Internet and E-Commerce Law in Canada

VOLUME 23, NUMBER 6 Cited as (2022), 23 I.E.C.L.C. OCTOBER 2022

• DETOXIFYING THE ANONYMOUS INTERNET ONE TROLL AT A TIME: NORWICH ORDERS •

Jordan Deering, Partner, Ryan Black, Partner, Tyson Gratton, Associate and Ryan Hamieh, Summer Student, DLA Piper LLP

Jordan Deering

Ryan Black

Tyson Gratton

When people create profiles and interact with one another online, doing so anonymously under an assumed username remains the most common approach.

• In This Issue •

LexisNexis®

While some major platforms have moved away from this model and have begun requiring users to register with their actual names, the vast majority of platforms continue to operate with anonymity as a key feature. When users layer anonymous accounts upon anonymous accounts it can be nigh impossible for parties who have been wronged online to identify the wrongdoers and hold them to account without the cooperation of platforms and ISPs who are able to connect anonymous usernames with identifying information such as names, email addresses, and IP addresses.

A Norwich order is an extraordinary equitable remedy that requires an innocent third party, which is tied up in the wrongdoing of another, to disclose certain information to the wronged party so that the wronged party may pursue a claim. As platforms and ISPs will generally refuse to disclose information about their users upon request and in some cases are prohibited from doing so absent a court order, Norwich orders have become a valuable tool in

INTERNET AND E-COMMERCE LAW IN CANADA

Internet and E-Commerce Law in Canada is published twelve times per year by LexisNexis Canada Inc., 111 Gordon Baker Road, Suite 900, Toronto ON M2H 3R1 by subscription only.

ISBN 0-433-43112-1 (print) ISSN 1494-4146
ISBN 0-433-44675-7 (PDF)
ISBN 0-433-44386-3 (print & PDF)

Subscription rates: $335.00 per year (print or PDF)
$485.00 per year (print & PDF)

General Editor
Lara Saraireh, LL.B., LL.M.
Content Development Associate
LexisNexis Canada Inc.
E-mail: lara.saraireh@lexisnexis.ca

Please address all editorial inquiries to:

LexisNexis Canada Inc.
Tel. (905) 479-2665
Fax (905) 479-2826
E-mail: ieclc@lexisnexis.ca
Web site: www.lexisnexis.ca

Canada to obtain the necessary information to pursue claims against people who infringe copyright, harass, defame, make threats of physical harm and death, or otherwise facilitate crime online.

The inquiry in a recent Ontario Superior Court of Justice case considered whether a legitimate objective justified the use of a Norwich order in an *ex parte* setting. An *ex parte* proceeding is one where the judge decides without all of the parties being present at the application—in this case the third party platform who was the subject of the application. In *Bungie Inc. v. TextNow Inc.*,[1] the Court established that there was rationale for proceeding absent TextNow, as concerns over the safety of the applicants provided sufficient justification in light of TextNow's policy to inform its customers of applications of this nature. This decision reemphasizes the unique utility of Norwich orders and how such orders can be obtained on an urgent and *ex parte* basis when there is a serious risk of harm.

THE BACKGROUND

The applicants were two Bungie Inc. employees, going by the pseudonyms James Doe and Jane Doe, who live in the US and work as developer and community manager, respectively, for Bungie's popular multiplayer game, *Destiny 2*. While games are an enjoyable pastime for many, others take it as an opportunity to harass, grief and troll (intentionally degrading the gameplaying experience of others through malicious activity), dox (using or exposing private or personal information about a particular individual on the internet with malicious intent, enabling others to do the same or make threats of harm) and even swat (that is, calling in emergency police requests that result in armed police officers arriving at the victim's address) other members of the gaming community. Game development employees who are public-facing, especially as "community managers" who responsible for interacting with and engaging with the game's online community, face the direct ire of these miscreants, often as a result of gameplay issues, development decisions, perceived community slights, racism, sexism, or a host of other reasons.

