Chicago-Kent Journal of Intellectual Property

Volume 13 | Issue 1 Article 8

9-1-2013

Canada's Inadequate Legal Protection Against Industrial Espionage

Emir Crowne

Tasha De Freitas

CANADA'S INADEQUATE LEGAL PROTECTION AGAINST INDUSTRIAL ESPIONAGE

Emir Crowne[*] *& Tasha De Freitas*[**]

ABSTRACT

Canadian law provides little protection for individuals and corporations against industrial espionage. Akin to the United States' Economic Espionage Act of 1996—with its broad definition of "trade secret" and accompanying protections and remedies—we propose that Canada enact legislation at the federal level to remedy many of the deficiencies that arise in bringing a claim under the usual breach of confidence action.

INTRODUCTION

Canadian law provides little protection for individuals and corporations against the very real threat and damage of industrial espionage. What is required is a federal law that captures both the actions of individual wrongdoers and of the corporations or companies that induced these individuals to commit those acts. A federal criminal law with heavy penalties would help balance the power differential in cases of a mammoth corporation preying upon a small company and would help provide the necessary deterrence that current Canadian law lacks. By protecting confidential information, particularly trade secrets, not only would Canada send a strong message to those tempted to participate in industrial espionage, but Canada would finally begin to live up to its international obligations to provide ample protection of intellectual property. The United States' Economic Espionage Act of 1996[1] and the extensive protection it provides for proprietary confidential information, by virtue of its broad definition of a "trade secret," addresses many of the Canadian judiciary's concerns relating to the criminalization of the theft of confidential information. A criminal law would also overcome many of the problems inherent in the use of tort law, which provides the primary protection of confidential information under Canadian law.

This Article examines the little protection current Canadian law provides against industrial espionage and how implementing something akin to the

---

 Associate Professor, University of Windsor, Faculty of Law, Barrister & Solicitor, Law Society of Upper Canada.

 Associate, Perry + Currier Inc.; Currier + Kao LLP.

[1] Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–1839 (West 2012).

United States' Economic Espionage Act of 1996 would prove beneficial to Canada. Part I provides background information about industrial espionage. Next, Part II discusses Canadian law and how it fails to adequately protect against the threat of industrial espionage. Part III then examines steps the United States has taken to combat industrial espionage. Finally, Part IV discusses Canada's international obligation to afford better protection to those vulnerable to industrial espionage.

I. BACKGROUND: INDUSTRIAL ESPIONAGE EXPLAINED

Industrial espionage, defined as one company spying on another to steal trade secrets or other proprietary information,[2] has a tremendous impact on the Canadian economy. Examples of proprietary information include: client lists, internal pricing schemes, investment strategies, technical schematics, blueprints, source code, and contract bid submission/tenders.[3] There is not a single statutory or common law definition of a "trade secret," but article 1711 of the North American Free Trade Agreement Between the Government of Canada, the Government of Mexico and the Government of the United States[4] provides a generally accepted definition of a "trade secret." For the purposes of this paper, trade secrets will be treated as a subset of confidential information, and "confidential information" will also include information that relates to non-technical matters such as business plans or pricing information.[5]

Industrial espionage can take place in a variety of circumstances and occurs for many different reasons. Apart from searching through a competitor's garbage and electronically accessing or compiling a competitor's secrets, confidential information may be exposed and obtained in the course of mergers and acquisitions, joint ventures and alliances, licensing relationships, and employment relationships, as well as through the use of consultants and advisors.[6] Acquiring the confidential information of a competitor can enable the perpetrator to undercut their competition by giving them a head start they would

---

[2] *Industrial Espionage*, BLACK'S LAW DICTIONARY 585 (8th ed. 2004).

[3] Oxana Iatsyk & Shelagh Carnegie, Knowing Your Enemy – Managing External Forces, Address at the Ontario Bar Association 2006 Institute of Continuing Legal Education: Corporate Counsel: Keeping Secrets Secret – Battling Industrial Espionage (Jan. 24, 2006).

[4] North American Free Trade Agreement, U.S.-Can.-Mex., art. 1711(1)(a), Dec. 17, 1992, 32 I.L.M. 289 (1993) [hereinafter NAFTA].

[5] Edward T. Fan, *Canada: Protection of Trade Secrets and Confidential Information*, MONDAQ (last updated June 4, 2008), http://www.mondaq.com/canada/x/61178/Trade+Secrets/Protection+Of+Trade+Secrets+And+Confidential+Information.

[6] Bruce N. McWilliam, Protecting Your Confidential Information & Trade Secrets, Address to the Ontario Bar Association 2006 Institute of Continuing Legal Education: Corporate Counsel: Keeping Secrets Secret – Battling Industrial Espionage (Jan. 24, 2006) (presentation on file with the Chicago-Kent Journal of Intellectual Property).

not have had but for the unauthorized use of the confidential information. This activity is also known as "spring-boarding."[7] Industrial espionage can also be conducted for personal profit. Information brokers are contractors who scour the world for proprietary information, using both legal and illegal means, and sell such information to interested clients.[8]

Although exact dollar figures are difficult to determine, in 1996 the Canadian Security Intelligence Service (CSIS) estimated the cost of industrial espionage to be approximately $1 billion per month CDN, and, as of 2006, that figure has likely increased due to improvements in communications technology and the increasingly global nature of the Canadian economy.[9]

II. ANALYSIS OF CANADIAN LEGAL APPROACHES TO INDUSTRIAL ESPIONAGE

This section examines how criminal law and tort law in Canada deal with industrial espionage. In analyzing those sources of law, we conclude that each fails to adequately protect individuals and corporations against industrial espionage.

A. Canadian Criminal Law: Current Law and Analysis

The Canadian Criminal Code affords victims of industrial espionage little protection. Strangely, the courts have prohibited the application of provisions like theft and fraud, which would appear to capture the nature of the act. The few provisions that could be used to prosecute the unauthorized taking of confidential information, such as the unauthorized use of a computer (section 342.1[10]), are so limited in scope that, at best, they would only capture the activities of the individual actors and not the companies or corporations that may have induced them to commit such crimes.

