# UIC John Marshall Journal of Information Technology & Privacy Law

Volume 10 Issue 4 *Computer/Law Journal - Winter 1990* 

Article 2

Winter 1990

# Hardware and Software Protection in Canada, 10 Computer L.J. 483 (1990)

George E. Fisk

Jane E. Clark

Follow this and additional works at: https://repository.law.uic.edu/jitpl

Part of the Computer Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

# **Recommended Citation**

George E. Fisk & Jane E. Clark, Hardware and Software Protection in Canada, 10 Computer L.J. 483 (1990)

https://repository.law.uic.edu/jitpl/vol10/iss4/2

This Article is brought to you for free and open access by UIC Law Open Access Repository. It has been accepted for inclusion in UIC John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of UIC Law Open Access Repository. For more information, please contact repository@jmls.edu.

# HARDWARE AND SOFTWARE PROTECTION IN CANADA

# GEORGE E. FISK & JANE E. CLARK\*

# I. INTRODUCTION

This paper<sup>1</sup> discusses the present state of Canadian Law relating to intellectual property protection for computer hardware and software. The topics considered include copyright, patents, trade secrets, criminal law and chip protection. One area of the law of evidence, a type of order known as an Anton Piller Order,<sup>2</sup> is also covered in detail, as this order is very useful in computer copyright cases.

As many of the persons attending this conference are Americans, I have tried to highlight, at the beginning of each section of the paper, a few of the major differences between Canadian and United States law on each general topic discussed. This will give our U.S. visitors some feeling of the similarity and differences between Canadian and U.S. law, and provide a context into which the computer law concepts can be placed.

# II. COPYRIGHT

#### A. GENERAL OVERVIEW OF COPYRIGHT

Canadian copyright law arises from the Canadian Copyright Act.<sup>3</sup> There is no common law copyright in Canada.<sup>4</sup> Common law principles are applied by the courts in deciding between possible remedies, but such things as the subject matter of copyright and what constitutes infringement are purely statutory.

<sup>\*</sup> Copyright 1990, George E. Fisk, Partner, and Jane E. Clark, Associate, Gowling, Strathy & Henderson, Ottawa, Canada K1N 8S3.

<sup>1.</sup> This is the text of an address by George Fisk given at the spring Joint Meeting of the Washington, Oregon and British Columbia Patent Law Associations in Vancouver, British Columbia on March 31, 1990.

<sup>2.</sup> The Anton Piller Order is a concept discussed in detail in Section VII of this paper.

<sup>3.</sup> Copyright Act, R.S.C. 1985, ch. C-42.

<sup>4.</sup> For a discussion of the early cases see Fisk, The Protection of Computer Software in Canada — The View as of September 1985, 2 CAN. INTELL. PROP. REV. 176 (1986).

The Canadian copyright law was originally based on the British Imperial Copyright Act of 1911.<sup>5</sup> Until 1976, U.S. and Canadian copyright law were quite different. However, with the new U.S. copyright law of 1976,<sup>6</sup> U.S. law became more like Canadian law.

Canada has a voluntary registration system for copyrights. It is not necessary to register before suing, although there is some advantage to registering because the registration grants certain presumptions which may shift the burden of proof in a lawsuit.<sup>7</sup> Unlike the U.S. system, a copy of the work is not filed when the work is registered. All that is filed is a form that gives some basic information, such as the title of the work, its date and place of the first publication, its owner and its author.

#### B. THE PROTECTION OF COMPUTER PROGRAMS BY COPYRIGHT

Until 1987, there was no provision in the Copyright Act which related specifically to computer programs. The case law therefore developed based on general principles of copyright. Initially, there were several cases where default judgments, interlocutory injunctions, or Anton Piller orders were obtained. In most of these cases, the court did not inquire as to whether copyright subsisted in computer programs, but rather assumed that it did.

There were several early interlocutory cases, however, where the Court did issue reasons why computer programs should receive copyright protection. Very short reasons were issued by the Ontario High Court in Spacefile Ltd. v. Smart Computing Systems Ltd.<sup>8</sup> More detailed reasons were issued by the Federal Court of Canada in *IBM v. Spirales Computer Inc.*<sup>9</sup> and the Quebec Superior Court and Court of Appeal in *RDG Inc. v. Dynabec Ltd.*<sup>10</sup> In each of these cases, the Court held that a computer program was a literary work.

The law in Canada was further established by the case of Apple Computer Inc. v. Mackintosh Computers Ltd.<sup>11</sup> (the "Canadian Apple" case). On the trial level, the judge ruled strongly in favour of software copyright, as he had in IBM v. Spirales.

A few days after the trial decision in the Canadian Apple case an Australian decision caused consternation among computer law practitioners in Commonwealth countries. The Australian High Court, by a

<sup>5. 1 &</sup>amp; 2 Geo. 5, ch. 46 (1911).

<sup>6.</sup> Copyright Act of 1976, Pub. L. No. 94-553, 90 Stat. 2541 (codified as amended 17 U.S.C. §§ 101 to 801 (1988)).

<sup>7.</sup> Copyright Act, R.S.C. 1985, ch. C-42, § 53.

<sup>8. 75</sup> C.P.R. (2d) 281 (1983).

<sup>9. 80</sup> C.P.R. (2d) 187 (1984).

<sup>10. 6</sup> C.P.R. (3d) 299 (1985).

<sup>11. 10</sup> C.P.R. (3d) 1 (F.C.T.D. 1986); aff'd, 18 C.P.R. (3d) 119 (F.C.A. 1987).

majority of 3 to 2, decided the case of Computer Edge Pty. v. Apple Computer Inc.<sup>12</sup> (the "Australian Apple" case). The Court held copyright did not exist in precisely the same programs that were held to be preceded in the Canadian Apple case. This was of particular concern to Canadian lawyers because the Australian Copyright Act also follows the wording of the British copyright statute. The Australian Copyright Act, however, is based on a more recent British statute than the 1911 Imperial Copyright Act from which Canada took its wording, and there are some significant differences in the two statutes.

The Canadian *Apple* case was appealed to the Federal Court of Appeal, and ultimately the Supreme Court of Canada. Both Courts considered and rejected the Australian decision. Instead, they affirmed the trial judge's conclusions with varied reasons.

The trial judge held copyright protection could be based on three grounds set out in Section 3 of the Copyright Act: reproduction, translation, or a contrivance. In the Court of Appeal, Hugessen and Mahoney, JJ., held the programs were reproductions rather than translations. MacGuigan, J., held they were either translations or reproductions. Only Hugessen, J., addressed the "contrivance" ground; he thought the programs were not contrivances.

The Supreme Court of Canada, praising the trial judge's reasons, held the programs were protected as reproductions. The Court found it unnecessary to go any further.<sup>13</sup>

The Australian Apple decision was reversed by a statutory change to the Australian Copyright Law.<sup>14</sup> Even though the Canadian Apple decision was sustained by the Supreme Court of Canada, Canada also amended its law so that computer programs would be protected specifically.<sup>15</sup>

#### C. THE STATUTORY AMENDMENTS OF 1987

The amendments to the Canadian Copyright Act,<sup>16</sup> which took ef-

- 15. Copyright Act Amendments, R.S.C. 1985, 4th Supp., ch. 10, §§ 1-5 (1989).
- 16. R.S.C. 1985, 4th Supp., ch. 10, § 24 (1989).

<sup>12. 65</sup> A.L.R. 33 (1986).

<sup>13.</sup> Apple Computer Inc. v. Mackintosh Computers Ltd., Nos. 20643, 20644 (S.C.C. June 21, 1990). The Court agreed with the trial judge and held copyright protection existed for the programs embedded in the silicon chip because they were reproductions of the programs in assembly language and as such protected under section 3(1) of the Copyright Act. The Court further agreed there was no merger of idea and expression in the programs. The Court found it was unnecessary to decide if silicon chips could also be regarded as a translation under section 3(1)(a) or a contrivance under section 3(1)(d) of the Copyright Act as the trial judge had done since the Court had held the programs were protected as reproductions.

<sup>14.</sup> Copyright Amendment Act, AUSTL. ACTS P., Vol. 1, Act 43 (1984).

fect in 1987, define computer programs as literary works. A "computer program" is defined as "a set of instructions or statements, expressed, fixed, embodied or stored in any manner, that is to be used directly or indirectly in a computer in order to bring about a specific result ....."<sup>17</sup>

The amendments also provide certain statutory exceptions to infringement.<sup>18</sup> The exceptions permit a person who owns an authorized copy of the computer program to make a single modified copy of the program to make it compatible with his own computer, or to make a single copy of either the original or a modified copy for the purpose of backup. These statutory provisions are somewhat similar to provisions often found in license agreements about the making of backup copies.

Therefore, barring some completely unexpected interpretation of the 1987 amendments by a Court, copyright exits in computer programs in Canada. Canada is a signatory of the Berne and Universal Copyright Conventions, so copyright exists in Canada in works which would be protected under those conventions.

Having settled the basic problem of protection, Canada is now just beginning to deal with the second generation problems. Questions of "look and feel," "structure, sequence, and organization" and the extent to which microcode can be protected have not been addressed by any Canadian court in a reasoned decision. There have been interlocutory injunction cases which addressed one or other of these questions.<sup>19</sup> However, these injunction cases are primarily concerned with the existence of an arguable case, and do not purport to decide the law on the matter.

When there are no Canadian cases on point, Canadian judges usually look to the law of other courts within the British Commonwealth. This is particularly the case in copyright matters, as many of our copyright principles were derived from British law. However, the second generation questions have not been finally decided in any Commonwealth case. Under these circumstances, the Canadian Courts may look at U.S. law, to see whether it is persuasive. However, these three second generation doctrines are still in the process of being defined in the United States, so no authoritative answer can as yet be obtained from that direction.

One other potential problem with Canadian Copyright law arises

<sup>17.</sup> Id. § 1 (3).

<sup>18.</sup> Copyright Act Amendments, *supra*, note 15, at § 5. These sections appear in the unofficial consolidation of the Copyright Act produced by the Department of Communications as Section 27 (4) (1)(m).

