Canadian Journal of Law and Technology

Volume 3 | Number 2 Article 4

4-1-2004

EF Cultural Travel v. Explorica: The Protection of Confidential Commercial Information in the American and Canadian Contexts

Suzanne White

EF Cultural Travel v. Explorica: The Protection of Confidential Commercial Information in the American and Canadian Contexts

Suzanne White †

Commercial information, once relegated to paper files stored in cabinets, is now more likely to be in digital form, allowing a myriad of people to access its contents. These electronic storehouses can subsequently be stored on the Internet, providing a handy but somewhat risky means of archiving valuable information. The United States Court of Appeals (1st Circ.) judgment *EF Cultural Travel v. Explorica*[1] is a clear indicator of the way in which the advent of the Internet has completely changed the constructive meaning of the traditional "office file". This paper attempts to provide an understanding of the scope and potential impact on policy relating to confidential information and the use of Internet robots. In addition, this paper will provide an assessment of whether or not the same — or similar — facts of the *Explorica* decision could be successfully argued under all relevant and equivalent Canadian law relating to the protection of confidential commercial information.

The *Explorica* Case: An Assessment

The *Explorica* case involves the development and use of a computer "scraper" or "robot" to garner information on the Internet. "Scrapers" and "robots" are synonyms for software programs that go through a Web site and extract specific information. These programs are the basis for popular Internet search engines such as Yahoo![2] and Google.[3] In this case, the defendant, Explorica, used an Internet robot to glean pricing information from the plaintiff, EF Cultural Travel's Web site, and subsequently used the information to undercut EF's prices. *Explorica* is a case that centres on U.S. legislation, the *Computer Fraud and Abuse Act* (CFAA).[4] The instant case involves a challenge by the appellant defendant, Explorica, against a preliminary injunction by a district court that prohibited them from "scraping" information from EF's site. The *Explorica* case is a landmark decision not just for the jurisdiction of the United States, but for every other country trying to legislate in the area of the Internet and, more importantly, in the area of confidential corporate information and its protection.

The facts surrounding the case indicate a new threat to businesses that are increasingly engaging in in-depth Internet e-commerce or advertising. EF Cultural Travel is the world's largest private student travel organization, having been in business for over 35 years. In 2000, Explorica was formed to compete in the same market. The new company employed a number of former EF employees. This proves to be a crucial point in the Court's assessment of the case. Most notably, the former vice-president of information strategy at EF, Philip Gormley, now vice-president at Explorica, came up with the idea that Explorica's success could be bolstered by offering student travel tours at prices below those of EF, prices which were already competitive.

At issue was how to find out these prices. Gormley considered many ideas, including copy-typing information from EF brochures, scanning the same information, or manually searching for each tour listed on EF's Web site. In the end, Gormley requested that Zefer, Explorica's Internet consultant, design a "scraper" computer program that would efficiently gather all the pricing information from EF's Web site. Zefer accessed the information on EF's Web site by using tour codes that other Internet "scrapers" or "robots" would not have access to. The pricing information, which included 154,293 prices for EF tours, was subsequently used to undercut EF's prices.

In granting the preliminary injunction against Explorica, using the provisions of the CFAA, the District Court found that EF would likely be able to prove on the merits that Explorica had violated the CFAA in a manner outside of the "reasonable expectations" of EF. Secondly, the Court found that EF could show that it suffered loss, as required by the CFAA in order to get a remedy, due to reduced business, harm to its reputation as the world's largest provider of private student travel, and the cost of diagnosing any possible harm that had been done to the

†Articling Student, Carter & Associates, Orangeville, Ont.

EF computer systems despite that it was impossible to prove whether Explorica's actions caused actual physical damage to its computers.

The District Court pointed out a number of factors upon which it founded its presumption that EF's pricing was characterized as a corporate confidential information site (subsequently an infringement of s. 1030(4)(*a*) of the CFAA). The fact that there was a copyright symbol on one of the Web site pages, which included a contact e-mail address for informational purposes, was an indicator that EF was exercising control over the information provided on the Web site. Secondly, the Court found that the confidentiality agreement signed by Gormley, former vice-president at EF who became vice-president at Explorica, was likely violated by the instructions that Gormley gave to Zefer in order to create the scraper. Thirdly, it was evident that Explorica used means that bypassed the inherent technical restrictions that EF had put into place to prevent the collection of the tour price codes.

