fogler rubinoff

Intellectual Property Bulletin

February 10, 2021

PROTECTING CONFIDENTIAL INFORMATION IN CANADA: IS THERE A BETTER WAY?

By Colleen Spring Zimmerman and Catherine Hart

Colleen Spring Zimmerman
Partner

t: 416.941.8884
cspringzimmerman@foglers.com

Catherine Hart
Associate

t: 416.864.7612
chart@foglers.com

The British Columbia decision *Equustek Solutions Inc. v Jack*[1] highlights the difficult, time consuming, and expensive exercise that organizations may find themselves in when an employee misuses confidential information. In today's environment, information can be downloaded, transferred or shared instantly. How can organizations best protect their intellectual property assets and confidential information to maintain their competitive advantage?

Intellectual Property and Confidential Information

Intellectual property and confidential information are related concepts. The World Intellectual Property Office defines intellectual property as "creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce."[2]

Confidential information, in comparison, includes any non-public information or material that is communicated or shared from a disclosing party to a recipient. The exact definition of confidential information may further be defined under an agreement between parties. What defines confidential information is the manner in which it is shared, rather than its particular features.

A disclosing party may have certain intellectual property rights in the embodiment of the confidential information or in the information found within it. Correspondingly, confidential information can be understood as a form of intellectual property.

In Canada, organizations can protect their intellectual property with statutory legal frameworks, such as the *Patent Act*[3], the *Copyright Act*[4] or the *Trademarks Act*[5]. However, protecting intellectual property can be an expensive exercise and it is impracticable to protect all confidential information using these means.

---

[1] 2020 BCSC 793 [*Equustek*]
[2] WIPO, *What is Intellectual Property?*, online: https://www.wipo.int/about-ip/en/
[3] RSC 1985, c P-4.
[4] RSC 1985, c C-42.
[5] RSC 1985, T-13.

Correspondingly, in the context of employees, organizations usually rely on employment contracts to provide wide protection over their confidential information. The courts have given wide scope to the definition of confidential business information and an organization can claim ownership over many varieties of information including trade secrets, formulae, client lists and even internal office memoranda[6]. The core requirement of confidential business information is that the creator of the information must have used their brain and produced a result which can only be produced by somebody who goes through the same process[7].

Enforcing Rights and Obligations: The Equustek Decision

Although organizations have a toolkit available to them to protect their intellectual property and confidential information, enforcing their rights to such property can prove challenging. The decision *Equustek Solutions Inc. v Jack*[8] of the British Columbia Supreme Court highlights the long and expensive journey that an organization may have to embark on to protect its intellectual property and confidential information.

Notably, the Plaintiffs began their legal battle against some of the Defendants in 2011, close to ten years ago. In another related proceeding, the Plaintiffs had to litigate all the way to the Supreme Court of Canada to force Google to de-index certain Defendants' websites, which were being used to unlawfully offer and sell the Plaintiffs' intellectual property.[9]

This decision concerned allegations by Equustek and its directing mind Mr. Angus and his holding company, that former employees and related entities stole confidential material regarding a product to create and sell their own product and related technical documents[10].

The individual Defendants included Mr. Marsh, an engineer who marketed and sold the Plaintiffs' products, being protocol converters, and later sold his business to Mr. Jack; Mr. Crawford and Mr. Ingraham, engineers who worked for Mr. Angus for a period of time; Mr. Jack, the directing mind behind the corporate Defendants ("**Datalink**"); and Messrs. Cheifots, engineers that worked on building Datalink's own protocol converter. The Plaintiffs also sued the website designer, Mr. Bunker, who provided the corporate Defendants with a website that could not be searched in a search engine.

Mr. Jack, Datalink and the Cheifots did not participate in the proceeding.

The Court was asked to consider whether the Defendants conspired to steal confidential material, including source code, from the Plaintiffs' protocol converter and associated technical documents and used what they stole to create their own protocol converter and associated technical documents[11].

---

[6] *Coco v. A.N. Clark (Engineers) Ltd.*, (1969) RPC 41 at 47.
[7] *Saltman Engineering Co. Ltd. v Campbell Engineering Co. Ltd.* (1948), 65 RPC 203 at 215.
[8] Equustek, *supra* note 1.
[9] *Google Inc. v Equustek Solutions Inc.*, 2017 SCC 34.
[10] *Ibid* at para 5.
[11] Equustek, *supra* note 1 at para 5.

The Plaintiffs further claimed breach of confidence, passing off, breach of contract and unjust enrichment, and breaches of the *Copyright Act* and the *Trademarks Act*. The Plaintiffs also alleged that the Defendants advertised the Plaintiffs' products on their internet websites to draw customers in, then shipped their own products and gave customers the impression that the Plaintiffs' products were no longer available[12].