<sup>19.</sup> See, e.g., Gemologists International Inc. v. Gem Scan International Inc., 9 C.P.R. (3d) 256, appeal denied, 10 C.P.R. (3d) 431 (Ont. H.C.J. 1986); Solartronix v. CEGEP de Jonquiere, 22 C.I.P.R. 101 (Que. S.C. 1988); Les Fourgons Transit Inc. v. Les Fourgons Ramco Inc., 26 C.P.R. (3d) 565 (Que. S.C. 1989).

from the concept of fixation. Although fixation is not required by the Copyright Act in order for a work to exist, case law has held that a work must exist in some material or tangible form before it can be protected.<sup>20</sup> As computer memories become larger and more reliable, it may occur that computer programs will be written directly into memory, without any hard copy being made. If this is the case, it may be necessary to consider whether fixation is really a necessary requirement for protection, and whether the holding of a work in the active memory of a computer can be considered as fixation.

# D. DATABASES

The collection of data and its use or sale is of course not new. Any written record is a collection of data. Even very large collections of data were quite common before the computer. For example, an encyclopedia, a telephone directory, and a set of legal reports are all large collections of data in written form. However, the computer has made large collections of data much more common, more accessible, and more easily copied.

The problem of fixation is likely to be important in the case of databases. Rapidly changing databases are likely to be held in active memory, and it is quite possible that the backup to such database will be in the memory of another computer, without any permanent or semi-permanent copy being made. As noted above, current law requires that a work be fixed before it is protected by copyright, and it may be held that the holding in memory is not fixation.

Holding large databases in memory also provides a practical problem of proof, as it is sometimes difficult to tell what the exact state of the work was at the time of the alleged infringement.

It is possible that developing technologies (such as laser disks) will solve both problems, by keeping an ongoing record, in a fixed form, of each change made to the database. This would permit the database to be reconstituted if the need ever arose, and would also provide the fixed form required to meet the standard set by existing case law.

Where a person has copied an entire collection of computerized data, the courts are likely to have little problem in finding infringement. The courts have already dealt with lawsuits on such "databases" as printed railway timetables and printed law books. The mere fact that data is in a computer, rather than in written form, should not create any insurmountable problems, once the fixation issue is determined.

A problem may occur where there is a large database and the defendant has copied only a small amount of it. For example, the

<sup>20.</sup> See Canadian Admiral Corp. Ltd. v. Rediffusion, Inc., Ex. C.R. 382. (1954).

database may deal with all stocks traded on the Vancouver Stock Exchange, but the defendant may be interested only in the information about one stock. In such a case, the data on other stocks is of no interest to him or her. The existing law on copyright infringement requires that there be at least a substantial amount of copying before infringement is found. In the case of a computerized database, a person who wishes to use a small portion does not even have to look at the remainder. Instead, he or she relies upon the computer program to find the small portion which he or she wants, and only that portion is displayed or printed out.

There have been no cases on this point in Canada. However, the question of whether there has been a "substantial" infringement would probably be addressed by saying that the infringement is substantial if it takes the portion of the database which is of interest in answering the infringer's question. In other words, the question of substantiality would be addressed in terms of quality rather than quantity. If any other holding were made, there would only be infringement where a large portion of database were copied. In practice, copying a large portion of the database is unlikely, unless somebody tries to duplicate the entire database to go into competition with the database writer.

One further matter which may arise in dealing with the question of the taking of information from a database is whether information is something which is capable of being "taken." This matter was addressed by the Supreme Court of Canada in a criminal case, R. v. Stewart.<sup>21</sup> The Court held that theft or taking implies depriving another of property. When a copy is made of information, or the information is displayed, the owner still retains the original of the information. Thus it can not be said he has been deprived of it. What he has been deprived of is the confidentiality of that information.

The court recognized that information loses much of its value when it is not exclusive, but did not see that confidentiality was "property" in the sense that it could be taken. The Court put forth the example of a person that has memorized stolen information. If he cannot forget it, is he then to be continuously charged with possession of stolen property?

This is less a copyright problem than a criminal law or trade secret problem. When information is acquired improperly, some sort of copy is usually made, so copyright infringement exists. Thus, for example, when information in a database is displayed on a screen and copied by hand, the manuscript copy would be a copy of the information in the database. However, if it is held the computer screen display is not a copy, because it is not fixed, then it might be possible for someone to

<sup>21. 1</sup> S.C.R. 963 (1988). See infra notes 104-14 and accompanying text.

access the database, read the information and act on it, all without infringing.

#### E. CONCLUSIONS REGARDING COPYRIGHT

By statutory amendment, Canadian Copyright law has evolved to the point where computer programs are fairly clearly protected by copyright. There does not seem to be any real doubt that databases are also protected. However, second generation issues such as "look and feel," "structure, sequence and organization" and microcode remain to be decided. The problem of whether taking small portions of a database is infringement also remains to be decided.

## **III. PATENT PROTECTION**

# A. INTRODUCTION

Many of the underlying principles of Canadian patent law are similar to those of U.S. patent law, as the Canadian Patent Act was originally modelled on the U.S. Patent Act of 1836. However, some major statutory differences exist. Canada has compulsory licensing in all fields to protect against patent abuse<sup>22</sup> and a complicated system of regulating the price of patented medicines. Since October 1989, the patent system has been based on the first-to-file rather than first-to-invent. Patents now remain in force for 20 years from the filing date, subject to payment of renewal fees.

# **B. HARDWARE**

Inventions relating to computer hardware fit easily within the realm of patent protection. Inventions involving structural and functional features of the hardware can be protected by patent, if they are new, useful, and not obvious.

# C. COMPUTER PROGRAMS

The patentability of computer programs is much less clear. Computer programs are not patentable *per se.* However, patents have been granted for processes or apparatus which utilize computer programs even where the only inventive step was in the novel computer program. The key to patentability appears to be integrating the results in a useful device or product. It should be noted that computer programs are frequently obvious and therefore unpatentable. Even though they involve

<sup>22.</sup> Patent abuse is defined as not working the invention on a commercial scale without satisfactory reasons and not supplying enough of a patented article. R.S.C. 1985, ch. P-4, § 65.

a great deal of work, this work is usually of a type which would be obvious to a person skilled in the art of computer programming.

# 1. The Patent Act

Two sections of the Patent  $Act^{23}$  present problems for software technology which manipulates data or merely produces intellectual information. Such programs fall outside section 2 which defines patentable subject matter; further, section 27(3) provides that no patent shall issue for "any mere scientific principle or abstract theorem."

# 2. Case Law

Case law regarding patentability of software-related inventions can be classified into three groups: court decisions (of which there has been only one to date), Patent Appeal Board decisions, and U.S. case law on statutory subject matter.

# a. The Schlumberger Case

The only court decision on program patentability is Schlumberger Canada Ltd. v. Commissioner of Patents.<sup>24</sup> In this decision, the court rejected a patent application relating to a process in which measurements from seismic bore holes were combined and processed by a computer, using a novel mathematical formula, to yield more useful information. The court found the process to be a "discovery of the various calculations to be made and of the mathematical formulae to be used in making those calculations  $\dots$ "<sup>25</sup> and therefore unpatentable.

The court formulated two principles for determining patentability of software inventions: "In order to determine whether the application discloses a patentable invention, it is first necessary to determine what, according to the application, has been discovered,"<sup>26</sup> and "the fact that a computer is or should be used to implement discovery does not change the nature of that discovery."<sup>27</sup>

Commentators have summarized the approach outlined in *Schlumberger*<sup>28</sup> in the following manner:<sup>29</sup> look at what has been discovered without regard to the presence of a computer, a computer program, or

<sup>23.</sup> R.S.C. 1985, ch. P-4.

<sup>24. 56</sup> C.P.R. (2d) 204 (F.C.A. 1981).

<sup>25.</sup> Id. at 206.

<sup>26.</sup> Id. at 205.

<sup>27.</sup> Id. at 206.

<sup>28.</sup> Id. at 204-206.

<sup>29.</sup> For example see McDonough, Appeal Board Decisions with Respect to Computer Software, 2 CAN. INTELL. PROP. REV. 10 (1985); Kent & Cheung, Patent Protection in Canada for Computer Related Technology, 3 CAN. INTELL. PROP. REV. 249 (1986).

an algorithm; if it is patentable, the presence of a computer to implement the discovery should not make the invention unpatentable.

# b. Patent Appeal Board decisions

It is convenient to sub-divide discussion of the Board decisions relating to computer technology according to the nature of the technology. Computer technology applications generally fall into three categories:

#### i. Control systems

Control systems involve the processing of information by a programmed computer. The refined information is then used to provide instructions for the control of an operating device for an overall better system.

The Board has reversed rejections of patent applications where the invention involves an overall combination which gives new and better results. Application of the information or post solution activity can be critical in making the subject matter patentable.

The application in *Re Application of Bartley & Gilles*,<sup>30</sup> disclosed a method and apparatus used in a variety of process control systems, such as electrical analog, digital electronic, pneumatic, mechanical, or hydraulic control system formats. The Board found it to be patentable. Although the method and means of the application used calculations to arrive at altered signals, the end result was an altered process and not merely a display of information.

Similarly, a patent was granted for an elevator system that could provide priority service to a designated floor.<sup>31</sup> The Examiner had rejected the application because the only novelty lay in the computer program. The Board found that what had been discovered was not merely the program but the kind of operation it brought to the elevator system.

Post-solution activity was important in an application for a system which optimised the performance of a multi-unit power plant producing energy from a variety of different fuels.<sup>32</sup> Incremental test results were processed by a computer. The system then reallocated fuel to provide optimum plant operating efficiency. The Board found patentability. This reallocation step clearly took it beyond the mere calculating of data. The sufficiency of the post solution activity was important in *Re Application of Gerber Garment Technology*.<sup>33</sup> The invention related to an automatically controlled sheet-cutting machine. Claim 1, which in-

<sup>30. 3</sup> C.P.R. (3d) 396 (P.A.B. 1983).

<sup>31.</sup> Re Application of Westinghouse Elec. Corp., 9 C.P.R. (3d) 202 (P.A.B. 1985).

<sup>32.</sup> Re Application of Measurex Corp., 10 C.P.R. (3d) 93 (P.A.B. 1983).