At trial on the merits, Justice Coffin explored the appellant Explorica's argument, among others, that the District Court mistook the breadth of the confidential agreement between Gormley and EF, and gave it a broader consideration than it merited. The confidentiality agreement read, in part that:

> Employee agrees to maintain in strict confidence and not to disclose to any third party, either orally or in writing, any Confidential or Proprietary Information … and never to at any time (i) directly or indirectly publish, disseminate or otherwise disclose, deliver or make available to anybody any Confidential or Proprietary Information or (ii) use such Confidential or [P]roprietary Information for Employee's own benefit or for the benefit of any other person or business entity other than EF.[5]

Coffin J. considered two e-mails that Gormley sent to Zefer which clearly indicated that Gormley was using the knowledge he acquired at EF to the benefit of Explorica: the e-mails not only indicated how to "scrape" the information from EF's Web site, but also the precise location to look for it. Furthermore, Explorica skirted the technical restraints placed on the Web site. In the end, however, the breach of confidentiality between Gormley and EF was the basis for relief. The District Court's decision was upheld, with the plaintiff EF awarded $21,000 in damages for the diagnostic procedures that the company underwent in assessing any possible damage to the EF Web server, an amount that met the $5,000 minimum damages requirement of the CFAA.

Legal Issues

The legal issues to be considered in this overview concern (a) the scope and potential impact of the *EF Cultural Travel v. Explorica* decision on policy relating to confidential information and the use of Internet robots; and (b) whether under the same or similar facts, the *EF Cultural Travel v. Explorica* decision could be successfully argued under all relevant and equivalent Canadian law relating to the protection of confidential commercial information.

Policy Considerations: After *Explorica*

The impact that the *Explorica* decision will have on policy relating to confidential information and the use of Internet robots will be significant for a number of reasons. In terms of confidential corporate information on the Internet, it is clear that the Internet offers the potential for both deliberate and inadvertent unauthorized disclosure of trade secrets.[6] This is because of the nature of the dissemination of trade secrets on the Internet. Trade secrets can be posted on company Web sites, transmitted by employees via e-mail to each other or to third parties, or posted by others who want to destroy the secrecy of the information.[7] At issue is whether or not a trade secret that has been posted to the Internet can still be considered secret.[8] There have been a series of American cases involving trade secret information procured from a branch of the Church of Scientology, which were considered by the Court to not have satisfied the elements of an action in breach of confidence. The Court held in one case that "despite the plaintiff's extraordinary measures to try to maintain the secrecy of its religious texts … it could not secure a trade secret preliminary injunction because it could not establish that the texts were 'not generally known' after they had been posted on the Internet by one or more individuals other than the defendant".[9] In a later case, the Court pointed out the grave concern it had with the impact of the Internet on intellectual property rights, stating that

> … one of the Internet's virtues, that it gives even the poorest individuals the power to publish to millions of readers, can also be a detriment to the value of intellectual property rights. The anonymous (or judgment proof) defendant can permanently destroy valuable trade secrets, leaving no one to hold liable for the misappropriation. Although a work posted to an Internet newsgroup remains accessible to the public for only a limited amount of time, once that trade secret has been released into the public domain there is no retrieving it.[10]

In the *Netcom* case, the Court found that Internet postings should usually be treated in the same manner as traditional mediums such as magazines and newspapers. However, it is clear that the question of whether posting trade secrets removes the secrecy characteristic of the information in question must be decided on a number of bases. There must be a consideration of the trade secret owner's interests and an acknowledgement of competition policies, which are to be favoured in order to stimulate business activity, among other issues.[11]

In *eBay Inc. v. Bidder's Edge Inc.*,[12] eBay, the plaintiff, allowed the defendant, Bidder's Edge to troll their site to glean information about which bid auctions they were offering. Bidder's Edge continued to use their trolling software after eBay asked them to stop, but eBay could not show harm to its server because of Bidder's Edge's activity. eBay argued its claim in trespass to

chattel, which was upheld, with the Court stating that the potential for diminution of the chattel is sufficient to make a trespass claim: all that has to be shown to start an action for trespass to chattel is an intermeddling or use without permission.[13] The *Explorica* decision is definitely in line with the *eBay* decision that protects corporate information as property.