In *R. v. Stewart*, the court found that the theft provisions in the Criminal Code could not apply to the unauthorized taking of confidential information itself because: (i) confidential information was not property under section 322(1);[11] (ii) confidentiality in and of itself does not impart an interest of which

---

[7] Cadbury Schweppes Inc. v. FBI Foods Ltd., [2000] F.S.R. 491, para. 67 (Can.) (WL); *see also* Terrapin Ltd. v. Builders' Supply Co. (Hayes), [1967] R.P.C. 375, 371 (Eng.); Coco v. A.N. Clark (Eng'rs.) Ltd., [1968] F.S.R. 415, 421 (Ch. D.) (WL).

[8] OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., ANNUAL REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE—2005 (Aug. 2006), *available at* http://www.ncix.gov/publications/reports/fecie_all/FECIE_2005.pdf.

[9] Andrew Jones, *Industrial Espionage in a Hi-Tech World*, 2008 COMPUTER FRAUD AND SECURITY 7, (Jan. 2008) (citing Derek Quinn, *Industrial Espionage*, RADIO CAN. INT'L (Sept. 5, 2006)).

[10] Criminal Code, R.S.C. 1985, c. C-46, s. 342.1 (Can.).

[11] *Id.* s. 322(1); R. v. Stewart, [1988] 1 S.C.R. 963, para. 33 (Can.).

the owner or source of the information could be deprived;[12] (iii) there is not a precise definition of the term "confidential information";[13] and (iv) finding that confidential information is property may have far reaching ramifications.[14] In light of these concerns, the court held that it was not the place of the judiciary to make a finding that confidential information is property under the Criminal Code and deferred to Parliament to make such a determination.[15]

According to the court, the subject of the theft must be something capable of ownership.[16] It must be property "capable of being taken or converted in a manner that results in the deprivation of the victim."[17] The court reasoned that in order for something to be stolen, it must belong to someone and "one cannot be deprived of confidentiality, because one cannot own confidentiality."[18] As an intangible, information could only qualify under the provision if it was capable of being converted.[19] Because conversion requires the act of interference, it must deprive the owner of the *use* and *possession* of the chattel, and, in the case of confidential information, because the alleged owner is not deprived of the information in this sense, it cannot be the subject of theft.[20] While confidentiality may impart some value to the information, the court found that this did not merit conferring a special property or interest in it to anyone.[21]

The court also found that deeming confidential information property under the Criminal Code would have far-reaching implications.[22] The criminal law is designed to prevent wrongs against society as a whole.[23] In situations in which society might benefit from the public release or greater accessibility to such information, the court found that characterizing confidential information as property would likely undermine this purpose.[24] If confidential information was considered property under the Criminal Code, it may capture "innocent" activity and indirectly restrict the movement of labor.[25] It may also unexpectedly trigger criminal responsibility.[26] The court reasoned that a person having committed "theft" of confidential information might be charged under other provisions of

---

[12] *Stewart*, [1988] 1 S.C.R. 963 at para. 38.
[13] *Id.* at para. 31.
[14] *Id.* at para. 30.
[15] *See id.* at para. 33.
[16] *Id.* at para. 21.
[17] *Id.*
[18] *Id.* at para. 37.
[19] *Id.* at para. 34.
[20] *Id.* at para. 35.
[21] *See id.*
[22] *See id.* at paras. 28–32.
[23] *Id.* at para. 28.
[24] *Id.*
[25] *Id.* at paras. 29–30.
[26] *See id.* at para. 27.

the Criminal Code for acts they might not have any control over.[27] For example, if a person could not forget the information, they could be prosecuted under section 354 (possession of property obtained by crime). Despite these drawbacks, we propose that confidential information should be—and already is—covered under the Criminal Code.[28]

Confidential information should qualify under the theft provisions of the Criminal Code. Section 322 allows the subject of theft to be "anything."[29] If Parliament wanted to restrict the definition of "anything" to cover only property, then it likely would have defined this in the legislation. Even if the subject of theft must be property, confidential information has the key characteristic of property—it is capable of being owned. Ownership of confidential information, like patents and other recognized forms of intellectual property, is about the use of ideas to the exclusion of others unless permitted by the owner or originator of the information.[30] The value of confidential information resides, at least partially, in the ability of the owner to control how, when, and to whom such information is released, and this value must be recognized by the courts. It is also important to note that section 322 does not require that the interest be proprietary, but merely *special*.[31] Why would the economic interest derived from the value of the confidentiality of the information not suffice?

A finding that confidential information is property under the Criminal Code would be in keeping with one of the primary goals of Canadian criminal law—to benefit society as a whole. Under Canadian patent law, patent protection of an idea arises when the patent application is filed, but the development of the idea usually takes place well in advance of that application. In order to obtain a patent, the idea must be novel, and this novelty is based on the invention's similarity to those claimed in prior filed applications.[32] If Party *A* is able to obtain critical design or test data ahead of Party *B*, but Party *B* acquires Party *A*'s design or test data and files an application first, Party *B* will gain patent protection to the detriment of Party *A*. Another critical issue arises when a competitor obtains a confidential list of investors and uses that list to interfere with funding crucial to the development of another party's idea. If competitors are allowed to interfere in the crucial development stages of projects that may have led to great benefit for society as a whole (e.g., medicines), then there is little incentive for scientists and inventors to pursue such noble causes. Therefore, providing protection for confidential information as property under

---

[27] *Id.*

[28] Criminal Code, R.S.C. 1985, c. C-46, s. 354 (Can.); *Stewart*, [1988] 1 S.C.R. 963 at para. 27.

[29] Criminal Code s. 322(1).

[30] *See generally* Endplex Invs. v. Derrydale Golf Course Ltd., 2008 CanLII 49330 (Can. Ont. S.C.).

[31] Criminal Code s. 322(1)(a).

[32] *See* Patent Act, R.S.C. 1985, c P-4, s. 28.2(1) (Can.).

the Criminal Code would encourage scientists and inventors to pursue such ideas with confidence that their ideas and information is protected.