<sup>33. 3</sup> C.P.R. (3d) 563 (P.A.B. 1984).

cluded the process step of "controlling the relative movement of the sheet material and the cutting tool with the machine commands generated,"<sup>34</sup> was not enough to make the process patentable. Additional steps dealing with feedback from the cutting tool were necessary for patentability. Once these additional steps were included, the Board found the applicant's end result was not merely a solution to an algorithm by a program. It was instead an invention involving the selective blade orientation at any time during the cutting operation to achieve an overall improved cutting result.<sup>35</sup>

# ii. Data Manipulation

Data manipulation systems involve computer processing of information to yield more meaningful information. An invention which only provides information is not patentable.<sup>36</sup> However, if the information is refined or integrated with some other apparatus, patentability might be present.

Several patents have been granted for inventions relating to seismic exploration. An invention which crated a three-dimensional display of the earth's subsurface was found to be patentable.<sup>37</sup> The Board found that "[I]t is the display of the co-ordinates in isometric form together with the computer processing steps that make up the applicant's invention, and the invention in our opinion is not merely performing calculations."<sup>38</sup>

They also held that a method of seismic exploration in which reflected signal waves of varying widths were processed through a computer to generate improved seismograms was patentable.<sup>39</sup> The result was a new and better signal-to-noise ratio and not a mere description of a machine method of manipulating analytical data or a mere mathematical theorem.<sup>40</sup>

- 37. Re Application of Seiscom Delta Inc., 7 C.P.R. (3d) 506 (P.A.B. 1985).
- 38. Id. at 510.
- 39. Re Application of Societe Nationale Elf Aquitaine, 6 C.P.R. (3d) 9 (P.A.B. 1984).

492

<sup>34.</sup> Id. at 564.

<sup>35.</sup> Id. at 564. See also Re Application of Bendix Corp., 5 C.P.R. (3d) 198 (P.A.B. 1985) (the fact that a computer is used to implement a discovery does not make the discovery unpatentable); Re Application of General Electric, 6 C.P.R. (3d) 191 (P.A.B. 1985) (same); Re Application of Rockwell International Corp., 6 C.P.R. (3d) 88 (P.A.B. 1983) (same); Re Application of Tokyo Shibaura Electric Co., 7 C.P.R. (3d) 555 (P.A.B. 1985) (same).

<sup>36.</sup> Schlumberger Canada Ltd. v. Commissioner of Patents, 56 C.P.R. (2d) 204 (F.C.A. 1981).

<sup>40.</sup> Id. at 12. For other cases involving seismic exploration and data manipulation see Re Application of Exxon Production Research Co., 3 C.P.R. (3d) 168 (P.A.B. 1983); Re Application of Western Geophysical Co. of America, 3 C.P.R. (3d) 386 (P.A.B. 1983).

# 1990] HARDWARE AND SOFTWARE PROTECTION

Re Application of Dialog Systems<sup>41</sup> involved an application for a system recognizing a speech signal. This case gives some insight into where the Board will draw the line. The Board rejected a claim which it found to be the equivalent of a mathematical algorithm that had been presented and solved.<sup>42</sup> However, another claim went further and disclosed an indication of a match of voice signals by disclosed apparatus. This was held to be more than mere obtaining of information from calculations and was patentable.<sup>43</sup>

#### iii. Operating software

Operating systems control the hardware functions or data base information storage and retrieval systems. A number of patents have been granted for these systems.<sup>44</sup> For example, the Board concluded that more than a series of calculations or a mere scientific principle or abstract theorem was present in an IBM application<sup>45</sup> which disclosed and claimed a method of storing, indexing and retrieving text data for text processing machines such as printers.

The application in *Re Application of Dissly Research Corp.*<sup>46</sup> disclosed a storage and retrieval system for database records. Here as well, the Board concluded that there was patentable subject matter.

The Board allowed two other applications which either avoided or released a "deadlock state" in data processing systems. Deadlocks can arise when multiple processes compete for a common resource. In *Re Application of Honeywell Information System*,<sup>47</sup> the invention avoided deadlocks through a combination of software, firmware, and hardware elements. The combination made use of multiple processes relying on common resources.<sup>48</sup> The Examiner had rejected the application finding it to be mere data or data structure. The Board disagreed. It found that the invention did more than merely determine useful information

<sup>41. 5</sup> C.P.R. (3d) 423 (P.A.B. 1985).

<sup>42.</sup> The claim which was rejected set out the use of the computer in a frequency compensation system to generate a sequence of frequency band equalized spectra over an interval. This claim would preempt a program for such a system and was therefore not patentable.

<sup>43.</sup> See also Re Application of Batelle Memorial Institute, 8 C.P.R. (3d) 133 (P.A.B. 1984). The invention related to a system to obtain an enhanced signal output including means for generating a reciprocal of a Walsh Transform system. The Board found it was patentable subject matter as it was more than mere calculations and more than an algorithm.

<sup>44.</sup> See, for example, the cases cited in Kent and Cheung, supra note 29, at 258.

<sup>45.</sup> Re Application of IBM, 6 C.P.R. (3d) 99 (P.A.B. 1984).

<sup>46. 6</sup> C.P.R. (3d) 420 (P.A.B. 1985).

<sup>47. 13</sup> C.P.R. (3d) 462 (P.A.B. 1986).

<sup>48.</sup> Id. at 466.

from calculations. In the other application,<sup>49</sup> the Board concluded that the system for releasing a deadlock was an arrangement of computing apparatus and was not a mere algorithm or program.<sup>50</sup>

A patent was granted for an invention which distributed programs selectively among a number of computer processors in a switched telecommunications network.<sup>51</sup> The Board once again found that the claims defined more than algorithms or calculations and were more than the execution of programs.

It appears from these decisions that the Board is willing to find patentable subject matter in software operating systems. The challenge is to avoid the label "mere calculations or algorithm or abstract theorem."

c. U.S. Case Law

The Patent Appeal Board has stated that U.S. decisions can be considered as persuasive<sup>52</sup> in determining statutory subject matter. The U.S. decisions are of course not binding.

With this caution in mind, I have set out a summary of the present U.S. position regarding statutory subject matter:

[d]oes the claim refer to a formula in the abstract (non-statutory), or does it implement or apply that formula in a structure or process which, considered as a whole, performs a function the patent laws were designed to protect (statutory).

Certain "quick-fix tests" have been used by the Courts to decide specific situations. Claims have been held non statutory where they:

- 1) Recite a field of use for a mathematical algorithm that is merely presented and solved
- 2) Consist of mere antecedent data gathering steps
- 3) Merely refer to apparatus, or
- 4) Simply read out the results of calculations.

Conversely, claims have been held statutory where they:

- Are directed to the internal operation of the computer, and are independent of the specifics of programs otherwise controlling the computer, or
- Embody a mathematical algorithm, if the claims would be statutory after deletion of the mathematical algorithm.<sup>53</sup>

51. Re Application of Janssens, 6 C.P.R. (3d) 213 (P.A.B. 1984).

<sup>49.</sup> Re Application of Fujitsu Ltd., 9 C.P.R. (3d) 475 (P.A.B. 1985).

<sup>50.</sup> Id. at 478, 479. The Board said: "We find the applicant's system is for releasing a dead-lock state during data processing and includes several components interacting to release one task from a resource and permit another task to use that resource. We do not find the subject-matter to be a programme or an algorithm."

<sup>52.</sup> Re Application No. 961,392 (Waldbaum's Application), 5 C.P.R. (2d) 162 (P.A.B. 1971); Re Application No. 096,284, 52 C.P.R. (2d) 96 (P.A.B. 1978); Re Application of Dialog Systems Inc., 5 C.P.R. (3d) 423 (P.A.B. 1984).

<sup>53.</sup> D. BENDER, COMPUTER LAW A-1 (1987).

# 1990] HARDWARE AND SOFTWARE PROTECTION

This is a distillation of several years of case law. The U.S. and Canadian positions are similar in that a mere formula or information, without any practical application, is not patentable subject matter.

#### D. CONCLUSIONS REGARDING PROGRAM PATENTABILITY

We can conclude that patent protection is available for hardware and software in appropriate circumstances.

To obtain patent protection for a pioneer program, the program should be integrated into a process or be applied in a practical manner. Care should be taken in drafting the claims so that they reflect statutory subject matter.

One unintended and somewhat amusing result in the case law is that it appears easier to get a patent claim to a process which takes place inside a computer than it is to get a claim to a process using a computer in some other application. Thus, a claim to something dealing with the operating system of the computer may well be easier to get than a claim dealing with an application program using a computer. The reason for this is that processes taking place in the operating system of the computer inevitably interface with a number of hardware elements, so that it is usually easy to draft hardware limitations into the claims. In an application program, the result of the program is frequently data which can be used to control a subsequent process, but there is not as clear a continuum between the process and the data as there is with an operating program inside a computer.

Much of the problem in finding general principles from the Patent Appeal Board cases arises because the Patent Appeal Board is trying to reconcile two conflicting views expressed in Schlumberger. First, Schlumberger has stated that the mere fact that a computer is or could be used to implement a discovery does not change the nature of the discovery. The other dictum is that the discovery of various calculations to be made and the algorithm for making these calculations is not patentable. In a case where there are pure mathematical calculations, these two principles are reconcilable. However, more and more computer programs are not used for mathematical purposes, but instead for carrying out a series of process steps for controlling some other piece of equipment. Processes are generally patentable, and it follows from Schlumberger that the presence of the computer should not render them unpatentable. However, except in a very few highly mathematical cases, where the sole output is a series of figures, this would tend to make all computer program cases patentable.

It is useful, in closing, to look at the word "algorithm." In many of the cases where claims have been rejected, they have been rejected on the basis that they merely set forth an "algorithm." The term is defined as "a set of rules or procedural steps that are intended to be followed in sequence to solve a particular problem or to produce a particular result."<sup>54</sup> This definition, of course, is a description of any process. Indeed, computer theorists consider that any process which has a finite number of steps and is communicable is an algorithm. Processes are one of the patentable classes of subject matter specifically set out in the Patent Act. It therefore appears that rejecting a claim on the ground that it sets forth an algorithm is an overly facile reason for rejecting a claim, which is based on some mistaken idea that algorithms only lurk within the dark recesses of computers.