In order for there to be protection of corporate information posted on Internet Web sites, the information itself must first be considered property. The September 16, 1999 issue of *The Economist* details another case of online auction provider eBay, which objected to the use of deep-linking to its sites by third party search sites, calling them "online parasites".[14] On the other hand, search site operators contend that the information posted on eBay's site is now part of the public domain. If the case goes to court, there could be a variety of intriguing outcomes. The courts could rule that copyright exists in data such as auction prices.[15] The springboard doctrine could apply in the sense that the search sites unfairly make money off of eBay because they use the information that eBay must collate and do not compensate eBay for the work it has done.

Moreover, a prohibition on the utilization of eBay's auction information could possibly reduce competition.[16] Bill C-23, which amended sections of the *Competition Act*,[17] was criticized as having too many gaps with respect to the confidentiality of provisions of international co-operation regime. This was the view given by the National Competition Law Section of the Canadian Bar Association in a release entitled "CBA Urges Better Protection for Confidential Information in Proposed Competition Law Amendments", which states that the Bill did not address the key issue of confidentiality held by the Competition Bureau.[18] It is evident, therefore, that confidentiality considerations will have to be made with an appreciation of worldwide business.

Explorica will have a definite influence on the nature of the employer-employee relationship, before, during, and after employment. The protection of corporate confidential information existed long before the advent of modern technology, but along with the convenience of electronic information storage exists the possibility that infinite copies can be created, disseminated and used against the employer's core business interests. Nortel Networks addresses this problem in its "Living Commitment No. 5", entitled "Protecting Assets".[19] Nortel advances the idea of "collective responsibility" within the corporation for the protection of corporate data. The Commitment states that "theft, carelessness, and unnecessary waste have a direct impact on the corporation's profitability, and ultimately, on all of our jobs".[20] Nortel goes on to state the premise upon which businesses can make incredible margins of profit, or sink into bankruptcy: "information is a key corporate asset".[21] The Nortel statement on Protecting Assets is a clear example of how critical it is for companies to hire the right people. If business or technical information is inadvertently or deliberately released to third parties, the information could be used to seriously undercut pricing, and to allow competitors to "springboard" ahead of Nortel by avoiding research and development obligations in order to create their own product.[22] By this statement, Nortel seems to acknowledge that once the trade secrets are out of their domain, the information is open to being collected and exploited by third parties; thus, its secrecy must be given the utmost protection. Nortel focuses on employees that may have access to "proprietary and confidential information — which may range from engineering designs, to employee records, to data entrusted to us by a customer or competitor".[23] These employees must be careful not to talk about company business in public, including restaurants, airplanes, or public pay phones.[24] The company's reputation, including that of its employees and of its products, is at stake in the event of disclosure of confidential information.[25] Finally, Nortel Networks reminds its employees that

> … our obligation to protect Nortel Networks' proprietary and confidential information continues even after we leave the company.[26]

The Commitment does not clearly indicate whether or not Nortel employees have to sign a confidentiality agreement, but the reminder speaks volumes in terms of the expectations Nortel has of its employees, even when they are no longer working under Nortel. The type of information that Nortel has, a large percentage of which is technical electronic information, indicates the type of work a large number of the employees engage in. Once these persons leave, they will most likely work in the same field, but can only do so without using any of Nortel's information to their employment advantage. Employees are increasingly mobile, and protection of the intellectual property rights in corporate information is becoming increasingly challenging.[27] The flow of technology is very difficult to gauge with such high turnover.

Employees and former employees can have a tremendous influence on the quality of data held by corporations. Although corporations like Nortel take significant steps to protect corporate information, such as the construction of Intranets (which are the internal networks that connect everyone in the company and keep third parties out), employees cannot be monitored once they log off their PC for the day or when they leave the company for good. These employees can provide a wealth of information that can be translated into business intelligence, information that can be used by competitors in the market.[28] The *Explorica* decision can also extend to other areas of information technology, including those used by corporations to advertise, to inform their clients and/or employees of events, and to display new pricing and products. E-mail is another way in which corporate confidential information can be

compromised because, like Web sites, e-mail has become subject to a number of programs dedicated to breaking its encryption and exposing information intended only for the recipient.