In this context, the applicants were subjected to increasing harassment and abuse of their personal information at the hands of an anonymous individual living in the United States. Evidence was submitted demonstrating that the harasser employed the use of the services of the respondent, TextNow Inc., to anonymize their conduct and communications. TextNow is a company registered in Ontario and, amongst other things, operates a service where it purchases access to phone networks operated by telephone companies, and then provides customers with inexpensive access to those networks. The net result is that while there are many legitimate uses for this service, in some cases it enables harrassers to efficiently make anonymous texts and phone calls. TextNow's terms of service make it clear that it functions to provide customers with anonymity, maintaining a policy that they only preserve records for 90 days, and (absent a non-disclosure order) will inform users of requests for customer information giving them seven days to dispute the request in court.

The applicants submitted ample evidence that one of TextNow's customers was harassing and doxing the individuals applicants. The abusive behaviour ensued through numerous calls, texts and offensive voicemails, sending death threats, and going so far as to order pizza to the applicants house (which, while sounding innocuous, is a direct threat in the context of known swatting opportunities).

The applicants submitted a Norwich application to extract information about the harasser from the customer database of TextNow. Generally these orders go unopposed upon notice. But in this context, the rationale for proceeding *ex parte* was the concern that TextNow has a policy to tell its customers of applications of this type, which may have lead to dire consequences. The Court considered whether to make an interim order prohibiting disclosure of the Norwich application by the respondent when served. Ultimately, the Court determined that notice of the application to TextNow should be waived in the interests of justice.

JUSTIFICATION FOR WAIVING NOTICE

For the Court to determine that notice of the application should be waived, they examined the established legal test for granting Norwich orders, including whether:

- The applicant has provided sufficient evidence to raise a valid, bona fide or reasonable claim;
- The applicant has established a relationship with the third party from whom the information is sought, such that it establishes that the third party is somehow involved in the acts complained of;
- The third party is the only practicable source of the information available;
- The third party can be indemnified for costs to which the third party may be exposed because of the disclosure; and
- The interests of justice favour obtaining the disclosure.

In determining whether to provide notice of the Norwich application to TextNow, the Court assessed the need for discovery and the proposed use for the information sought. The arguments against providing notice generally underscore whether notice to the alleged wrongdoer may precipitate the dissipation of assets or additional offences.

The Superior Court concluded that notice of the application should be waived because the delay necessary to give notice of the proceeding could entail severe consequences, elaborating that if TextNow followed its posted policy and informed its customer of the application, the harm the customer may commit is serious given evidence of anti-social behaviour and overt threats. The Court clarified that providing notice would be foolhardy given the nature of threats made against the applicant Bungie employees.

Finally, the Court elaborated that this equitable remedy ought to be made available to identify people in circumstances of harassment, racism, doxing, overt threats or the abuse of private information. Regardless of the wrongdoer's location, the Court elaborated that the identity of targets should be discoverable provided the prerequisites of a Norwich application are met.

FUTURE OUTLOOK

As anonymity surges throughout the globe, it becomes increasingly difficult to identify individuals who have committed wrongdoing. The progression of social

media and identity-concealing apps contributes to this inconspicuousness and functions to hinder legal investigations.

The Superior Court's affirmation of *ex parte* Norwich relief in circumstances of online harassment serves to give yet another tool to pierce the veil of duplicitous offenders. This equitable remedy will prove valuable in certain litigation settings and serve to diminish strain and cost in cross-border investigations. And, when the circumstances dictate, removing the obligation to provide notice expedites legal proceedings and ensures the potential consequences of litigation are mitigated well in advance.