#### IV. TRADE SECRET PROTECTION

#### A. INTRODUCTION

The law of trade secrets essentially protects against breaches of faith. It protects confidential information or innovations from being taken by another party in breach of its obligations. A trade secret may consist of a formula, pattern, device or compilation of information and which gives an advantage over competitors who do not know or use it. U.S. practitioners will recognize this definition as taken from the U.S. Restatement of Torts.<sup>55</sup> Both hardware and software may benefit from trade secret protection.

The key in this area of the law is secrecy. As soon as the secrecy is lost, either by diligent investigation, or some other legal means, the protection ends.<sup>56</sup> Unlike patents or copyright, trade secret protection may only be enforced against those who receive the information in confidence.<sup>57</sup> It does not offer protection against the world.

#### **B. BASIS FOR PROTECTION**

Trade secrets have been protected on the basis of breach of trust and confidence, breach of express or implied contract, and invasion of a proprietary right.<sup>58</sup> Sopinka, J., of the Supreme Court of Canada, characterized the jurisdictional basis as a mixture of all three: "The founda-

<sup>54.</sup> DICTIONARY OF COMPUTING 7 (1982).

<sup>55.</sup> The definition in American RESTATEMENT OF TORTS, § 757 (1930), was cited with approval in R.L. Crain Ltd. v. Ashton, O.R. 303 (1949), 309, aff 'd, O.R. 62 (C.A. 1950).

<sup>56.</sup> R.L. Crain Ltd. v. Ashton, O.R. 303 (1949); Eldon Industries v. Reliable Toy, 54 D.L.R. (2d) 97 (Ont. H.C.J. 1964); International Tools v. Kollar, 2 O.R. 201, *rev'd in part*, 1 O.R. 669 (C.A. 1968).

<sup>57.</sup> This is subject to an exception. Trade secret protection can be enforced against third parties who receive confidential information from the confidee knowing that it is confidential. LAC Minerals Ltd. v. International Corona Resources Ltd., 26 C.P.R. (3d) 97, 119 (S.C.C. 1989), following Liquid Veneer Co. Ltd. v. Scott, 29 R.P.C. 639, 644 (Ch. 1912).

<sup>58.</sup> Morrison v. Moat, 9 Hare. 241 (Ch.D. 1851), aff'd, 21 L.J. Ch. 248 (C.A. 1852).

tion of action for breach of confidence does not rest solely on one of the traditional jurisdictional bases for action of contract, equity or property. The action is *sui generis*, relying on all three to enforce the policy of law that confidences be respected."<sup>59</sup>

# C. ELEMENTS REQUIRED

Three elements are required to obtain trade secret protection: the information must have the necessary quality of confidence, it must have been imparted in circumstances where obligations of confidence arise, and there must be unauthorized use of the information without lawful excuse to the detriment of the communicating party.<sup>60</sup>

#### 1. Secrecy

Preserving confidentiality is the most difficult of the three elements to prove and to practice. Cases have set out some guidelines which should be practised to preserve confidential information.<sup>61</sup>

For computer technology, important protective steps include: restricting access to source code on a need-to-know basis, marking confidential information as such, requiring employees to sign agreements obligating them to maintain confidentiality, distributing computer software in object form, under licenses requiring the licensees to maintain the confidentiality of the software and prohibiting reverse engineering, decompilation, and disassembly, and locking up magnetic media containing confidential information and keeping it under strict supervision.

# 2. Relationship which Imparts Obligation of Confidence

Disclosure to others does not destroy the secrecy of the information where the disclosure is made in confidence, such as to an employee, to a prospective business partner to induce him to do business, or pursuant to a licence agreement requiring an obligation of confidence. A contractual or fiduciary relationship is not necessary<sup>62</sup> for enforcement of trade secret rights.

Although one can look to the law for protection even in the absence of an agreement, well drafted licensing contracts make the par-

<sup>59.</sup> LAC Minerals Ltd., 26 C.P.R. (3d) at 157, following F. GURRY, BREACH OF CONFI-DENCE 25-26 (1984) and R. GOFF & G. JONES, THE LAW OF RESTITUTION 664-667 (3d ed. 1986).

<sup>60.</sup> LAC Minerals Ltd., 26 C.P.R. (3d) at 103; Coco v. A.N.Clark (Engineers) Ltd., R.P.C. 41 (Ch.D. 1969).

<sup>61.</sup> B. SOOKMAN, COMPUTER LAW, ACQUIRING AND PROTECTING INFORMATION TECH-NOLOGY 4-30 to 4-32 (1989) (discusses several cases and the badges they have set out).

<sup>62.</sup> LAC Minerals Ltd., 26 C.P.R. (3d) 97, 124.

ties' rights more certain. The party imparting the confidential information will want to ensure broad protection by using encompassing terms; the receiving party, on the other hand, will want the terms precisely defined. The receiving party must be careful that it does not preclude its own research in the particular area. If it has customers that are competitors of the party divulging the information, it should ensure the agreement will not interfere with continued relations.

In computer technology licensing agreements, it is common to address the following four matters: marking and designation of the confidential matter as confidential, identifying which employees will be in charge of, and have access to, the confidential information, the specific uses which may be made of the confidential information, and the designation of what is not confidential information.<sup>63</sup>

#### 3. Misuse of the Information

A person may not use confidential information, obtained in circumstances imparting confidentiality, without the owner's express or implied consent. He cannot use a trade secret disclosed to him by a third party if he has notice of the fact it is a secret and is being improperly disclosed.<sup>64</sup>

When information is partially public and partially confidential, a confidant will be restrained from enjoying "lead time" or using the confidential information as a springboard ahead of the rest of the public.<sup>65</sup> In Seager v. Copydex,<sup>66</sup> Lord Denning stated:

When the information is mixed, being partly public and partly private, then the recipient must take special care to use only the material which is in the public domain. He should go to the public source and get it; or, at any rate should not be in a better position than if he had gone to the public source. He should not get a start over others by using the information which he received in confidence. At any rate, he

66. 2 All E.R. 415 (C.A. 1967).

<sup>63.</sup> For further discussion see Brait, The Unauthorized Use of Confidential Information, 5 CAN. INTELL. PROP. REV. 180, 188-198 (1988).

<sup>64.</sup> See LAC Minerals Ltd., 26 C.P.R. (3d) 97; see also Polyresins Inc. v. Stein-Hall Inc., 5 C.P.R. (2d) 183 (Ont. H.C.J. 1971).

<sup>65.</sup> In Terrapin, Ltd. v. Builders' Supply Co. (Hayes), Ltd., R.P.C. 128, at 130 (1960) (followed in Cranleigh Precision Engineering Co. v. Bryant, 3 All E.R. 289, at 301 (Q.B.D. 1964)), Roxburgh, J., stated:

As I understand it, the essence of this branch of the law, whatever the origin of it may be, is that a person who has obtained information in confidence is not allowed to use it as a springboard for activities detrimental to the person who made the confidential communication, and springboard it remains even when all the features have been published or can be ascertained by actual inspection by any member of the public.

Id.

should not get a start without paying for it.67

# D. REMEDIES

Remedies available for breach of trade secret rights include injunctive relief restraining use and disclosure of the confidential information, damages or an accounting of profits. A recent decision of the Supreme Court of Canada has added constructive trusts to this list.<sup>68</sup>

# 1. Injunctive Relief

The use or disclosure of a trade secret may be enjoined.<sup>69</sup> Because it is an equitable remedy, the judge has discretion in deciding whether to grant an injunction. If damages will adequately compensate the breach, an injunction generally will not be granted. Courts have considered several factors such as the nature of the information, its relative significance, and its identifiability in deciding whether to award damages or grant injunctions.<sup>70</sup>

If an injunction is issued, its term will last as long as the confiden-

<sup>67.</sup> Id. at 417.

<sup>68.</sup> LAC Minerals Ltd., 26 C.P.R. (3d) 79. La Forest, J., wrote the majority judgement on this aspect of the case, Wilson, J., and Lamer, J., concurring. McIntyre and Sopinka, JJ., dissented on this point.

<sup>69.</sup> Morrison v. Moat, 9 Hare. 241 (Ch. D. 1851).

<sup>70.</sup> Brait, supra note 63, at 204 summarizes the discussion in F. GURRY, supra note 59, at 398-410 as follows:

<sup>1)</sup> The Nature of the Information: Injunctions will be more readily available in the case of personal rather than commercial or technical information, and information of relative insignificance is less likely to result in the granting of an injunction.

<sup>2)</sup> The Extent to Which the Information Has Been Made Public: Where the information has been previously published, an injunction is less likely to be granted as it may have little practical effect.

<sup>3)</sup> The Extent of Contribution to the Defendant: If the confidential information has made a major contribution to the defendant's getting an injunction will be appropriate, whereas if the contribution is only a minor one, then damages will generally be the better remedy [Footnote omitted]. The amount of labour and effort required to produce the information will also be a determining factor.

<sup>4)</sup> Good Faith and Change of Position: If a defendant has, in good faith, substantially changed his position in reliance upon the availability of the confidential information, this will be a strong factor mitigating against the granting of an injunction. [Footnote omitted]. It appears that both elements—good faith and an irrevocable change of position—are necessary for this particular factor to have an essentially determinative influence on the exercise of the court's discretion. Two of the leading British cases in the field, where good faith was present but irrevocable change of position was not, serve to indicate this. In both cases the court granted injunctions. [Footnote omitted].

<sup>5)</sup> Certainty of Terms: As noted previously, courts are very reluctant to grant an injunction unless its extent can be readily determined and thus enable the party enjoined to know exactly what he is prohibited from doing. At the very least, the principle can stand as a procedural requirement governing the drafting of the terms of the injunction.

COMPUTER/LAW JOURNAL

[Vol. X

tial information remains secret.<sup>71</sup> If the information becomes public immediately, defendants will generally be restrained for some period after that time to prevent them from benefitting from the early start.<sup>72</sup>

Interlocutory injunctions are also available. The three necessary criteria, a strong *prima facie* case, irreparable harm, and balance of convenience,<sup>73</sup> are often easily established in trade secret matters.