In *Guillot v. Istek Corp*,[29] a Canadian case decided in July 2001, the Court declined to issue an injunction to force certain material off the Web, even though it may have been copied. The Court held "that material freely posted on the Internet may include an implied licence to make copies for personal use".[30] With respect to the use of Internet robots, *Explorica* makes a strong statement against the use of Internet robots, but only in the context of garnering information that has been clearly digitized or encrypted in such a way that others should not access it. Internet robots are an integral part of the Internet, without which most of the information on the Internet would not be accessible for legitimate purposes. Robots,[31] which are software programs, are responsible for gathering information for Web search engines that index the information for Web surfers. Information can also be gathered for Internet marketing by compiling statistics on, for example, the effectiveness of a particular Web site or campaign.[32] Unfortunately, the incredible assistance in Internet research that robots provide is marred when they are used for purposes contrary to proper Internet decorum (also known as "Netiquette"), or even for the purposes of an illegal act. These specialized robots work 24 hours a day,[33] and therefore can collect a vast amount of information in a relatively short period of time if compared to similar work done by a sole Internet researcher. Robots can search every area of the Internet, picking up e-mail addresses, information about Web sites, and the like.

The *Explorica* decision brought to light the problems that Internet robots can cause to a host Web site if allowed to target a specific site to garner a substantial amount of data. Alicia Riddell's article "Internet Robots: What Do They Have to Do With Libraries?",[34] demonstrates that Internet robots can cause a host of problems. Too many requests to the server can result in server overload, causing service slowdown for others accessing the site.[35] Related to the first problem is network overload, as robots use up a considerable amount of bandwidth.[36] For these reasons, and many others, The Robots Exclusion Protocol,[37] a way in which server administrators can tell if a robot is wanted or not at that server, was developed in 1994. This can disallow access to a site by adding the names of the robot to a file called *robot.txt*.[38] However, in the end, the benefits of Internet robots significantly outweigh the means of how robots search the Web. If properly manipulated, Internet robots are the most effective way of indexing information found on the Web, and can actually reduce traffic on the Web by lowering the amount of casual browsing and lowering the amount of time a site is visited by one user.[39]

The proliferation of unsolicited e-mail, or spam, can be characterized as another means by which commercial computer databases can be compromised. Every day, millions of unsolicited e-mail messages are received by countless Internet users, taking up space in their e-mail boxes, consuming their time in separating the unwanted messages from their desired communications, and sometimes offending Internet users with their content. The American case of *CompuServe Inc. v. Cyber Promotions*[40] dealt specifically with the right of an online computer service to block unsolicited commercial e-mail from being delivered to its subscribers. In *CompuServe*, CompuServe Inc. sought a preliminary injunction against Cyber Promotions in order to restrain it from sending commercial e-mail advertisements to its users. The defendant Cyber Promotions had used CompuServe accounts as one method of sending what it called "bulk e-mail" to CompuServe users, leading them to believe that the e-mail messages were being sent by CompuServe itself. The Court stated that Cyber Promotions' actions were a trespass to CompuServe's chattel, its computers and computer services, as the number of spam e-mail messages received by CompuServe to deliver to its users compromised the operation of its computer systems and storage capacity for legitimate e-mails. As such, the preliminary injunction against Cyber Promotions was granted. The *CompuServe* case is instructive in that it treats computers as property or chattels, and e-mail messaging, electronic bytes of information whizzing through cyberspace, as a method by which trespass can be effected.

Protection of Corporate Confidential Information in the Canadian Context

There are a number of Canadian statutes that deal with the protection of information, but this is limited to the way in which government agencies handle personal information.[41] There is currently no legislation that specifically governs the protection of corporate confidential information. However, the Canadian *Criminal Code*,[42] section 342.1, criminalizes the unauthorized use of a computer:

> **342.1.** (1) Every one who, fraudulently and without colour of right,
>
> (a) obtains, directly or indirectly, any computer service,
>
> (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,
>
> (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (*a*) or (*b*) or an offence under section 430 in relation to data or a computer system, or
>
> (d) uses, possesses, traffics in or permits another person to have access to a computer password that would

> enable a person to commit an offence under paragraph (*a*), (*b*) or (*c*)
>
> is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

Unauthorized use of a computer is punishable by a maximum 10-year imprisonment term. Subsection 342.2(1) also prohibits the manufacture, possession, sale, offering for sale, or distribution of any device that makes the unauthorized use of a computer as described in subsection 342.1(1) possible, an offence punishable by up to two years' imprisonment under paragraph 342.2(1)(*a*).

