Wide Web, which allows users to search for and retrieve information stored in remote computers, as well as, in some cases, to communicate back to designated sites. In concrete terms, the Web consists of a vast number of documents stored in different computers all over the world. Some of these documents are simply files containing information. However, more elaborate documents, commonly known as Web "pages," are also prevalent. Each has its own address-"rather like a telephone number."

[para31] Navigating the Web is relatively straightforward. A user may either type the address of a known page or enter one or more keywords into a commercial "search engine" in an effort to locate sites on a subject of interest. A particular Web page may contain the information sought by the "surfer," or, through its links, it may be an avenue to other documents located anywhere on the Internet. Users generally explore a given Web page, or move to another, by clicking a computer "mouse" on one of the page's icons or links. Access to most Web pages is freely available, but some allow access only to those who have purchased the right from a commercial provider. The Web is thus comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services.

The United States' Electronic Communications Privacy Act (ECPA) of 1986 attempted to update the wiretap statute by prohibiting the unlawful access, use and disclosure of electronic communications. The intent was interpreted to exclude stored electronic message, once the intended recipient opened the messages.[27] Other cases adopted a more restrictive interpretation of the law.[28]

VI. CANADA'S APPROACH

The *Criminal Code's* search provisions were amended to provide for a search warrant to be used to search computers. The regular warrant provision contained in s.487 of the Code was amended to afford broad latitude to the police to conduct searches of computers without complying with Part VI. Section 487 specifically deals with computer searches as follows:

> (2.1) A person authorized under this section to search a computer system in a building or place for data may
> (a) use or cause to be used any computer system at the building or place to search any data contained in or available to the computer system;
> (b) reproduce or cause to be reproduced any data in the form of a print-out or other intelligible output;
> (c) seize the print-out or other output for examination or copying; and
> (d) use or cause to be used any copying equipment at the place to make copies of the data.
>
> (2.2) Every person who is in possession or control of any building or place in respect of which a search is carried out under this section shall, on presentation of the warrant, permit the person carrying out the search
> (a) to use or cause to be used any computer system at the building or place in order to search any data contained in or available to the computer system for data that the person is authorized by this section to search for;
> (b) to obtain a hard copy of the data and to seize it; and
> (c) to use or cause to be used any copying equipment at the place to make copies of the data.

It seems self evident that a search warrant, rather that a Part VI authorization, is the appropriate order to search a computer. The problem is that an interception or a search, which ever the order required in the circumstances, depends upon laws that are limited to the territory of the state.

---

[27] *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir., 1994)

[28] *United States v. Smith*, 155 F.3d 1051, 98 Cal. (9th Cir., 1998) In Canada, *R. v. McQueen* (1975), 25 C.C.C. (2d) 262 at 265 (Alta. C.A.) the court interpreted the word intercept contained in s.183. The court stated:

> In interpreting new legislation, a good starting place is to consider the dictionary definition of words used. The Shorter Oxford English Dictionary, 3rd ed., defines:
>
> > Intercept 1. trans. To seize, catch, or carry off on the way from one place to another; to cut off from the destination aimed at -- 1548. b. To stop the natural course of (light, heat, etc.); to cut off (light) from anything 1945. c. *To interrupt* -- 1759. d. *To check, cut off (passage or motion) from one place to another* 1596. 2. To prevent, check, stop, hinder 1576. 3. To mark off or include (a certain space) between two points or lines; hence, to contain, enclose. 4. To cut off (one thing) from another, or (ellipt.) from sight, access, etc. 1662.
>
> In, at least, its primary sense the word intercept suggests that there must be an interference between the place of origination and the place of destination of the communication. If Parliament intended the word intercept to be used in this primary sense, then there was no interception here.

A Canadian search warrant or authorization has no effect outside Canada. Conversely a foreign search warrant or intercept authorization is ineffective in Canada. Mutual legal assistance provisions are available to assist another state. Canada has enacted *the Mutual Assistance in Criminal Matters Act* to use in various requests under relevant Treaties and Conventions. S. 10 of the Act permits a foreign country to request Canadian authorities to obtain a search authorization on their behalf in Canada. The section provides:

> 10. The Criminal Code, other than section 487.1 (telewarrants) thereof, applies, with such modifications as the circumstances require, in respect of a search or a seizure pursuant to this Act, except where that Act is inconsistent with this Act.

Part VI of the *Criminal Code* specifically limits authorizations to specifically listed offences. A foreign MLAT request seeks evidence that assists a foreign offence. Therefore a wiretap authorization is not available under the mutual assistance law. It is inconsistent with the Mutual Legal Assistance Act. The Council of Europe's draft Cybercrime Convention illustrates the problem when digital traffic moves across jurisdictions.

It is clear that nations must co-operate if they are every able to respond to Internet crimes. Additionally, the interception of private communications is hamstrung due to shifting technology. Interceptions now occur at the carrier's switch. As global communications and world trade agreements develop, switches are not always located in the country where a targeted private communication occurs. If the place of interception is a switch the locale of the switch may require that the local interception law must be used to authorize the interception. This raises an interesting question if the offence under investigation prevents the issuance of an authorization. Again, this illustrates that nations must co-operate to address crime in the digital age.

VII. CONCLUSION

Individuals around the world perceive that the digital age minimises privacy to the altar of technological convenience. In Canada, this has led to enhanced privacy obligations for businesses. These provisions have unexpected impact on the police and the business community. The Internet is the latest tool for investigators and criminals.

The ability to investigate this communication medium is something that will challenge law enforcement for the foreseeable future. Equally significant, the territorially limitations of domestic wiretap laws significantly limits law enforcement. Nations will have to respond to these issues or admit that the 21st century creates an unregulated communication environment.