# 2. Damages or an Accounting of Profits

The object in awarding damages is to put the plaintiff in the position in which he would have been if the breach had not occurred. A number of different ways to calculate damages are available depending on the circumstances. The court may also order an accounting of the defendant's profits resulting from the misappropriation.<sup>74</sup>

#### 3. Constructive Trusts

In the recent case *LAC Minerals v. International Corona Re*sources,<sup>75</sup> the Supreme Court endorsed the use of constructive trusts as a remedy for breach of confidence. In a three to two decision, a constructive trust was found to be an appropriate remedy, if in the circumstances it is the only remedy that will do justice.

Entitlement to the remedy requires "an [unjust] enrichment, a corresponding deprivation, and the absence of any juristic reason for that enrichment."<sup>76</sup> Once these three elements have been established, the court must then examine the circumstances to determine whether the constructive trust is the appropriate remedy to address the unjust enrichment.<sup>77</sup>

The confidential information does not have to be property. The constructive trust can both recognize and create a right of property. In adopting the view expressed in a standard text,<sup>78</sup> La Forest, J. stated: "In their view, a proprietary claim should be granted when it is just to grant the plaintiff additional benefits that flow from the recognition of

74. Canadian Aero Services Ltd. v. O'Malley, S.C.R. 592 (1974).

76. Pettkus v. Becker, 2 S.C.R. 834 (1980).

78. See R. GOFF & G. JONES, THE LAW OF RESTITUTION, supra note 59.

<sup>71.</sup> International Tools v. Kollar, 2 O.R. 2d (1966), rev'd in part, 1 O.R. 669 (C.A. 1968).

<sup>72.</sup> Id.; see Terrapin, Ltd. v. Builders' Supply Co. (Hayes) Ltd., R.P.C. 128, 130 (1960).

<sup>73.</sup> American Cyanamid Co. v. Ethicon Ltd., 1 All E.R. 504 (H.L. 1975). The first element in England is not "a strong *prima facie* case." This is a Canadian requirement. In England all that is required is "a substantial issue to be tried." *Id.* 

<sup>75.</sup> LAC Minerals Ltd. v. International Corona Resources Ltd., 26 C.P.R. (3d) 97 (1989).

<sup>77.</sup> LAC Minerals Ltd., 26 C.P.R. (3d) 97, 131 (following Hunter Engineering Co. v. Syncrude Canada Ltd. 1 S.C.R. 426 (1989)).

a right of property. It is not the recognition of a right of property that leads to the constructive trust."<sup>79</sup>

In the case, LAC Minerals was found to hold valuable property containing gold deposits in trust for Corona. Corona had given LAC Minerals confidential information regarding gold deposits in this particular piece of property for the purpose of developing the property jointly. LAC had then obtained the property on its own account. Damages were almost impossible to quantify because of the uncertainty of the amount of gold, gold prices, and inflation. An injunction was useless because the total benefit had accrued to the defendant through a single misuse of the information. In the circumstances, the only just remedy available was the constructive trust.<sup>80</sup>

# 4. Defence to an Action for Breach of Contract

In Computer Workshops Ltd. v. Banner Capital Market Brokers  $Ltd.,^{81}$  the breach of trade secret rights was successfully used as a defence to a breach of contract action. The plaintiff company was engaged in the sale of microcomputers and accessories. It entered into a contract for the supply of computers with the defendants. In doing so, the plaintiff had access to the defendants' software system that would take six months to develop independently. The plaintiff used this information in developing software for competitors of the plaintiff. Upon learning of this, the defendants repudiated the contract. The plaintiff brought an action for damages. The action was dismissed. The court found that the plaintiff was in breach of an implied term of the contract and in breach of its duty of confidence.<sup>82</sup> The court felt this was a breach going to the root of the contract.

#### E. CONCLUSIONS REGARDING TRADE SECRETS

The scope of trade secret protection is far narrower than that provided by copyright and patent law. However, as long as the subject is kept secret software and hardware matters that would not qualify for protection under these latter two branches can qualify for trade secret protection.

<sup>79.</sup> LAC Minerals Ltd., 26 C.P.R. (3d) at 133.

<sup>80.</sup> Id. at 132.

<sup>81. 64</sup> O.R. (2d) 266 (Ont. H.C.J. 1988).

<sup>82.</sup> The court also found a breach of a fiduciary duty. From LAC Minerals Ltd., 26 C.P.R. (3d) 97, we now know that there is no fiduciary relationship between parties dealing at arms length.

# V. CHIP PROTECTION LEGISLATION

# A. INTRODUCTION

Semiconductor chips are essential components of all modern computers. They are tiny, intricate electrical circuits, usually made of silicon. Complex patterns are etched on and in the chips by light, chemicals, electrons from an electron beam, or a combination of all three. When connected to a larger circuit within the computer chips perform a myriad of functions. Depending on the design, chips can have data or computer programs permanently encoded in them. They can also store data and programs at later times, and be erasable or non-erasable.

Designing the complex circuitry patterns within the chips can be expensive and time consuming. In comparison to the design cost, the production costs are low in comparison. Since chips can be easily copied, companies are tempted to copy the circuit design of competitors' successful chips.

Both patent and copyright laws were considered to be inadequate for chip protection. A completely new form of intellectual property protection was therefore developed.

# B. THE U.S. STATUTE

The United States passed a chip protection act in 1984.<sup>83</sup> It protects the "mask works" used in generating the elaborate three dimensional design of chips for a maximum of ten years. "Mask work" refers to a method of chip protection which involves exposing light through a series of masks onto the surface of the chip and carrying out chemical treatments between the exposures. This was the prevailing method of making chips at the time the U.S. act was passed. Although this method is still used in some cases, many chips are made without masks so that the term is somewhat dated.

The U.S. Act gave reciprocal protection to those countries that protected U.S. chips in their markets or took steps to implement similar legislation within a short period of time. Several countries have done so. The U.S. has granted interim protection to Canada based on its good faith efforts towards enacting similar chip legislation.

# C. CANADA'S CHIP PROTECTION ACT

Canada recently passed an act<sup>84</sup> to protect integrated circuit "topographies." This term, which is also used in some other countries, is de-

<sup>83.</sup> Semiconductor Chip Protection Act, Pub. L. No. 98-620, 98 Stat. 3347 (1989); 17 U.S.C. §§ 900 et seq.

<sup>84.</sup> Integrated Circuit Topography Protection Act, S.C. 1990, ch. 36. Formerly Bill C-57, given Royal Assent June 27, 1990.

# 1990] HARDWARE AND SOFTWARE PROTECTION

fined as the two- or three-dimensional pattern of circuit elements for making integrated circuit products. "Topography" is thus independent of the technology by which the chip is made. Topographies must be registered to obtain the draft Act's protection.

#### 1. Registration

One condition of registration is that the topography be original.<sup>85</sup> Originality is defined to require that the creation be more than a mere reproduction of all or part of another topography, that it be the result of an intellectual effort, and that it must not be commonplace among either chip designers or manufacturers at the time of its creation.<sup>86</sup>

The application for registration must be made either before or within two years after the first commercial use of the topography.<sup>87</sup> Protection is for a term of ten years starting from the earlier of the registration date or the first commercial use of a chip embodying the topography.<sup>88</sup>

# 2. Exclusive Rights and the Exceptions

Under the Act, the owner of a protected topography will have the exclusive right to reproduce, import or commercially exploit either the topography or the chips that incorporate the topography.<sup>89</sup>

Three provisions limit the owner's exclusive rights: the reverse engineering provisions,<sup>90</sup> the innocent purchaser exception,<sup>91</sup> and the loss of remedies for unmarked chips.<sup>92</sup>

The reverse engineering exceptions were included to encourage competition and development. A party may "reverse engineer" a protected topography for the purpose of analysis, evaluation and teaching. Topographies derived from the reverse engineering that satisfy the originality requirements are also exempted from infringement actions.<sup>93</sup>

The latter two provisions protect "innocent infringement." Persons who import or sell chips in Canada without knowledge that the chips are infringing Canadian chip protection rights are not liable for infringement until notified that the chips are protected.<sup>94</sup> Even after notification, the innocent purchaser is permitted to sell existing inventory

85. Id. § 4(1)(a).
86. Id. § 4(2).
87. Id. § 4(1)(b).
88. Id. § 5.
89. Id. § 3.
90. Id. §§ 6(2)(a), (b).
91. Id. § 10.
92. Id. § 11.
93. Id. §§ 6(2)(a), (b).
94. Id. § 10.

on payment of a reasonable royalty.<sup>95</sup>

Owners of unmarked chips cannot recover damages from an infringer who is unaware of the registration.<sup>96</sup> The owner may only obtain an injunction. This provision is designed to encourage creators to mark their chips with a notice showing their rights.

#### 3. Action for Infringement and Remedies

The owners of protected topographies, and in some cases licensees, can enforce their exclusive rights by suing for infringement<sup>97</sup> subject to the above three exceptions. There is a three year limitation period for bringing the action.<sup>98</sup>

The remedy section is broadly worded. The court can make "such orders as the circumstances require." The section goes on to list several remedies included in the expression.<sup>99</sup>

### D. INTERNATIONAL CHIP PROTECTION

The World Intellectual Property Organization ("WIPO") drafted a chip protection treaty, which was passed in May, 1989 by a vote of 49 to 2, with five countries, including Canada, abstaining.<sup>100</sup> Japan and the United States were the countries voting against the treaty. Because these two countries are the world's largest chip producers and users, there is real doubt as to how effective the treaty will be.

# VI. CRIMINAL AND QUASI-CRIMINAL SANCTIONS

# A. INTRODUCTION

Criminal law can also be used to protect computer technology. Traditional criminal offenses, and recent statutory amendments both to the Criminal Code and the Copyright Act, may be used to stop those criminally exploiting computer technology. Using the criminal law to go after infringers can be effective and inexpensive. The Crown Prosecutor (the Canadian equivalent to a U.S. District Attorney) gathers the evidence and bears the cost of appearing in Court. However, the criminal burden of proof is, of course, more difficult to meet, as proof is required beyond a reasonable doubt.

<sup>95.</sup> Id. § 10(b).