Subsection 430 (1.1) further criminalizes mischief in relation to data:

> (1.1) Every one commits mischief who wilfully
>
> (a) destroys or alters data;
>
> (b) renders data meaningless, useless or ineffective;
>
> (c) obstructs, interrupts or interferes with the lawful use of data; or
>
> (d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

This is an offence that can carry a maximum imprisonment term of five years if an individual is found guilty of an indictable offence under subsection 430(5). Both the unauthorized use of a computer and the mischief in relation to data are hybrid offences which can be punishable on summary convictions as well.

The necessary elements of the cause of action for breach of confidence are derived from *Coco v. A.N. Clark*, a British case.[43] These elements include (a) that the information conveyed was confidential, (b) that it was communicated in confidence, and (c) that it was misused by the party to whom it was communicated, as it was restated in *Lac Minerals Ltd. v. International Corona Ltd.*,[44] the first Supreme Court of Canada case to apply the three-pronged *Coco v. Clark* test.

The "springboard doctrine", first articulated in *Terrapin Ltd. v. Builders' Supply Co. (Hayes) Ltd.*,[45] states 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 …[46]

The springboard doctrine would be applicable in scenarios where, for example, products cannot be reverse-engineered by the defendant, so the defendant utilizes confidential information. In this case, the issue would be whether or not the law should allow the use of information used in a breach of confidence to the benefit of the defendant. Another instance in which the springboard principle would apply would be where products can be reverse-engineered, but where the defendant uses the plaintiff's information as a means of efficiency. In this instance, it is likely that the court would find that the defendant was not entitled to use information acquired by the plaintiff as a springboard to enter into competition. The springboard principle is useful in the protection of the plaintiff's investment of time, money, and research for the acquisition of valuable information to be used as a force in their respective market.

The English Court of Appeal case, *Faccenda Chicken Ltd. v. Fowler*,[47] has been applied by Canadian courts in the context of the use of company information by a former employee. At the trial level of this case, the judge created three categories of information. Category 1 information includes trivial, public information that reasonable persons would not consider to be confidential. In this situation, an employee is free to use and disclose the information at any time during and after employment.[48] Category 2 information describes when the employee was either expressly told information is confidential or when it is obviously confidential due to its very nature, and includes "know-how". An employee is bound to maintain the confidentiality during the course of employment but can use or disclose once employment ceases unless expressly bound by a non-competition/restrictive covenant, which must be reasonable in time and space.[49] Finally, Category 3 information includes trade secrets, which an employee can *never* use or disclose during or after employment regardless of whether expressly bound by non-competition clause or restrictive covenants.[50] In *Faccenda Chicken*, Fowler, a former employee of a mobile refrigerated chicken enterprise, started his own business, employing eight Faccenda employees, including a supervisor, five van salesmen, and two others who worked in Faccenda's office. None of the employees was bound by a restrictive covenant, so the plaintiff employer had to argue that the confidential information was a trade secret, according to the Category 3 classification of information that is not protected by a restrictive covenant. The use of Faccenda's sales information was at issue, since Fowler used route information, client names and addresses, among other data, in order to boost his business.[51]

Faccenda's claim was dismissed, as the sales information was not found to be a trade secret:

> We are satisfied that, in the light of all the matters set out by the judge in his judgment, neither the sales information as a whole nor the information about prices looked at by itself fell within the class of confidential information which an employee is bound by an implied term of his contract of employment or otherwise not to use or disclose after his employment has come to an end.[52]

Canadian and British case law does indicate, however, that the courts will find former employees liable for breach of confidence actions in circumstances where the former employee held a certain position of authority.

In the case of *Quantum Management Services Ltd. v. Hann*,[53] two employees who were placement coordinators at an employment placement agency left to form their own agency, Pinstripe. They were not senior officers, nor were they directors. The defendants, Hann

and Taaffe, were very successful in their work, having been the top two employees at Quantum. The Court found that these former employees owed a fiduciary obligation to the corporation, not because they were senior officers but because they were senior employees. The Court considered the fact that the majority of Pinstripe's new clients were from Quantum, since Hann had memorized the information in the client database. The Court held that:

> While acknowledging that Hann and Taaffe were not "top management" in the general sense of that expression, I am, nevertheless, satisfied that they were senior employees in relation to their exclusive clients — no other employees could deal with Hann's or Taaffe's clients … Therefore, both Hann and Taaffe had a duty not to solicit or deal with former customers of Quantum with whom they had exclusive placement rights within a reasonable time before quitting Quantum's employ.[54]

It is clear from this case that senior officers and senior employees are prohibited from using information from their former employer's business to the employer's detriment, and that a former employer can be successful in an action for breach of confidence against senior employees.