Similarly, the court in *Stewart* found that it was unlikely that the taking of confidential information would qualify as fraud.[33] Based on findings that confidential information was not property, the court found that the necessary element of deprivation could not be met.[34] As the hotel was not defrauded of any money or economic advantage and only stood to lose the information's confidentiality, it had not and would not likely suffer any prejudice to its economic interests.[35] This finding does seem to take into account the reason why the hotel wanted to keep the information (names of its employees) confidential. The defendant wanted to obtain the information in order to unionize the hotel's employees.[36] Unionizing would have likely meant the hotel would have to increase the benefits it granted to its employees and possibly make it more difficult for it to negotiate lower cost employment arrangements.[37] Are these concerns not "economic interests?" The main reasons for committing industrial espionage are *economic interests* including gaining a competitive economic advantage, which, by its very nature, leads to the victim's detriment.

As previously discussed, other criminal provisions, such as sections 342.1 (unauthorized use of a computer) and 430(1.1) (data mischief) would only capture specific types of industrial espionage.[38] If the acts do not involve computer devices (such as searching through a competitor's trash) then section 342.1 may not apply. Acts captured under section 430(1.1) focus on denying access to or destroying data (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,"[39] which may include confidential information). This provision would not cover instances in which someone only copied the data or confidential information.

The mobility of labor is unlikely to be affected by deeming confidential information as property under the Criminal Code. Restrictive covenants in employment contracts that attempt to stop former employees from releasing or using confidential information during- subsequent employment have been upheld by the courts.[40] Additionally, it is unlikely that an employee unable to forget the confidential information, through no fault of their own, would have the requisite intent to support a conviction under section 354 of the Criminal

---

[33] R. v. Stewart, [1988] 1 S.C.R. 963, paras. 47–48 (Can.).
[34] *Id.* at para. 35.
[35] *See id.* at para. 37.
[36] *Id.* at para. 2.
[37] *See Facts About Unions*, UFCW CANADA, http://www.ufcw.ca/index.php?option=com_content&view=article&id=29&Itemid=49&lang=en (last visited Dec. 7, 2013).
[38] Criminal Code, R.S.C. 1985, c. C-46, ss. 342.1, 430(1.1) (Can.).
[39] *Id.* s. 342.1(2).
[40] *See* Jiffy Foods Ltd. v. Chomski, [1973] 3 O.R. 955 (Can. Ont. H.C.J.).

Code. This provision requires that the individual has the *intention* to possess the subject-matter of the charge as well as *specific knowledge* of its spurious character.[41] It is unlikely that inadvertent memory of the confidential information would meet this scienter requirement.

The court's concern over a lack of a precise definition for the term "confidential information" is likely no longer justified in light of *Pharand Ski Corp. v. Alberta.*[42] A precise definition is not necessary in order for the court to make a determination of whether information is confidential. As will be discussed later in this paper, the court has established a set of factors to aid in this determination.[43] Using factors to determine whether an individual has committed a criminal offense would not be unique to confidential information. Section 467.11(3) of the Criminal Code provides factors for the court to consider when determining if "an accused participates in or contributes to any activity of a criminal organization."[44]

In sum, confidential information should be deemed property under the Criminal Code to provide protection to individuals' ideas and projects where protection afforded by other areas of law falls short. Protection of confidential information falls in line with the overarching goal of furthering the public good and does not interfere with current Canadian case law or statutory law.

B. Canadian Tort Law

Similar to Canadian criminal law, Canadian tort law also does not provide adequate protection for those who fall victim to industrial espionage. Because the cause of action is based on common law, courts have been slow to adapt to the evolving nature of industrial espionage. This section examines current tort law and the elements of a cause of action, and it discusses the shortcomings in tort law as it relates to the protection of confidential information and the victims of industrial espionage.

1. Current Tort Law

As discussed above, criminal law is usually inapplicable to cases of industrial espionage; therefore, the primary recourse for victims is through tort law. The dominant cause of action is breach of confidence, but in some cases victims have also attempted to recover their losses by claiming a breach of

---

[41] TREMEEAR'S ANNOTATED CRIMINAL CODE OF CANADA (Carswell 2013) (emphasis added).

[42] *See generally* Pharand Ski Corp. v. Alberta (1991), 80 Alta. L.R. 2d 216 (Can. Alta. Q.B.).

[43] *See infra* Part II.B.2.a.

[44] Criminal Code, R.S.C. 1985, c. C-46, s. 467.11(3) (Can.).

fiduciary duty (in equity).[45] Because the moving party bears the burden to prove each element of the cause of action, use of tort law as the primary legal recourse for victims makes it likely that many instances of industrial espionage go unanswered by the court.[46] As a result, there is little deterrence for wrongdoers as long as they choose their victims wisely. As the court held in *Lac Minerals Ltd. v. International Corona Resources Ltd.*, breach of confidence is a sui generis cause of action in which plaintiffs can apply for relief on the basis of contract, property and equity.[47] An action for breach of confidence is rooted in the relationship between the two parties[48] and is not meant to protect or place a value on the confidential information itself. It is, instead, meant to protect the relationship between the parties, regardless of how direct or indirect that relationship may be.[49] Because the focus is the relationship between the parties, there may be instances where defendants have been able to avoid liability purely on the basis of an insufficient relationship between the parties and without regard to the damage and the confidential nature of the information.

2. Analysis of Tort Law

Under tort law, unauthorized disclosure or use of trade secrets can be brought under a cause of action for breach of confidence. There are three elements to a breach of confidence.[50] First, the information must be confidential.[51] Second, the information must have been imparted in circumstances importing an obligation of confidence.[52] Third, there must have been an unauthorized use of the information by the party to whom it was communicated (the "confidee") to the detriment of the party communicating it.[53] These three elements are discussed below.

---

[45] *See, e.g.*, R. v. Stewart, [1988] 1 S.C.R. 963, para. 24 (Can.); Lac Minerals Ltd. v. Int'l Corona Res., [1990] F.S.R. 441, 482 (Can.) (WL).

[46] *See generally Lac Minerals*, [1990] F.S.R. 441.

[47] *Id.* at 495.

[48] Fan, *supra* note 5.

[49] *See Stewart*, [1988] 1 S.C.R. 963 at para. 24 (protections in tort granted to confidential information are primarily concerned with the obligations of good faith or fiduciary relationships between the parties).