<sup>96.</sup> Id. § 11.

<sup>97.</sup> Id. § 8.

<sup>98.</sup> Id. § 12.

<sup>99.</sup> Id. § 9 (sets out the powers of the court).

<sup>100.</sup> Diplomatic Conference for the Conclusion of a Treaty on the Protection of Intellectual Property in Respect of Integrated Circuits, Washington, D.C., May 8-26, 1989. For details see Copyright, Monthly Review of the World Intellectual Property Organization, No. 6, June 1989, at 191-206.

#### 1990]

#### **B. TRADITIONAL OFFENSES**

# 1. Theft

The theft provision (§ 322) states that "Every one commits theft who fraudulently . . . takes . . . anything . . . with intent . . . to deprive . . . the owner of it . . . . "<sup>101</sup> The present position is that tangible property (hardware) can be the subject of theft; however, misappropriation of information in a computerized database, or unauthorized reproduction of computer programs or data, can not.

Hardware, which is tangible personal property, obviously qualifies as "anything" within the theft provision.<sup>102</sup> Possession of property pursuant to a crime,<sup>103</sup> may also be used.

"Anything" has been held not to include computer programs if there is only copyright infringement, without more. In R. v. Stewart,<sup>104</sup> the Supreme Court of Canada stated:

Copyright is defined as the exclusive right to produce or reproduce a work in its material form (s.3). A mere copier of documents, be they confidential or not, does not acquire the copyright nor deprive its owner of any part thereof. No matter how many copies are made of a work, the copyright owner still possesses the sole right to reproduce or authorize the reproduction of his work.<sup>105</sup>

If something physical is taken, such as a disc or piece of paper, then a theft charge may apply.<sup>106</sup>

"Anything" also does not include confidential information but for different reasons. Confidential information has been held not to be "property" under the Criminal Code.<sup>107</sup> Therefore, taking computer data or confidential information stored on a computer will not support a conviction for theft.<sup>108</sup>

In R. v. Stewart, the Supreme Court said it was not deciding whether confidential information may be "property" for civil law purposes. However, their characterization will undoubtedly be somewhat

107. R. v. Stewart, 1 S.C.R. 963.

108. Id. See also R. v. Czerlau, 30 O.A.C. 165 (O.C.A. 1988); R. v. Offley, 70 A.R. 365 (Alta.C.A. 1986).

<sup>101.</sup> R.S.C. 1985 Ch. C-46, § 322 (emphasis added).

<sup>102.</sup> Hewson v. R., 2 S.C.R. 82 (1979).

<sup>103.</sup> R.S.C. 1985 Ch. C-46, § 354.

<sup>104. 1</sup> S.C.R. 963 (1988).

<sup>105.</sup> Id. at 982.

<sup>106.</sup> B. SOOKMAN, *supra* note 61 at 7-3 sets out some American cases and a British case where this has occurred: Hancock v. Texas, 402 S.W. 2d 906 (Tex. Crim. App. 1966), *aff'd*, 379 F.2d 552 (5th Cir. 1967); Louisiana v. Tanner, 534 So. 2d 535 (La. Ct. App 1988); R. v. Coles, C.A., Mustill, L.J., unreported, May 20, 1988 (robbery of computer discs containing computer programs).

persuasive in civil matters. The Court based this finding on both public policy and the nature of confidential information.

The Court found that public policy did not favour treating confidential information as property for criminal purposes. The Court felt that free flow of information and greater accessibility to information was perhaps better for society than protecting the economic or commercial interests in confidential information.<sup>109</sup> In addition, the question of what comprised confidential information was vague and difficult to determine even in civil cases. In a criminal context several questions might arise: "Is confidentiality based on the alleged owner's intent or on some objective criteria? At what point does information cease to be confidential and would it therefore fall outside the scope of the criminal law?"<sup>110</sup> The Court added that while some confidential information might be in need of protection through the criminal law, balancing the competing interests was a political decision more properly left to Parliament.<sup>111</sup>

The Court went on to find that confidential information was not "anything" which could be stolen within section 322 because its nature meant it could not be taken or converted in a manner that deprived the victim of its use, except in rare circumstances:

Confidential information is not of a nature such that it can be converted because if one appropriates confidential information without taking a physical object, for example by memorizing or copying the information or by intercepting a private conversation, the alleged owner is not deprived of the use or possession thereof. Since there is not deprivation, there can be no conversion. The only thing that the victim would be deprived of is the confidentiality of the information. In my opinion, confidentiality cannot be the subject of theft because it does not fall within the meaning to the "anything" as defined above.<sup>112</sup>

P.L. Biro and M. Chromecek discuss this issue in an article analyzing the R. v. Stewart decision.<sup>113</sup> They submit that confidentiality is an intrinsic part of the definition of confidential information and should be characterized as something different than information per se. They argue that the confidentiality is what makes the information valuable, and the value is lost when the owner is deprived of exclusive control

<sup>109.</sup> R. v. Stewart, 1 S.C.R. at 977.

<sup>110.</sup> Id. at 978.

<sup>111.</sup> Id.

<sup>112.</sup> Id. at 980. A case with precisely such "rare circumstances" reached the Supreme Court only two years later, which leads one to suspect that such circumstances are not as rare as the Court thought. See LAC Minerals Ltd. v. International Corona Resources Ltd., 26 C.P.R. (3d) 97 (1989). One distinction is that LAC Minerals Ltd. dealt with a true trade secret having a commercial value. See infra note 121.

<sup>113.</sup> Biro & Chromecek, Is Confidential Information Property? — One More Time, 5 CAN. INTELL. PROP. REV. 233 (1988-89).

over the information. They make the analogy that a land owner has a right against a trespasser even though the trespasser has not deprived the owner of continued use of the land.<sup>114</sup>

# 2. Fraud

Anyone selling unauthorized copies of software and manuals can be convicted of fraud pursuant to section 380 of the Criminal Code.<sup>115</sup> This section makes it an offence to defraud the public or any person of any property, money, or valuable security. Evidence of dishonesty and deprivation of the owner must be shown to establish fraud.<sup>116</sup> A direct relationship between the victim and the offender is, however, unnecessary.<sup>117</sup>

In *R. v. Ram*,<sup>118</sup> the accused was convicted by judge and jury of fraud. Mr. Ram had copied and sold computer software and manuals owned and copyrighted by IBM and other companies. At trial, evidence was introduced to show that unauthorized reproduction of manuals and software placed the manufacturers at risk of economic loss, establishing the deprivation element, and that Mr. Ram had intended to defraud those manufacturers and put them at risk of economic loss, establishing the dishonesty and *mens rea* element. In sentencing Mr. Ram, the

115. R. v. Ram, unreported decision of Dymond, J., March 26, 1987, District Court, Toronto, fully discussed in case comment by Finlay, 4 CAN. COMP. L. REP., No. 7 at 109-113 (1987); R. v. Leahy, 21 C.P.R. (2d) 422 (Ont. Prov. Ct. 1988). In movie video pirating situations, fraud convictions were entered for selling or renting to the public unauthorized copies of films in R. v. Kirkwood, 73 C.P.R. (2d) 114 (O.C.A. 1973) and R. v. Fitzpatrick, 11 C.C.C. (3d) 46 (B.C.C.A. 1984).

116. R. v. Olan, 2 S.C.R. 1175 (1978).

117. R. v. Kirkwood, 73 C.P.R. (2d) 14 (O.C.A. 1973). In this case, the accused had knowingly sold and distributed counterfeit video tapes of movies. The victims named were "such companies and persons as would be caused loss by the unlawful distribution of video tapes of motion picture films." The Court of Appeal said:

I am satisfied that the respondent's willingness to enter into the commercial distribution of the counterfeit video cassettes constitutes evidence from which the trier of fact may infer an awareness on his part of a risk of prejudice to the economic interests of the real owner of distribution rights and copyright. Notwithstanding the absence of a relationship, these owners could be defrauded of the money earned or to be earned by the respondent.

Id. at 120.

<sup>114.</sup> Id. Biro and Chromecek also argue that confidential information meets the criteria set out in section 322(1)(d):

But it is equally true that the appropriation or disclosure of confidential information will, even if it cannot amount to a "deprivation" by virtue of the fact the "owner" never lost the information *per se*, have the effect of transforming that information in such a manner that "it cannot be restored in the condition in which it was at the time it was taken or converted" (another "property" feature recognized by § 283(1)(d) of the Criminal Code) [now 322(1)(d)].

Id. at 241.

<sup>118.</sup> Dist. Ct., Toronto, March 26, 1987. See Finlay, supra note 115 at 109-113.

Judge considered the extent of Mr. Ram's activities. She remarked that a prosecution for fraud was warranted, as Mr. Ram's activities could not be considered merely a civil wrong nor a summary breach of the Copyright Act. He was given a five month prison sentence and put on probation for three years. He was prohibited from being involved in any business that made copies of computer software for rent or sale during the probation.<sup>119</sup>

Unauthorized disclosure of confidential information will not support a fraud conviction. There is no "property, money, or valuable security" of which to defraud a person.<sup>120</sup> R. v. Stewart distinguished trade secrets and copyrighted material from amorphous confidential information. The Court said that with trade secrets and copyrighted material, the requisite deprivation would be clear.<sup>121</sup>

Obviously, fraud requires a criminal *mens rea*. Therefore, mere copying in good faith, even coupled with sale, will not support a fraud conviction.

# C. DEFACING A TRADE MARK

The Criminal Code provides penalties for forging a trade mark, and for defacing a trade mark. In one Quebec case,<sup>122</sup> the copier copied a program and a manual. He did not remove the trade mark of the owner when copying the program and was convicted of forging a trade mark. He removed the trade mark when copying the manual and was convicted of defacing the trade mark. This seems to pose a conundrum for copiers of trade marked products.