[***Jordan Deering*** *is a Partner and the Chair of DLA Piper Canada's Corporate Crime, Compliance & Investigations Group. Her practice for the last 20 years has focused on litigation, investigations and regulatory proceedings involving all aspects of fraud and corporate misconduct. She regularly acts for banks and corporate clients in respect of these sensitive, high stakes mandates.*

Ryan Black *is a Partner practises technology-related business law, with a particular focus on information technology, practicing games and esports, and internet-facing businesses. As a former software and Internet developer, Ryan has a unique insight to emerging technology matters, such as cybersecurity, blockchain technologies, artificial intelligence, open source software, deepfakes, cloud computing, and social media.*

Tyson Gratton *is an Associate and has a business law practice which is focused on advising video game, virtual and augmented reality, information technology, and ecommerce businesses. In his practice, Tyson works alongside companies from across Canada, the United States, and abroad who are creators, developers, integrators, innovators, distributors, and service providers.*]

---

[1] *Bungie Inc. v. TextNow Inc.*, [2022] O.J. No. 3342, 2022 ONSC 4181.

• MODERNIZING CANADA'S DIGITAL TRADE POLICY: CANADIAN CONSULTATIONS ON A MODEL DIGITAL TRADE AGREEMENT •

Clifford Sosnow, Partner, Peter Kirby, Partner, Novera Khan, Associate, and Christopher Little, Associate, Fasken LLP


Clifford Sosnow


Peter Kirby


Novera Khan


Christopher Little

On July 15, 2022, the Government of Canada initiated a public consultation process regarding the development of a model digital trade agreement. The government is seeking the views of industry

stakeholders, non-governmental organizations, and other interested Canadians regarding the development of the model agreement, its potential scope and content, as well as potential trading partners with whom Canada may seek to negotiate.

We provide some background regarding digital trade and explore the potential implications of the development of a model agreement below.

BACKGROUND: WHAT IS DIGITAL TRADE?

Digital trade is a broad concept that is most often used to refer to digitally enabled, cross-border commercial transactions of goods and services that may be either digitally or physically delivered. For example, the purchase of goods (e.g., books) through an online marketplace is facilitated by digital technologies, but such goods may ultimately be physically delivered. Digitally enabled transactions of goods and services may also forego physical delivery and hence overcome geographical barriers in the context of cross-border trade. Streaming services, for example, are digitally enabled and the services (e.g., music, movies, and television programs) are digitally delivered to customers.

Digital trade also encompasses cross-border transfers of data that are essential to the global connectivity of businesses, governments, and supply chains. This movement of data has enabled the creation of new and rapidly evolving services that promote more efficient business operations, such as cloud computing, artificial intelligence (AI), the Internet of Things (i.e., the interconnection of physical objects embedded with technologies connecting and exchanging data with other devices via the internet), and additive manufacturing (i.e., digital engineering and manufacturing).

PURPOSES OF A DIGITAL TRADE AGREEMENT

Many of Canada's recent international trade agreements cover digital trade, though these have focused narrowly on digital products (e.g., computer programs, sound recordings or other products that are digitally encoded) that can be transmitted electronically, rather than digitally encoded and physically delivered products (as these are captured by existing rules). The Canada-United States-Mexico Agreement (CUSMA), for example, contains a chapter on Digital Trade[1] that commits the parties not to apply customs duties to digital products, to protect personal information, and to cooperate on important security issues in electronic communications. Likewise, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) contains a chapter on Electronic Commerce[2] that includes similar commitments.

More recently, countries that recognize the economic opportunities associated with the expansion of digital trade have begun to negotiate dedicated digital trade agreements. The most noteworthy example is the Digital Economic Partnership Agreement (DEPA)[3], originally initiated between Chile, New Zealand, and Singapore, which Canada has requested to join[4]. The DEPA builds upon the CPTPP Electronic Commerce chapter by adding enhanced commitments related to facilitating digital trade and cooperation on emerging issues including AI, privacy, and digital inclusion.

By establishing a model Canadian digital trade agreement, Canada is attempting to position itself at the forefront of the development of international rules governing digital trade policies. The development of a model agreement would enable Canada to work with potential trading partners in order to pursue its goals of facilitating commercial activity, addressing potential market access impediments, and building consumer trust and confidence. The Canadian government anticipates that businesses would benefit from greater certainty and predictability, particularly small and medium-sized businesses that can face significant cost and administrative burdens complying with ambiguous or unbalanced digital trade rules.