In *McCormick Delisle & Thompson Inc. v. Ballantyne*,[55] an Ontario Superior Court judgment, management consultants previously employed by McCormick Delisle left to form their own consulting firm. The Court here held that:

> It is, however, quite clear, even from the general evidence which was adduced on the liability issue, that the consequences of the defendant's conduct to the plaintiff was almost disastrous and the benefit to the defendants was substantial. This is, in my view, one of the clearest cases of unfair competition by departing employees.[56]

The plaintiff employer suffered loss from the defendant Ballantyne and two other employees who lured away client relationships that took a long time to nurture and maintain. An issue that has been addressed at common law is that of the categorization of information. In *Matrox Electronic Systems Ltd. v. Gaudreau*,[57] the Court addressed this issue by stating that:

> The problem with respect to scientific and technical information is especially difficult, because the more information with business value approaches "pure science", the more persuasive the claim becomes that it is part of the public domain, and thus properly regarded as part of the intellectual equipment of the employee as a research scientist or engineer rather than information pertaining particularly to the employer's business.[58]

In awarding a remedy to the former employer, the Court stated that:

> In the present case, it is the Court's opinion that the predetermined period of protection (two years from the date each individual Defendant ceased working for Plaintiff) available under the springboard principle has expired and Plaintiff is not entitled to extend its "private obligations" into a "public duty". Plaintiff's remedy will be limited to damages.[59]

At common law, the general principle is that restraint of trade contracts are *prima facie* void because every person should be allowed to exercise any lawful trade. However, a restrictive covenant that meets the three conditions outlined in *Jiffy Foods Ltd. v. Chomski*[60] will be upheld so as to protect the covenantee. This includes meeting the three conditions of being (a) reasonable, (b) founded on good consideration, and (c) not too vague.[61] In short, in Canada, there is protection for confidential corporate information under the action of breach of confidence, regardless of whether there exists a restrictive covenant prohibiting the disclosure of the information. However, it is clear that the requirements of both *Coco v. Clark* and *Faccenda Chicken* must be met in order for a breach of confidence action to be made out in an employment relationship, and that any existing restrictive covenant be reasonable in order to be enforced.

Canadian Breach of Confidence Law as Applied to *Explorica*

Could the *Explorica* case be successfully argued under all relevant and equivalent Canadian law relating to the protection of confidential commercial information? Beginning with the *Coco v. Clark* test, which requires that information must be confidential, that there must be an obligation of confidence, and that there must be unauthorized use to the detriment of the plaintiff, it is highly probable that *Explorica*, if argued in Canada, would satisfy these requirements. Firstly, the information has the necessary quality of confidence because although the information, in its numerical format, was in the public forum, the information garnered by Explorica was in the rough code form that only EF should have known how to decipher. Secondly, there was an obligation of confidence on Gormley, the former vice-president of EF, not to disclose any of the confidential information that he learned while at EF, as was stipulated in the confidentiality agreement he signed while an employee. Finally, the use of EF's pricing information was unauthorized because its collection went beyond the restraints of EF's Web site and was subsequently used to undermine their force in the private student travel industry.

Faccenda Chicken provides three categorizations of information with respect to its use after employment ceases. Category 3 information includes trade secrets, which an employee can never use or disclose during or after employment, whether or not a non-competition clause exists. EF's pricing information code is a trade secret, because whether or not Gormley had signed the confidentiality agreement, it is obvious that EF would not want this information to be disclosed because such disclosure would hurt its interests.

The *Terrapin* springboard doctrine is utilized to prevent a confidant from unfairly profiting from the efforts of another company. Explorica's "scraping" of pricing information from EF's Web site gave Explorica the opportunity to get pricing information on student travel tours in a manner hundreds of times faster than

manually going through the drop-down menus on the EF site. Therefore, EF's pricing information and its collection by Explorica would merit injunctive relief against its use because (a) there was an alternate method by which Explorica could have acquired the information (i.e., by the normal manual method or by using printed materials published by EF on its tours), and because (b) Explorica used the information to specifically undercut EF's long-established prices in the industry. Although it may be argued that the springboard doctrine promotes anti-competitiveness, the springboard doctrine is actually a means of promoting fair competition in any given industry.