<sup>119.</sup> Id. See also R. v. Leahy, 21 C.P.R. (2d) 422 (Ont. Prov. Ct. 1988), where the accused was ordered to trial after a preliminary inquiry. The accused ran a "software evaluation" club. All members were required to sign a membership agreement, the terms of which provided that a member was allowed to take copied software and manuals only for evaluation purposes. Once a member had evaluated the material, the disc was to be erased and the manuals returned. The evidence established that in practice, customers bought and kept the copied discs. Most of the stock consisted of copied manuals and discs. The judge found there was evidence to show that the club was merely a facade. The real nature of the operation was to distribute unauthorized materials in breach of the rights of ownership that the manufacturers had in the products. The judge found that a properly instructed jury could find the dishonest conduct required to support a fraud conviction.

<sup>120.</sup> R. v. Stewart, 1 S.C.R. 963 (1988).

<sup>121.</sup> The Supreme Court approved the reasoning of the Court of Appeals:

Although the respondent would have received some money for the information I find it difficult to see how this hotel suffered the requisite deprivation or detriment within the meaning of R. v. Olan . . . The deprivation would be clear if the confidential information had been in the nature of a trade secret or copyrighted material having a commercial value intended to be exploited by the victim.

R. v. Stewart, 42 O.R. (2d) 225, 236 (1983).

<sup>122.</sup> R. v. Locquet, 5 C.P.R. (3d) 173 (Court of Sessions of the Peace) (1985).

# 1990] HARDWARE AND SOFTWARE PROTECTION

#### D. AMENDMENTS TO THE CRIMINAL CODE

Two amendments to the Criminal Code were enacted in 1985 to deal specifically with computer crime: Section 342.1(1) covers fraudulent interception of any function of a computer system or fraudulently obtaining any computer service, and section 430(1.1) covers computer mischief.

# 1. Unauthorized Use — Section 342.1

Unauthorized use of computer systems and computer services was seen as a growing problem. Parliament reacted by passing section 342.1(1). This section makes it an offence to obtain, directly or indirectly, a computer service (defined as including data processing and the storage or retrieval of data) by fraudulent means, to intercept any function of a computer system, or to use a computer system with intent to commit one of the first two offenses or an offence under section 430 (mischief) in relation to data or a computer system.

Several terms are defined in section 342.1(2). Given the definitions of "data" and "computer program," it may be an offence to store or retrieve computer programs and data from any computer system by fraudulent means.<sup>123</sup> The scope of this section is as of yet uncertain.

#### 2. Computer Mischief — Section 430(1.1)

The new "computer mischief" offence specifically relates to data. The new provision makes it an offence to wilfully destroy or alter data, render it meaningless, useless or ineffective, obstruct or interfere with the lawful use of data or with any person lawfully using the data, or to deny access to data to any person entitled to access it.

# E. QUASI-CRIMINAL OFFENSES - COPYRIGHT ACT

It is an offence under the Copyright Act knowingly to make, sell, rent, exhibit, distribute or import for trade, any infringing copy of a work in which copyright subsists.<sup>124</sup> The penalties for such action have increased dramatically with the new Copyright Act. The maximum fine per transaction has increased from \$200.00 to \$1,000,000.00. These new penalties should act as a strong deterrent to copyright infringement and

<sup>123. &</sup>quot;Data" is defined as "representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system." R.S.C. 1985, ch. C-46,  $\S$  342.1(2).

<sup>&</sup>quot;A computer program" is "data representing instructions or statement that, when executed in a computer system, causes the computer system to perform a function." Id.

<sup>&</sup>quot;Computer service" includes "storage or retrieval of data." Id.

<sup>124.</sup> Copyright Act, R.S.C. 1985, ch. C-42, § 42, as amended, 4th Supplement, ch. 10, § 10.

also make it worthwhile for police and Crown prosecutors to lay Copyright Act charges.

# F. CONCLUSIONS REGARDING CRIMINAL/QUASI-CRIMINAL SANCTIONS

Both traditional and new criminal provisions can be effectively used to protect computer technology. The particular provision employed must be carefully chosen as the courts strictly construe all criminal statutes.

Of the traditional offenses, theft is the most appropriate for computer hardware. Both fraud and the Copyright Act offenses protect against the sale of unauthorized copies of computer programs and manuals.

The scope of the new computer offenses in the Criminal Code will be determined by further decisions of the courts.

# VII. ANTON PILLER ORDERS

# A. INTRODUCTION

Finally, I would like to discuss Anton Piller orders. An Anton Piller order is an exceptional remedy, which is extremely useful in intellectual property disputes where evidence of infringement can be quickly destroyed.

The order is best described as a civil search warrant, despite the refusal of the courts to label it as such.<sup>125</sup> An Anton Piller order is distinguished from a search warrant because it does not authorize forceful entry onto any premises. It is an order *in personam* ordering a defendant to permit entry and inspection of the documents by the plaintiff. Of course, if permission is not forthcoming, the defendant faces contempt of court proceedings.

The order derives its name from an early case which granted the unique remedy.<sup>126</sup> Counsel seeking the order found some support in nineteenth century case law.<sup>127</sup> This was all the ammunition Lord Den-

127. This is fully discussed in Berryman, Anton Piller Orders: A Canadian Common Law Approach, 34 U. TORONTO L.J. 1, 3-6 (1984).

<sup>125.</sup> In Anton Piller KG v. Manufacturing Processes Ltd., Ch. 55 (C.A. 1976), Lord Denning confirmed the authority in Entick v. Carrington, 2 Wils K.B. 275 (1965), that there is no common law power to give a search warrant. Lord Denning stated that the order merely contemplated entry and inspection by the permission of the defendants. Anton Piller KG, Ch. at 60. This is discussed by Rock, The "Anton Piller" Order: An Examination of its Nature, Development and Present Position in Canada, 5 ADVOCATES' QUARTERLY 191, 192-193, 208 (1984-85), and by Smith, Computer Pirates and Anton Piller Orders: The Remedy and its Use in Canada, 4 CAN. COMP. L. REP., No. 5, 75, 78 (1987).

<sup>126.</sup> Anton Piller KG, Ch. 55 (C.A. 1976). Actually, the Anton Piller case was the second in which such a remedy was granted, but it has given its name to the proceeding. The earlier case was in the Chancery division: E.M.I. v. Pandit, 1 W.L.R. 302 (1975).

ning required to create the new remedy. Since this decision, the Anton Piller order has been widely use in England. It has also gained acceptance in Canada,<sup>128</sup> although Canadian courts have generally been more conservative in granting prejudgment remedies.

#### B. JURISDICTION TO GRANT THE ORDER

The Court's jurisdiction to grant the order has been founded on four separate grounds. There is some debate as to which is the appropriate basis in Canada.<sup>129</sup> The grounds are:

1. The Court's inherent jurisdiction over a defendant *in personam* as recognized by the nineteenth century common law case authorities.<sup>130</sup>

2. The Rules of Practice providing for pre-trial discovery and inspection of the defendant's property.<sup>131</sup>

3. The power of the Canadian Courts to grant an injunction when it is "just and convenient" to do so. $^{132}$ 

4. The Court's inherent jurisdiction to preserve the integrity of its own processes against destruction of property or evidence by the defendants.<sup>133</sup>

Commentators agree that there are problems in defining the jurisdiction to grant an Anton Piller order too narrowly. Berryman suggests "Accepting that square pegs don't fit round holes, it has been suggested that Canadian courts should utilize their inherent jurisdiction to advance this remedy."<sup>134</sup>

# C. PRE-CONDITIONS TO THE GRANT

Three requirements must be satisfied before an order will be granted:

First, there must be an extremely strong prima facie case. Secondly,

129. For a detailed discussion of jurisdiction, see Berryman, supra note 127, at 10-18, and Rock, supra note 125, at 207-212.

130. See generally Rock, supra note 125, and Berryman, supra note 127.

131. Rock, *supra* note 125, at 211, considers the analogy between the discovery process and Anton Piller orders to be "fragile indeed."

132. In Ontario, § 114 of the Courts of Justice Act, S.0. 1984, ch. 11.

133. See generally Rock, supra note 125, and Berryman, supra note 127.

134. Berryman, supra note 127, at 18. Rock, supra note 125, at 213, suggests a hybrid view: that it is a remedy arising from the injunction jurisdiction but fashioned and effected by the inherent jurisdiction of the court.

<sup>128.</sup> Bardeau Ltd. v. Crown Food Equipment Ltd., 66 C.P.R. (2d) 183 (Ont. H.C.J. 1982); Nintendo of America Inc. v. Coinex Video Games Inc., 69 C.P.R. (2d) 122 (F.C.A. 1982); Aldrich v. Struk, 8 C.P.R. (3d) 369 (B.C.S.C. 1984); Culinar Foods Inc. v. Mario's Food Products Ltd, 12 C.P.R. (3d) 420 (F.C.T.D. 1986); Sunwell Engineering Co. v. Mogilevsky, 12 C.P.R. (2d) 560 (Ont. H.C.J. 1982); IBM v. Certain Unknown persons carrying on business as The Value Club, No. T-112-87 (F.C.T.D. January 21, 1987). It was recognized in Chin-Can Communication Corp. v. Chinese Video Centre Ltd., 70 C.P.R. (2d) 184 (F.C.T.D. 1982) but the facts did not merit granting the order.

the damage, potential or actual, must be very serious for the applicant. Thirdly, there must be clear evidence that the defendants have in their possession incriminating documents or things, and that there is a real possibility that they may destroy such material before any application *inter partes* can be made.<sup>135</sup>

Because this order is an exceptional remedy, it is critical have strong evidence satisfying each of the three conditions.<sup>136</sup>

#### D. PROCEDURAL SAFEGUARDS

In addition, the courts have imposed a number of procedural safeguards to protect of the defendant.

1. Undertaking as to Damages

Generally, the applicant is required to give an undertaking as to damages and give proof of its financial ability to answer the undertaking.<sup>137</sup>

#### 2. Service Requirements

The order must be served personally by the plaintiff's solicitor, who is required to explain, in plain language, what the order means and the obligations it imposes on the defendant. Supporting affidavits must usually be served with the order as well. This gives the defendant an immediate opportunity to decide whether to bring a motion challenging the order.<sup>138</sup>

#### 3. Specifics as to Time, Place, and What May be Removed

The order must specify the time and place of the search, the names and numbers of those that will do the search, and the property or documents that may be removed and copied. In order to protect the defendant's confidential information, often only persons independent of the

<sup>135.</sup> Anton Piller, Ch. 55 at 62 (opinion of Lord Ormrod). Nintendo of America Inc. v. Coinex Video Games Inc., 69 C.P.R. (2d) 122 (F.C.A. 1982) approved this test in Canada.