[50] PETER NEUMANN & JEFFREY SACK, ETEXT ON WRONGFUL DISMISSAL AND EMPLOYMENT LAW § 4.3.1 (1st ed. 2013).

[51] *Id.*

[52] *Id.*

[53] *Id.*

a. Element 1: The Information Must Be Confidential

In *Pharand Ski*, the court provided six factors to determine whether the information in question has the necessary qualities of confidence.[54] These factors include: (i) the extent to which the information is known outside the owner's business; (ii) the extent to which it is known by employees and others involved in the owner's business; (iii) the extent of measures taken by the plaintiff to guard the secrecy of the information; (iv) the value of the information to the plaintiff and his/her competitors; (v) the amount of money or effort expended by the plaintiff in developing the information; and (vi) the ease or difficulty with which the information could be properly acquired or duplicated by others (i.e., through their independent endeavors).[55] However, these factors need not be applied in order to find that the information was confidential if the court has found that the information was used by the defendant for the purpose of spring-boarding.[56] The factors in *Pharand Ski* are not exhaustive and the weight given to each one is completely at the discretion of the court.[57] Whether information is deemed confidential will depend on the facts in each particular case.[58] In determining whether these factors have been met, the courts appear to place significant weight on the information's novelty or "originality," the plaintiff's control over access to the information, and the documentary evidence the plaintiff is able to adduce on his own behalf. Remarkably, the reason why the plaintiff attempted to keep the information confidential did not seem to be a great consideration for the *Pharand Ski* court.[59]

Information that is public property or public knowledge is less likely to be considered confidential.[60] However, if the plaintiff has taken sufficient measures to restrict access to or limit knowledge of such information outside of the plaintiff's business, or the information itself has a "significant element of originality not already in the realm of public knowledge . . . . [as in] a significant twist or slant to a well-known concept,"[61] the court may find that the information had the requisite quality of confidence. For example, in *Interfirm Comparison*

---

[54] Pharand Ski Corp. v. Alberta (1991), 80 Alta. L.R. 2d 216, para. 136 (Can. Alta. Q.B.).

[55] *Id.*

[56] Stenada Mktg Ltd. v. Nazareno, 1990 CanLII 917 (B.C. S.C.).

[57] *Pharand Ski*, 80 Alta. L.R. 2d 216 at para. 136.

[58] Re Gauntlet Energy Corp., 2003 ABQB 718, para. 45 (Can. Alta. Q.B.).

[59] *See, e.g.*, *Pharand Ski*, 80 Alta. L.R. 2d 216 at para. 145 (finding information confidential without analyzing plaintiff's reason for keeping the information confidential); *Stenada Mktg.*, 1990 CanLII 917 (analyzing alleged confidential information without regard to plaintiff's reasons for keeping information confidential).

[60] Saltman Eng'g Co. v. Campbell Eng'g Co., [1963] 3 All E.R. 413, 415 (Eng.) (QL).

[61] Fraser v. Thames Television Ltd. (1982), [1984] Q.B. 44, 66 (Eng.).

(Australia) Party Ltd. v. Law Society of New South Wales,[62] the court found that restricting access only to those individuals whom had requested the information and registered with the plaintiff ensured that the information was only known to a small group of individuals outside of the plaintiff's business, providing it with a character of confidence.[63] Further, in terms of the information's novelty or "originality," in *Di Giacomo v. Di Giacomo Canada*,[64] although the constituent elements of the process at issue were commonly known, the ingenuity of the process was critical in the court's finding that it had the requisite character of confidence.[65] In contrast, a lack of originality defeated the plaintiff's case in *Promotivate International Inc. v. Toronto Star Newspapers Ltd.*[66] Despite finding that the disclosure of the plaintiff's idea to the defendants was made in confidence, because the plaintiff's idea was not, in the court's opinion, wholly original in that essential elements were well-known, the plaintiff's claim was defeated.[67]

The manner in which the information is disclosed and the plaintiff's control over access to this information also appears to have a significant bearing on the court's determination of the information's confidentiality, particularly in regard to the third factor. In evaluating the sufficiency of these measures, the court applies the reasonable person standard,[68] and appears to focus on the consistency of the application of the measures, the quality of documentary evidence, and the clarity of the instructions for confidentiality. Inconsistent application of measures to limit access and group exposure to the information at issue, lack of documentary evidence and vague instructions to employees significantly undermined the plaintiff's case in *Yates Circuit Foil Co. v. Electrofoils Ltd.*[69] The court found that the plaintiff had frequently allowed "workmen, sub-contractors and customers [to be] shown the plant quite freely with no reservations as to secrecy" except in limited circumstances.[70] Although the plaintiff insisted that he gave all the branch managers instructions to use extreme care when showing visitors around his plants, the plaintiff was not able to adduce sufficient documentary evidence of these instructions or practices,

---

[62] Interfirm Comparison (Austl.) Pty. Ltd. v. Law Soc'y of N.S.W. (1975), 45 F.L.R. 21 (S.C. N.S.W.) (WL).

[63] *Id.*

[64] Di Giacomo v. Di Giacomo Canada, 1989 CarswellOnt 2336 (Can. Ont. H.C.J.) (WL).

[65] *Id.* at para. 107.

[66] Promotivate Int'l Inc. v. Toronto Star Newspapers Ltd., 1985 CanLII 1995 (Can. Ont. S.C.).

[67] *Id.*

[68] Matrox Elec. Sys. Ltd. v. Gaudreau, [1993] Q.J. No. 1228, para. 99 (Can. Q. S.C.) (QL).

[69] *See generally* Yates Circuit Foil Co. v. Electrofoils Ltd. (1975), [1976] F.S.R. 345 (U.K.) (WL).