The Plaintiffs sought damages for past and future loss of sales; punitive damages; injunctive relief; an accounting and disgorgement of the Defendants' profits arising from all sales of products other than Equustek's own products; a declaration that the Defendants held monies in a constructive trust for the Plaintiffs, and equitable tracing of such funds; an order piercing the corporate veil and holding all of the Defendants jointly and severally liable; special costs, or in the alternative, costs; and interest[13].

The Allegations

In 2005, the Defendants were alleged to have worked together to create a product that would complete the same functions as the Plaintiffs' protocol converter. Each individual Defendant played a role, whether translating the Plaintiffs' source code, directing such copying, building the external components of the device, or establishing a website to support Datalink customers. The Defendants used aliases to communicate with potential customers on some occasions.

In March 2008, Datalink began shipping its protocol converter. When a customer purchased one of the Plaintiffs' products, Datalink would send the customer a Datalink protocol converter and claim that it was an improved version of the requested Equustek product[14]. The packages included a letter which referred to an enclosed CD with application notes, a user manual and a reference to a website: www.datalink-gateways.com. It was identical to the known Datalink website www.datalinkgateways.com, apart from the hyphen, and not discoverable through an internet search.

The Holding

The Court held that that Mr. Crawford was liable for breach of confidence as a result of his actions in respect of the development and marketing of the Datalink product. The Court held that Mr. Crawford outright copied certain source code that belonged to the Plaintiffs and that he had access to source code while employed by Equustek. The Court noted that Mr. Crawford did not provide adequate evidence to establish that he reverse engineered the Plaintiffs' product and did not copy it[15].

The Court further held Mr. Crawford and Mr. Jack liable for copyright infringement by knowingly and intentionally copying a vast quantity of Equustek's manual and application notes[16].

---

[12] *Ibid* at para 6.
[13] *Ibid* at para 8.
[14] *Ibid* at para 62.
[15] *Ibid* at para 234.
[16] *Ibid* at para 286.

Mr. Jack was also held liable for passing off, breach of confidence, and conspiracy. The Court held that only Mr. Jack was personally liable for passing off despite the participation of the other Defendants in the unlawful enterprise. The Court emphasized that Mr. Jack was unquestionably the architect of the marketing plan that saw Datalink offer its products as a replacement for Equustek products and that the company was not run as a collective with others. The Court noted that Mr. Jack controlled the messaging on the websites and appeared to have been the point of first contact with customers[17]. Datalink was also held liable for passing off, breach of confidence and conspiracy.

The other non-participating Defendants, the Cheifots, were also held liable for breach of confidence and conspiracy, primarily by virtue of their non-participation in the proceeding[18]. Mr. Bunker, Mr. Ingraham and Mr. Marsh were not held liable for any of the claims.

The Plaintiffs requested that the Court's orders only be applied to those individuals with an interest in Datalink. Correspondingly, the Court held that the Plaintiffs were entitled to orders concerning unjust enrichment, accounting and disgorgement, a declaration of constructive trust and piercing the corporate veil against Mr. Jack, Datalink and the Cheifots[19].

Lessons Learned

After approximately 10 years of litigation, the Plaintiffs achieved a successful adjudication of their dispute. However, it remains to seen how much money the Plaintiffs will actually collect against Mr. Jack, Datalink and the Cheifots. That will be determined at a post-judgment hearing which means that the Plaintiffs still have ongoing litigation. It appears that both Mr. Jack and the Cheifots have been absent from the jurisdiction for many years now and are probably judgement proof in the jurisdiction.

This case reminds organizations that recourse to the courts should be considered only as a last resort. Litigation is a lengthy and expensive process that leaves few satisfied, even with a favourable decision in hand. One other option is to involve the police which in certain circumstances may result in the activities ceasing but would not result in any relief of the type sought in this litigation.

Organizations are best positioned to protect their intellectual property and confidential information by creating specific policies on how information will be shared and to whom, and by monitoring who is accessing and downloading company intellectual property and confidential information on a regular basis. Further, organizations are always strongest when their employees are invested in the success of their employer. Organizations should consider establishing systems, such as employee stock option plans or particular compensation structures, that encourage the alignment of employees' interests with those of the organization.

[17] *Ibid* at para 305.
[18] *Ibid* at para 253.
[19] *Ibid* at para 400.

However, when employees are determined to steal confidential information the only practical option may be litigation. The plaintiff must enter that litigation knowing that it may be costly and time consuming and that the chances of obtaining financial relief may be remote, depending on the circumstances and assets of the defendants.