With respect to the confidentiality agreement signed by Gormley, the covenant must meet the requirements set out in *Jiffy Foods*. In a Canadian court, it is likely that the covenant would be upheld for the following reasons. The covenant was reasonable because Gormley entered into the agreement voluntarily, knowing that it was broad in the sense that he could not disclose anything that might hurt the interests of EF. Moreover, the covenant was founded on good consideration, since Gormley could still work in the student travel industry field, as long as he did not unfairly prejudice EF's position in the market. Finally, the covenant was not too vague. It was explicit and gave a precise definition of what types of information were not to be disclosed.

It is clear in reviewing the Canadian *Criminal Code* that individuals and businesses will be able to find some relief not only through civil litigation court proceedings, but also through *Criminal Code* protections. With the threat of imprisonment ranging from 2 to 10 years, depending on the offence, those who would attempt to interfere with and/or jeopardize another's Web site have had to consider these stiff possible consequences since 1997, when the first anti-computer interference provision came into force in the *Criminal Code*. The "unauthorized use of a computer" offence in subsection 342.1(1) can clearly be analogized to the actions of obtaining information from EF Cultural Travel's Web site, basically indirectly intercepting the information storage function of EF Cultural Travel's Web site. Further, Explorica would be in contravention of subsection 342.2(1) of the *Criminal Code* in that it possessed a device, namely the "robot scraper", that enabled it to access without authorization and to fraudulently use EF Cultural Travel's Web site. Finally, Explorica may or may not have been considered in contravention of subsection 430(1.1), "mischief in relation to data", since it did not obstruct EF Cultural Travel's lawful access to its data. However, the garnering and reuse of EF Cultural Travel's travel information rendered it ineffective in terms of its business competitiveness.

Conclusion

The *Explorica* decision holds a number of implications for Canadian corporations that engage in electronic commerce and other activities that utilize the Internet. One commentator writes that

> … it has become increasingly important for commercial lawyers to be acutely aware of intellectual property issues. These arise not only in connection with the building of patent portfolios … but are becoming much more the "stuff" of day-to-day commerce.[62]

The Internet is, for the most part, a wonderful tool for the marketing of products and advertising. Although the information posted on a Web site is open to the viewing of all who happen upon it, there is clearly a legal limit to how much information can actually be taken from the Web site and then used. The *Explorica* case sets a precedent in favour of protecting corporate information, but corporations should be advised that they must take care in the selection of employees. Eighty per cent of security attacks are internal,[63] so what is disclosed to employees is crucial for data security. Corporations must also create reasonable restrictive covenants that will be upheld in court in the event of an alleged breach of confidence. The possibilities of accessing information, even if it is in the form of electronic "gibberish", are greater today than ever before, and Canadian corporations must be aware of this. Although a preliminary injunction can be sought, even a few days of undercutting prices can be extremely damaging to a corporation.

Explorica's legal ramifications can also affect Canadian corporations internationally. In the pursuit of corporate "rainmakers", foreigners who have an expertise in an area coveted in the Canadian market can often be lured from one corporation to another. Does this mean that the information that they have garnered over the years at their previous place of employment, which is what makes them "gold", cannot be disclosed? It may also be in the best interest of corporations to implement a strong policy of internal hierarchical disclosure, so that only the most senior employees are entrusted with the information and so that these employees must sign the broadest confidentiality agreements possible. In light of recent global experiences with computer viruses such as the "Sasser" worm, "Lovebug", and "My Doom", it is obvious that it is not always possible to protect computer systems and data, but in the event that these portals of information are compromised, there is a growing precedent towards respecting the integrity of commercial information.

Notes:

[1] 274 F.3d 577 (1st Cir. (Mass.) [hereinafter *Explorica*].

[2] For more information please see: http://www.yahoo.ca.

[3] For more information please see: http://www.google.ca.

[4] 18 U.S.C. s. 1030 [hereinafter CFAA].

[5] *Supra* note 1 at 582.

[6] *Milgrim on Trade Secrets*/Vol 4: Chapter 17 Intellectual Property and the Internet * /§ 17.03 Trade Secrets and the Internet, *available at* http://www.bender.com.

[7] *Ibid.*

[8] *Ibid.*

[9] *Ibid.*

[10] *Ibid.*

[11] *Ibid.*

[12] (2000) 100 F. Supp. 2d 1058 [hereinafter *eBay*].