[70] *Id.* at 376.

which would have indicated a strong policy to maintain confidentiality.[71] What documentation the plaintiff could adduce was deemed by the court as too vague because it did not give clear directions on what could and could not be discussed or what was confidential.[72] The court found that this left too much discretion for the person receiving these instructions to be effective.[73] As a result, only the information that the plaintiff was able to adduce sufficient documentary evidence for was deemed confidential.[74] In contrast, in *Matrox Electronics Systems Inc.*, the fact that every employee and visitor was given clear instructions regarding confidentiality, including employee confidentiality agreements, and that the plaintiff maintained a high level of control over where visitors and employees could travel on the plaintiff's premises were key in the court's finding that the information had the requisite quality of confidentiality.[75] Although the court found it was not necessary for an employee to be expressly advised on each and every occasion that information being disclosed to him or her was confidential, given the overwhelming evidence of the security measures taken by the plaintiff to control access to the information and to ensure that knowledge of the information outside of the plaintiff's business was limited, the court found that a reasonable person standing in the shoes of the recipient of such information would have realized upon reasonable grounds that it was being disclosed in confidence.[76]

Given the holdings in the above-mentioned cases, it is apparent that tort law is an inappropriate method for fighting and deterring industrial espionage, particularly in cases where there is a great differential in power and resources between the parties. As it can be appreciated, proving a breach in confidence is a considerable effort. Because the onus is on the plaintiff to prove on a balance of probabilities each element of the tort, it is likely that many instances of industrial espionage go unchecked. Whether a perpetrator of the breach is found liable is not based on the confidential information at stake, but rather it appears to be a matter of resources and whether the plaintiff has suffered serious financial damage. This makes it likely that the plaintiff will not have the resources necessary to adduce sufficient evidence to meet the burden of proof. Even if the plaintiff does meet his or her burden, the awarded damages are likely to be inadequate because they will not account for the value of the loss of confidentiality, but instead will only restore the plaintiff to the position he or she

---

[71] *Id.* at 346.
[72] *Id.* at 380.
[73] *See id.*
[74] *See id.* at 371.
[75] Matrox Elec. Sys. Ltd. v. Gaudreau, [1993] Q.J. No. 1228, paras 98–99 (Can. Que. S.C.) (QL).
[76] *Id.* at para. 99.

would have occupied "but-for" the breach.[77] This policy objective may make application of tort law to a situation of industrial espionage inappropriate.

b. Element 2: The Information Must Have Been Imparted in Circumstances Importing an Obligation of Confidence

An obligation of confidence can arise through contract or equity. In contract, an obligation of confidence may arise through employment, through a joint venture or partnership, and through a licensor-licensee relationship.[78] In equity, depending on the nature of the relationship between the parties, an obligation of confidence may arise as a result of the circumstances surrounding the imparting of the information viewed from the perspective of the reasonable person.[79] Less frequently, an obligation of confidence may result from a finding of a fiduciary relationship between the parties.[80] If a plaintiff is unlikely to succeed in proving a breach of confidence, a finding of a fiduciary relationship would be favorable to the plaintiff because the plaintiff need not have suffered a detriment in order to establish a breach of fiduciary duty.[81] In equity, a third party in possession of confidential information may be found liable for breach of confidence if there was either express or implied knowledge of the information's confidentiality.[82]

The court in *Faccenda Chicken Ltd. v. Fowler* provided a set of principles to consider in determining whether an employee was under an obligation of confidence. These principles borrow from both contract and equity. These considerations include: (i) any express terms or obligations in the employment contract itself; (ii) whether there are any implied terms or obligations that would impute confidentiality; (iii) the duty of good faith or fidelity of the employee during the course of his or her employment; and (iv) additional factors to determine whether any particular information falls within an implied term of the contract.[83] These additional factors include: (i) the nature of the employee's employment; (ii) the nature of the information itself (whether or not the information can be classified as a trade secret or requires the level of protection of a trade secret); (iii) whether the employer impressed upon the employee the confidentiality of the information (not only in words but in attitude towards the

---

[77] *See* Yates Circuit Foil Co. v. Electrofoils Ltd. (1975), [1976] F.S.R. 345, 395 (U.K.) (WL).

[78] *See generally* Cadbury Schweppes Inc. v. FBI Foods Ltd., [2000] F.S.R. 491 (Can.) (WL).

[79] Coco v. A.N. Clark (Eng'rs.) Ltd., [1968] F.S.R. 415, 420 (Ch. D) (WL).

[80] MARTIN P.J. KRATZ, CANADA'S INTELLECTUAL PROPERTY LAW IN A NUTSHELL 107 (1998).

[81] Fan, *supra* note 5.

[82] *See Cadbury Schweppes*, [2000] F.S.R. 491 at para. 36; Interfirm Comparison (Austl.) Pty. Ltd. v. Law Soc'y of N.S.W. (1975), 45 F.L.R. 21 (S.C. N.S.W.) (WL).

[83] Faccenda Chicken Ltd. v. Fowler (1985), [1986] I.C.R. 297, 308–09 (Can.) (WL).

information); and (iv) whether the relevant information could be easily isolated from other information the employee is allowed to disclose.[84] These factors are to be applied using a "reasonableness" standard.[85]

Situations of joint ventures, partnerships, and licensor-licensee relationships are restrictive. In any of these cases, duties and obligations of confidentiality must be found in the contract itself. The presence of an express provision of confidentiality in the joint venture contract may be sufficient for the court to find that the information at issue was communicated in circumstances importing an obligation of confidence.[86] In contrast, in *Chicago Blower Corp. v. 141209 Canada Ltd.*,[87] the lack of an explicit duty in the licensing agreement between the parties to keep the information confidential not only during, but also *after* the term of the agreement expired, was critical to the court's finding that the obligation of confidence of the defendant with respect to the information at issue ended after the licensing agreement expired.[88] To alleviate the harshness of this principle, the court may still find an obligation of confidence to exist in a licensing agreement if the plaintiff did not anticipate that his know-how, imparted in confidence, would be used against him after the agreement expired.[89] Where an express agreement is absent, the court may also find an implied obligation of confidentiality in the course of negotiations regarding a joint venture between the parties,[90] and a defendant may be found in breach of this obligation if he later uses the confidential information discovered during the negotiation process as a spring-board.[91]

The use of equity to find an obligation of confidence is less certain, however. In order for the court to find that an obligation of confidence arose from the circumstances surrounding the imparting of the information, those circumstances must have been such that "any reasonable man standing in the shoes of the recipient of the information would have realised that upon reasonable grounds the information was being given to him in confidence."[92] The court in *Pharand Ski* discussed general circumstances that would give rise to an obligation of confidence, including whether confidentiality was an express term of any agreements between the parties, whether there was any assurance of

---

[84] *Id.* at 310.