<sup>136.</sup> In Chin-Can Communication Corp. v. Chinese Video Centre Ltd., 70 C.P.R. (2d) 184 (F.C.T.D. 1982), the order was not granted because the evidence was not strong enough.

<sup>137.</sup> Often the applicant will have to post a bond as security for the undertaking. For example in *Nintendo of America*, 69 C.P.R. (2d) 122, IBM v. Certain Unknown persons carrying on business as The Value Club, No. T-112-87 (F.C.T.D. January 21, 1987), and Aldrich v. Struk, 8 C.O.R. (3d) 369 (B.C.S.C. (1984), the plaintiffs had to post bonds of \$75,000, \$50,000, and \$5,000 respectively.

<sup>138.</sup> If a statement of claim has been issued, it is also generally required to be served. If a statement has not been issued, the court usually directs the plaintiff to issue and serve the statement of claim with the order or within two days of serving the order.

plaintiff can carry out the search and those persons are ordered not to disclose their findings to the plaintiff.

### 4. Restrictions on Use

The order may provide that the plaintiff can only use the documents or information for the purposes of the civil proceedings against the defendant.

### 5. Duty of Full Disclosure

Motions for Anton Piller orders are almost always brought *ex parte* since the very essence of the order is surprise. Courts have therefore imposed a duty to make full disclosure on the applicant. There can be severe consequences for failing to do so. Any hint of less than full disclosure can result in the discharge of the order without regard to the merits of the plaintiff's case.<sup>139</sup>

Collier J. had this to say: "The law is clear that where there has been non-disclosure of relevant facts, whether deliberate or unintentional, an *ex parte* injunction can and usually ought to be set aside."<sup>140</sup>

# E. SCOPE OF THE ORDER

Anton Piller orders grant extraordinary rights to plaintiffs. The rights in each case will depend on the particular order, but such orders can be very sweeping.<sup>141</sup> An order can direct the defendants to submit to a search of their premises and to disclose specified information, and can restrain them from taking certain action.

The order can specify more than seizure of the infringing articles

<sup>139.</sup> Steele, J., in Bardeau Ltd. v. Crown Food Equipment Ltd., 66 C.P.R. (2d) 183 (Ont. H.C.J. 1982), thought that non-disclosure of any material fact may be fatal to an Anton Piller order even if it did not bear directly on the granting of the order. This view was not followed in Midway Mfg. v. Bernstein, 67 C.P.R. (2d) 112 (F.C.T.D. 1982). Although there was non-disclosure of a material fact, he allowed the Anton Piller order to stand.

<sup>140.</sup> Midway Mfg. v. Bernstein, 67 C.P.R. (2d) at 117.

<sup>141.</sup> For example in *IBM*, No. T-112-87 (F.T.C.D., January 21, 1987) 69 C.P.R. (2d) 122 (F.C.A. 1982), the plaintiffs were permitted to search any premises, warehouse, home, automobile or other storage facility used for copying or storing the infringing materials. The Value Club was required to disclose, *inter alia*, all infringing objects, documents, or copies in its possession, power, custody or control and to disclose the means for cataloguing and viewing computer software programs and data. The defendant had to provide the means to open all storage facilities, to permit the plaintiff's solicitors to make copies of its software programs and documents on the Club's equipment, identify all person directing the activities of the Club and allow photographs of articles found on the premises and the premises themselves. An interim injunction prohibiting several acts such as disposing of the plaintiff's wares or making further copies or destroying evidence was also granted. *See* Smith, *supra* note 125, at 76-77 for discussion of the order.

or the plaintiff's property. Blueprints, plans and business documents of the defendant which are useful to the plaintiff's case may also be specified. The order may specify that business premises, homes and cars be searched for the purpose of inspecting, removing, and copying all materials subject to the order.<sup>142</sup>

Disclosure of the defendant's suppliers and customers may be required by the Anton Piller order. The order also may restrain the defendants from destroying evidence.

#### F. THE ISSUE OF SELF-INCRIMINATION

When an Anton Piller order requires a defendant to disclose information and documents to a plaintiff, the issue of self-incrimination may arise. The disclosed information could conceivably make the defendant subject to criminal<sup>143</sup> and quasi-criminal<sup>144</sup> sanctions. It has yet to be determined whether section 13 of the Canadian Charter of Rights and Freedoms which protects against self-incrimination will apply to Anton Piller orders.<sup>145</sup>

The law which has been developed in Great Britain would probably be persuasive, in the absence of Canadian cases. The House of Lords has held that whether a privilege against self-incrimination arises depends on the following circumstances: whether charges are pending or have been laid, whether the charges are serious, and whether the disclosure the plaintiff seeks in a civil action would be likely to constitute proof against the defendant in criminal proceedings.<sup>146</sup> This decision was overruled legislatively in England. A defendant is now required to respond to an Anton Piller order by providing the information, but the responses are inadmissible in criminal proceedings for related offenses.<sup>147</sup>

143. For example see Criminal Code, R.S.C. ch. C-46, §§ 342.1 and 380.

<sup>142.</sup> For example see IBM, No. T-112-87 (F.T.C.D., January 21, 1987) 69 C.P.R. (2d) 122 (F.C.A. 1982). This is discussed by Rock, supra note 125 at 197-98, and Smith, supra note 125, at 77-78.

<sup>144.</sup> For examples see the Copyright Act, R.S.C. 1985, ch. C-42, § 42, as amended, 4th Supp., ch. 10, § 10; and the Patent Act, R.S.C. 1985, ch. P-4, §§ 74-78.

<sup>145.</sup> The protection under the Evidence Acts of Canada and Ontario does not apply to Anton Piller orders. At that stage the defendants are not witnesses giving oral evidence in court. Section 13 of the Charter protects witnesses who testify in any proceedings. There was some discussion of this in Apple Computer Inc. v. Minitronics of Canada Ltd., 19 C.P.R. (3d) 15, 35-36 (F.C.T.D. 1988).

<sup>146.</sup> Rank Film Distributors Ltd. v. Video Information Centre, 2 All E.R. 76 (H.L. 1981).

<sup>147.</sup> Supreme Court Act of 1981 (U.K.), ch. 54, § 72. For further discussion see Smith, supra note 125, at 80-81; Rock, supra note 125, at 205-207; Paciocco, Anton Piller Orders: Facing the Threat of the Privilege Against Self-Incrimination, 34 U. TORONTO L.J. 26 (1984).

#### G. USE OF THE ORDER

While Anton Piller orders are generally thought of as a form of pre-trial preservation of evidence, sometimes the execution of an order is dispositive of the dispute. The nature of the infringer or the market for particular items makes this so. For instance, "backroom" manufacturers generally have no substantive defence to an action, nor the resources to involve themselves in prolonged litigation. Once the order is executed, the plaintiffs have the necessary proof and that is the end of the case.

An Anton Piller order can be used effectively in a volatile market. Infringing articles can be seized to prevent much of the damage from occurring. This is important where the defendant is a "fly by night" infringer so that litigation, even if successful, often offers little hope of monetary recovery.

The very qualities that make the remedy effective, such as surprise and broad search powers, also leave room for great abuse. The procedural safeguards already discussed are in place to curb the possible abuse and should be stringently followed.

Aggressive tactics may result in punitive damages as they did in Columbia Pictures Industries Inc. v. Robinson.<sup>148</sup> Aggravated damages were awarded against plaintiffs even though the defendant was found to be a rogue, a pirate and a devious person. The plaintiffs established their case of copyright infringement, but, the judge found that the plaintiffs had acted oppressively in executing the Anton Piller order and had flagrantly disregarded the defendant's rights. Scott, J., found that the plaintiffs' principal motive was to close down the defendant and not to preserve evidence. The plaintiffs were ordered to pay £10,000 in damages, the main component of which was the aggravated damages.<sup>149</sup>

<sup>148. 3</sup> All E.R. 338 (Ch.D. 1986). See also Berryman, Anton Piller Injunctions Revisited: Columbia Pictures Industries Inc. v. Robinson, 3 I.P.J. 317 (1987.) Scott, J., was concerned by the abuse which may occur when executing Anton Piller orders. He set forth additional procedural guidelines which should be followed: (1) The order should not be broadly drafted, (2) A list of material should be taken by the solicitors executing the order before they leave the defendant's premises, (3) Material not covered by the order should not be removed, even with the defendant's "consent," (4) The material seized should be placed with a neutral party such as an officer of the court or given to the defendant's solicitors on their undertaking to provide safe custody and production, and (5) There should be full disclosure in the affidavits in support of the order. 3 All E.R. at 371-372.

<sup>149.</sup> The £10,000 included compensatory damages as well but only from the legitimate part of the defendant's business. Very little of his business was legitimate. Losses attributable to the sale or copying of other pirated videotapes not belonging to the plaintiffs could not be recovered. Scott, J., said that such an award would countenance an "application by the highwayman against his partner for an account." 3 All E.R. at 379.

# VIII. CONCLUSIONS

Computer technology may be protected in a number of ways. Considering the nature of this area, and the rapid advances in computer technology, it would appear the law has done rather well. Legislative and judicial initiatives have adapted intellectual property laws to deal with this new technology.

Depending on the circumstances, computer programs can secure copyright, patent, or trade secret protection. Hardware related inventions may be kept as trade secrets, or disclosed to the public in exchange for patent protection. Semiconductor chips are now entitled to their own unique protection.

Criminal and quasi-criminal sanctions are always lurking around as well. They may be invoked to curb criminal activity in both hardware and software matters.

Finally, Anton Piller orders now offer assistance in obtaining evidence to prove the infringement of intellectual property rights, particularly copyright.

While protection of software in many of these areas is available, the extent of the law's protection has not yet been defined. As with any intellectual property rights, the courts must balance the competing interests of the creator and the public. The creator, of course, desires strong protection to reward the time and money expended in developing the creation. The public interest, on the other hand, benefits from narrow protection allowing free competition. We must await future court decisions to see which interest the courts will favour in computer technology matters.