[13] *Ibid.*

[14] *The Economist* (16 September 1999), p. 118.

[15] *Ibid.*

[16] *Ibid.*

[17] R.S. 1985, c. C-34.

[18] "CBA Urges Better Protection for Confidential Information in Proposed Competition Law Amendments". The Information Service of the Canadian Bar Association, *available at* http://www.cba.org/News/Releases/2001_releases/2001-10-23_comp.asp (last accessed: 20 May 2004).

[19] "Protecting Assets". Nortel Networks Web site, *available at* http://www.nortelworks.com/corporate/community/ethics/living5.html (last accessed: 15 March 2002).

[20] *Ibid.*

[21] *Ibid.*

[22] *Ibid.*

[23] *Ibid.*

[24] *Ibid.*

[25] *Ibid.*

[26] *Ibid.*

[27] Richard A. Brait, "Commercial Law in the Age of the Internet." (1999) 48 UNB LJ 243 at 244.

[28] Rene Lewandowski, "Corporate Confidential: the new information professionals". *Financial Post* (March 1999): *available at* http://www.competia.com/home/art8.html (last accessed: 15 March 2002).

[29] *Guillot v. Istek Corp* [2001] F.C.J. No. 1165 [hereinafter *Istek*].

[30] *Ibid.* at para 7.

[31] For a list of Internet Robots, please see: "A (VERY) Brief List of Robots, Wanderers and Searchers". UNB Saint John Ward Chipman Library, *available at* http://www.unbsj.ca/library/research/robots1.htm (last accessed: 20 May 2004) and John December, "New Spiders Roam the Web". *Computer Mediated Communication Magazine* 1.5 (1994): *available at* http://sunsite.unc.edu/cmc/mag/1994/sep/spiders.html (last accessed: 20 May 2004).

[32] "What does Spam Emails and Robots have in common?" The Internet Centre. (31 March 2001): *available at* http://www.incentre.net/incentre/frame/news/2001Mar31.html (last accessed: 20 May 2004).

[33] *Ibid.*

[34] Alicia Riddell, "Internet Robots: What Do They Have to Do With Libraries?" University of Alberta, School of Library and Information Studies (March 1997): *available at* http://www.slis.ualberta.ca/598/alicia/robhtm.htm (last accessed: 8 March 2002).

[35] *Ibid.*

[36] *Ibid.*

[37] *Ibid.*

[38] *Ibid.*

[39] *Ibid.*

[40] (1997) 962 F. Supp. 1015 (U.S. Dist. – Southern Ohio) [hereinafter *Compuserve*].

[41] *Privacy Act*, R.S. 1985, c. P-21, *Personal Information Protection and Electronic Documents Act*, 2000, c. 5; *Access to Information Act*, R.S.C 1985, c. A-1.

[42] *Criminal Code*, R.S. 1985, c. C-46.

[43] [1969] R.P.C. 41 (Ch.) [hereinafter *Coco* v. *Clark*].

[44] [1989] 2 S.C.R. 574 [hereinafter *Lac Minerals*].

[45] (1960), 5 R.P.C. 128 (C.A.) [hereinafter *Terrapin*].

[46] *Ibid.*

[47] (1985), [1986] 1 All E.R. 617, [1986] 3 WLR 288 (C.A.) [hereinafter *Faccenda Chicken*].

[48] *Ibid.*

[49] *Ibid.*

[50] *Ibid.*

[51] *Ibid.*

[52] *Ibid.*

[53] [1992] O.J. No. 2393 (Ont. Sup. Ct) [hereinafter *Quantum*].

[54] *Ibid.*

[55] [1999] O.J. No. 5654 (Ont. Sup. Ct.) [hereinafter *McCormick Delisle*].

[56] *Ibid.* at para 45.

[57] [1993] Q.J. No. 1228 (Q. Ct) [hereinafter *Matrox*].

[58] *Ibid.* at para 72.

[59] *Ibid.* at para 107.

[60] [1973] O.J. No. 271 (C.A.) [hereinafter *Jiffy Foods*].

[61] *Ibid.*

[62] *Supra* note 27 at 248.

[63] Stephanie Perrin, "The Limits of Privacy" (Censorship and Privacy: Civil Liberties in a Digital Age, Faculty of Law, University of Toronto, 25 January 2002) [unpublished].