[85] *See id.* at 306.

[86] Promotivate Int'l Inc. v. Toronto Star Newspapers Ltd., 1985 CanLII 1995 (Can. Ont. S.C.).

[87] Chi. Blower Corp. v. 141209 Can. Ltd. (1990), 30 C.P.R. 3d 18 (Can. Man. Q.B.).

[88] *Id.*

[89] Yates Circuit Foil Co. v. Electrofoils Ltd. (1975), [1976] F.S.R. 345, 382 (U.K.) (WL).

[90] Lac Minerals Ltd. v. Int'l Corona Res., [1990] F.S.R. 441, 491–92 (Can.) (WL).

[91] *Id.* at 447–48.

[92] Promotivate Int'l Inc. v. Toronto Star Newspapers Ltd., 1985 CanLII 1995 (Can. Ont. S.C.).

confidentiality, whether there is custom in the field in which the information was disclosed, and whether the nature of any implied obligations following formed express agreements of confidentiality.[93] In *Matrox*, the court found that the extensive security measures taken by the plaintiff, including employee confidentiality agreements and the inherent obligations of confidentiality of the defendants as engineers, were sufficient to give rise to an obligation of confidence on the basis of the reasonable person.[94] There is very little in the way of a structured approach to the application of this test, limiting the ability of the plaintiff to predict whether a defendant had an obligation of confidence towards him. This is particularly true in situations that do not involve employment between the parties (i.e., rival corporations).

There is no presumption of a fiduciary relationship between arms-length commercial entities[95] but one may arise if one party places itself in a position of vulnerability by sharing confidential information.[96] There are three elements required to prove the existence of a fiduciary relationship: (1) the fiduciary has scope for the exercise of some discretion or power; (2) the fiduciary can unilaterally exercise that power or discretion so as to affect the beneficiary's legal or practical interests; and (3) the beneficiary is peculiarly vulnerable to or at the mercy of the fiduciary holding the discretion or power.[97] It is possible for the court to find a fiduciary relationship without the presence of the first two elements, but vulnerability or dependency of the beneficiary is essential.[98] Although the court in *Lac Minerals* found that vulnerability or dependency was present in the relationship between the plaintiff and the defendant, the fact that it was a commercial relationship entered into voluntarily and that the plaintiff had the ability to protect itself in contract was sufficient to conclude that there was not a fiduciary relationship between the parties.[99]

A finding that the circumstances imparted an obligation of confidence, particularly in the employment context, may depend on whether the court classifies the information at issue as a trade secret.[100] For example, in *Faccenda Chicken*, the court held that information will only be protected in this sense if it can be properly classed as a trade secret or as material that by nature would require the same protection.[101] However, the court did not provide specific

---

[93] Pharand Ski Corp. v. Alberta (1991), 80 Alta. L.R. 2d 216, paras. 147–61 (Can. Alta. Q.B.).

[94] Matrox Elec. Sys. Ltd. v. Gaudreau, [1993] Q.J. No. 1228, paras. 99–100 (Can. Que. S.C.) (QL).

[95] *See Lac Minerals*, [1990] F.S.R. at 490.

[96] *Id.*

[97] *Id.* at 485 (quoting Frame v. Smith, [1987] S.C.R. 99, para. 60 (Can.)).

[98] *Id.*

[99] *Id.* at 490.

[100] Faccenda Chicken Ltd. v. Fowler (1985), [1986] I.C.R. 297, 310 (Can.) (WL).

[101] *Id.*

guidelines to determine whether information could be classified as a trade secret, but did state that it may include secret manufacturing processes and information that is in limited circulation.[102]

Scientific and technical information may not be classified as trade secrets by the court if this information is too close to "pure science" and, therefore, likely in the public domain and the "intellectual equipment" of the ex-employee.[103] The court will also consider the attitude of the employer towards the information[104] in determining whether information will be classified as a trade secret. The court has not defined this quality and has not offered any guidance in terms of what kind of evidence would be required by a plaintiff to prove this characteristic. However, even if the court does find that the circumstances of the disclosure give rise to an obligation of confidence, the final element must still be proven (namely, unauthorized use of that information).

c. Element 3: Unauthorized Use of the Information by the Party to Whom It Was Communicated to the Detriment of the Party Communicating It

Information received in confidence by the defendant used for any purpose other than that for which it was conveyed which results in a detriment to the plaintiff will likely entitle the plaintiff to relief.[105] Proof of both the misuse of the information and the detriment of its misuse are required to satisfy this element.[106] In cases involving alleged spring-boarding, if the court is satisfied that the defendant would have likely discovered the information without the confidence of the plaintiff, then it may find that the defendant's misuse of the information did not result in a detriment to the plaintiff.[107] Proving misuse of confidential information may be more difficult if the information at issue is classified as business information. Plaintiffs may then have to rely on purely circumstantial evidence to prove their case on a balance of probabilities.[108] This circumstantial evidence will then have to be weighed against the testimony of defendants who will likely deny everything.[109]

---

[102] *See id.* ("In addition, the fact that the circulation of certain information is restricted to a limited number of individuals may throw light on the status of the information and its degree of confidentiality.")*.*

[103] Matrox Elec. Sys. Ltd. v. Gaudreau, [1993] Q.J. No. 1228, para. 72 (Can. Que. S.C.) (QL).

[104] Yates Circuit Foil Co. v. Electrofoils Ltd. (1975), [1976] F.S.R. 345, 370–80 (U.K.).

[105] *See generally* Abode Props. Ltd. v. Schickedanz Bros. Ltd., 1999 CanLII 19053 (Can. Alta. Q.B.).

[106] *See id.* at paras. 47–50.

[107] *See id.* at paras. 48–51.

[108] *Matrox*, [1993] Q.J. No. 1228 at para. 94.

[109] *Id.*

Because a plaintiff must wait until the defendant has misused the information to its detriment, a plaintiff could face the hardship of launching multiple causes of action based on the same breach. For example, if the defendant is a broker of confidential information, he may have shared that information with multiple parties over a long period of time. If that information has been passed onwards in various forms (i.e., from subcontractors to third parties, etc.), the plaintiff would have the onerous burden of proving each successive liability. Furthermore, it is also unlikely that a defendant who acquires confidential information has an immediate use for it. In this situation, a plaintiff would have to wait until the defendant actually misuses the information. Finally, if the damage from the initial breach is severe, a plaintiff may be financially unable to pursue legal action, thereby allowing the downstream recipients to escape liability as well.

3. Punitive Damages in Tort Law

Tort law's damages principal—to restore the plaintiff to the position he would have occupied "but-for" the breach—is inappropriate to cases of industrial espionage. Punitive damages, on the other hand, are an exception to the rule in that they are not meant to compensate for injury caused, but rather they are meant to punish the wrongdoer and deter future bad behavior.[110] Considering the impact of industrial espionage on the Canadian economy, Canadian law should allow for a cause of action that provides clear protection for and deters misuse of confidential information through the punishment of offenders, regardless of the availability or desirability of punitive damage awards.

III. THE UNITED STATES' APPROACH

Unlike Canada, the United States succeeded in passing legislation that would adequately protect those whose proprietary information is stolen.[111] If Canada were to adopt the main features of the United States' Economic Espionage Act of 1996, it would solve many of the problems and concerns regarding misuse of confidential information. The first part of this section explains the basics of the Espionage Act. The second part of this section analyzes how implementing the key aspects of the Espionage Act would be beneficial for Canada in combating industrial espionage.

A. Economic Espionage Act of 1996

The United States' federal protection of confidential proprietary information is embedded in Title I of the Espionage Act, which was "enacted to

---

[110] Vorvis v. Ins. Corp. of B.C., 1982 CanLII 266, para. 26 (Can.).
[111] *See* Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–1839 (West 2012).

create a national scheme to protect United States' proprietary economic information, [and to provide] for both criminal and civil penalties for the theft of trade secrets benefitting either a foreign government or a private entity."[112] It characterizes trade secrets as property capable of being owned.[113] It also addresses many of the court's concerns in *Stewart* as well many general concerns regarding tort action to combat industrial espionage.

Section 1832 of the Espionage Act provides explicit protection against the theft of trade secrets.[114] Activities such as appropriating, taking, carrying away, concealing, possessing, receiving, or duplicating trade secrets without authorization will likely violate this provision.[115] This provision also prohibits conspiracies to steal protected information; therefore, the confidential information need not always have been taken for criminal charges to apply.[116] Further, receipt of confidential information by an independent third party is also enough.[117] Because attempts to obtain protected information are also prohibited, a defendant need not be successful in order to attract prosecution under this provision.[118] Therefore, the defendant would be held accountable for *all* the information they attempted to obtain in the breach and not just the information that could be attributed to a specific harm the victim has suffered. In turn, this reduces the necessity of having to revisit the breach in subsequent legal actions. Corporations are also subject to this provision and penalties for corporate offenders are specified.[119] The ability provided in this Act for the United States' government to assert jurisdiction over extra-territorial conduct likely enables prosecution of multinational corporations.[120]

The Espionage Act uses a broad definition of a "trade secret" that encompasses many types of information a person or organization would want to keep confidential.[121] The definition includes financial, business, and procedural information, as long as reasonable measures were taken to keep such information secret, and the information derives either actual or potential independent economic value.[122] As affirmed by the court in *United States v. Martin,* both tangibles and intangibles are included within this definition of a

---

[112] J. Michael Chamblee, Annotation, *Validity, Construction, and Application of Title I of Economic Espionage Act of 1996 (18 U.S.C.A. §§ 1831 et seq.),* 177 A.L.R. FED. 609 (2002).
[113] Economic Espionage Act of 1996, 18 U.S.C. § 1839(4).
[114] *Id.* § 1832.
[115] *Id.* § 1832(a).
[116] *Id.* § 1832(a)(5).
[117] *Id.* § 1832(a)(3).
[118] *Id.* § 1832(a)(4).
[119] *See id.* § 1832(b).
[120] *Id.* § 1837.
[121] *See id.* § 1839.
[122] *Id.* § 1839(3).

"trade secret."[123] Additionally, information does not lose its trade secret protection when it is the subject of a patent application because United States' "patent laws do not mandate that once a patent application is filed and approved, the inventor must open his files and fully disclose all of the technical and financial information ever created on the invention."[124] Although the novelty or uniqueness of the information may inform the courts in determining whether something is a matter of general knowledge, skill, or experience, a novelty or inventiveness requirement will not be strictly imposed in order for material to be considered a trade secret.[125]

B. Analysis of the Espionage Act

The Espionage Act addresses many of the court's concerns in *Stewart* and many general concerns regarding the use of tort law to combat industrial espionage.[126] First, it will not likely hinder the movement of labor. The Espionage Act was designed to prevent employees (and their future employers) from taking advantage of confidential information that was gained, discovered, copied, or taken while employed elsewhere. It was not designed to "prohibit lawful competition such as the use of general skills or parallel development of a similar product."[127] Further, the high level of intent required to successfully convict a defendant ensures that accidental receipt, acquisition, or unintentional possession of a trade secret will not likely result in criminal penalties.[128] The Espionage Act also does not prohibit whistleblowers or otherwise lawful activity.[129] Because it is a federal criminal offense, the onus is on the government to "prove beyond a reasonable doubt that the defendant sought to acquire information which the defendant believed to be a trade secret, regardless of whether the information actually qualified as such"[130] The vast resources of the federal government will likely reduce, if not eliminate, a power imbalance between a financially devastated victim and a wealthy corporate defendant. Moreover, because the provision also prohibits tempted use, a defendant would not have to actually use the information to the victim's detriment in order to be prosecuted.[131] Finally, this Act instructs courts to take the steps necessary and

---

[123] U.S. v. Martin, 228 F.3d 1, 11 (1st Cir. 2000).
[124] U.S. v. Hsu, 185 F.R.D. 192, 201 (E.D. Pa. 1999).
[125] 142 Cong. Rec. S12213 (daily ed. Oct. 2, 1996).
[126] *See generally* Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–1839 (West 2012).
[127] Chamblee, *supra* note 112, § 5 (quoting *Martin*, 228 F.3d at 56).
[128] Economic Espionage Act of 1996, 18 U.S.C. § 1832.
[129] *Id.* § 1833.
[130] Chamblee, *supra* note 112, § 9 (citing U.S. v. Hsu, 155 F.3d 189 (3d Cir. 1998)).
[131] Economic Espionage Act of 1996, 18 U.S.C. § 1832(a)(4).

appropriate to preserve the confidentiality of the information that is the subject of the proceeding.[132]

IV. INTERNATIONAL TREATIES

Canada's international obligations demand greater protection of confidential information. Current Canadian law does not satisfy the requirements of the North American Free Trade Agreement (NAFTA) and the World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs) for protecting valuable information. The first part of this section will explain both the NAFTA and TRIPs agreements. The second part of this section will argue that Canada needs to amend its laws in order to be in compliance with these international obligations.

A. NAFTA and TRIPs Explained

Both NAFTA and TRIPs[133] require Canada to protect information that is "secret."[134] Article 1711 of NAFTA requires each member to "provide the *legal means* for any person to *prevent trade secrets* from being *disclosed to, acquired by, or used* by others without the consent of the person *lawfully in control of the information* in a manner contrary to honest commercial practices."[135] A "trade secret" is broadly defined and likely includes any information held by a person, legal or otherwise, that has been kept reasonably secret, and which has or is likely to have commercial value.[136] The TRIPs agreement uses the same parameters as NAFTA to define the type of information each member is to protect, characterizing this information as "undisclosed information" rather than a "trade secret."[137] Both agreements use language of ownership in describing the required treatment of this information, which suggests that confidential information could give rise to a proprietary interest.[138] To be protected, such information would have to be capable of being "acquired" or "used" and in the lawful control of a person.[139] Furthermore, because TRIPs provides that information that is lawfully within the control of both natural and legal persons will be protected, then corporations as legal persons will also likely be afforded

---

[132] *Id.* § 1835.

[133] Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994), *available at* http://www.wto.org/english/docs_e/legal_e/27-trips.pdf [hereinafter TRIPs].

[134] NAFTA, *supra* note 4, art. 1711(1); TRIPs, *supra* note 133, § 7 art. 39(2).

[135] NAFTA, *supra* note 4, art. 1711(1) (emphasis added).

[136] *Id.* arts. 1711(1)(a), (b), (c).

[137] TRIPs, *supra* note 133, § 7 art. 39(1); *see* NAFTA, *supra* note 4, art. 1711(1).

[138] *See* TRIPs, *supra* note 133, § 7 art. 39; NAFTA, *supra* note 4, art. 1711.

[139] NAFTA, *supra* note 4, art. 1711(1); TRIPs, *supra* note 133.

protection.[140] TRIPs also takes into consideration the public's interest in this undisclosed or confidential information where disclosure may be necessary to protect the public.[141] Moreover, tort law may still play a role in protection of this information as a breach of confidence may be deemed a violation of this agreement.[142]

B. How NAFTA and TRIPs Require Changes in Canadian Law

Given the requirements previously laid out by NAFTA and TRIPs, it is apparent that Canada needs to change the way it combats industrial espionage. With both agreements requiring a legal mechanism to protect trade secrets, Canada should not rely on a patchwork of common law tort doctrines and judicial re-examination of its Criminal Code provisions for such protection. Indeed, Canada is legally required to do something more. Specific legislation is needed. In the absence of such legislation, courts should take note of Canada's international obligations with respect to trade secrets, and interpret domestic law in light of those obligations going forward, as both NAFTA and TRIPs have been incorporated into Canadian domestic law.[143] For instance, it may lead to *Stewart* being distinguishable or no longer considered good law in light of those obligations.

---

[140] TRIPs, *supra* note 133, § 7 art. 39(2).

[141] *Id.* § 7 art. 39(3).

[142] *See id.* § 7 art. 39(2).

[143] See the Supreme Court of Canada's remarks in *Nat'l Corn Growers Assn. v. Canadian Import Tribunal*, [1990] 2 S.C.R. 1324 (Can.):

> The first comment I wish to make is that I share the appellants' view that in circumstances where the domestic legislation is unclear it is reasonable to examine any underlying international agreement. In interpreting legislation which has been enacted with a view towards implementing international obligations, as is the case here, it is reasonable for a tribunal to examine the domestic law in the context of the relevant agreement to clarify any uncertainty. Indeed where the text of the domestic law lends itself to it, one should also strive to expound an interpretation which is consonant with the relevant international obligations.
>
> Second, and more specifically, it is reasonable to make reference to an international agreement at the very outset of the inquiry to determine if there is any ambiguity, even latent, in the domestic legislation. The Court of Appeal's suggestion that recourse to an international treaty is only available where the provision of the domestic legislation is ambiguous on its face is to be rejected.

CONCLUSION

The problem of industrial espionage demands a better approach than what Canadian law currently provides. Although it is the predominant approach, tort law is likely not the most effective or the most appropriate method to combat industrial espionage. Placing the burden of proof—particularly in regard to breach of confidence—on a victim who has likely suffered serious financial damage probably limits the number of incidents of industrial espionage reaching the courts. This likely provides little deterrence for a wealthy corporation or savvy information broker to commit such acts. Given that the purpose of tort law is not to punish or deter, tort law, from a policy perspective, may not be the most appropriate approach to combat industrial espionage.

As the Espionage Act, NAFTA, and TRIPs suggest, confidential information should give rise to a proprietary interest and this proprietary interest should be protected under Canadian criminal law. Sections 1832–39 of the Espionage Act give an example of a criminal legislative framework that offers a proper balance between the protection of confidential information and public policy. Criminal law requires a high level of intent; therefore, only those unauthorized individuals and organizations that intended to take information known to be confidential would be in violation of these provisions. This scheme offers many benefits beyond the predominant tort law approach. Given the resources of the federal government and the investigative powers of its key agencies, including the Royal Canadian Mounted Police, it is likely that more instances of industrial espionage will be brought to the courts' attention. Combined with severe criminal penalties, such an approach would likely provide the necessary deterrence that Canadian law currently lacks.