CONCLUSION

Those wishing to provide input on the development of a model digital trade agreement may do so

by e-mail[5] prior to the closing of the consultation period on September 13, 2022. Potential topics that could be addressed include, but are not limited to, competition policies; cybersecurity; intellectual property; subsidies; standards and interoperability; electronic transaction frameworks; and online consumer protection.

Further consultations are expected after the initial consultation process. Fasken will continue to monitor developments regarding the development of a model digital trade agreement and provide updates accordingly.

[***Clifford Sosnow*** *is a Partner at Fasken and co-Chair of the firm's International Trade and Investment Group. He also advises the firm on sanctions and anti-bribery and corruption compliance.*

Peter Kirby *is a Partner at Fasken and practices in the area of international trade and customs law.*

Novera Khan *is an Associate at Fasken. She maintains a broad commercial litigation and dispute resolution practice at Fasken. She also advises clients in the areas of international trade and customs law and communications law.*

Christopher Little *is an Associate at Fasken and a member of the firm's Procurement, International Trade & Investment, and National Security Groups.*]

---

1 Canada-United States-Mexico Agreement (CUSMA) - Chapter 19 - Digital Trade, online: https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/text-texte/19.aspx?lang=eng.

2 Comprehensive and Progressive Agreement for Trans-Pacific Partnership, Consolidated TPP Text – Chapter 14 – Electronic Commerce, online: https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/14.aspx?lang=eng.

3 Online: https://www.mfat.govt.nz/assets/Trade-agreements/DEPA/DEPA-Signing-Text-11-June-2020-GMT-v3.pdf.

4 See: "Minister Ng announces Canada's request to join the Digital Economy Partnership Agreement" (May 22, 2022), online: https://www.canada.ca/en/global-affairs/news/2022/05/minister-ng-announces-canadas-request-to-join-the-digital-economy-partnership-agreement.html.

5 Email: TMSconsultation@international.gc.ca.

• WHAT'S THE SECRET TO PROTECTING TRADE SECRETS? •

Anita Nador, Partner and Madison MacColl, Associate, Gowling WLG LLP

Anita Nador

Madison MacColl

In technical terms, a trade secret is a form of intellectual property pertaining to information that is commercially valuable. Why? Well, by virtue of the fact that it's secret.

Valuable, secret information can take many forms. For example: the formula for Coca Cola's signature beverage, or the fabled "Original Recipe" of Kentucky Fried Chicken (KFC). It could apply to anything, really, including a manufacturing process, a method for doing business, research projects, business plans, source codes, and even algorithms. The list is potentially endless.

In order to maintain inherent value in the information, the secret has to be safeguarded and reasonable IP security measures need to be taken. How does one do that? Unlike other forms of IP, such as patents, trademarks, designs, or copyright, there is no searchable registry of trade secrets. Although many countries have laws outlining how misappropriation of trade secrets is a crime, enforcement can be a long and costly process.

Further, unless one can quickly identify a misappropriation and contain it, the secret is often, well, no longer secret. Although certain technology allows for the tracking and identification of potential security breaches, it can also facilitate the

speedy transmission (including inter-jurisdiction transmission) of information.

LEGAL ENFORCEMENT

Criminal provisions in Canada

Recent amendments to section 391 of the *Canadian Criminal Code* have made it an offence to "knowingly obtain, communicate or make available a trade secret" by deceit, falsehood, or other fraudulent means[1] or does so knowing that it was obtained by deceit, falsehood or other fraudulent means.[2] The *Criminal Code* defines "trade secret" as any information that: (a) is not generally known in the trade or business that uses or may use that information; (b) has economic value from not being generally known; and (c) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[3]

However, the *Criminal Code* excludes as an offence situations where the trade secret was obtained through independent research and development, or by reverse engineering.[4] Charges can proceed on an indictable or summary offence basis. If convicted as an indictable offence, one could be subject to imprisonment of up to 14 years. On summary conviction, maximum sentencing would be two years less a day and/or a fine of up to $5000 CDN.

Under the *Criminal Code*, law enforcement will bear the burden of investigating and charging those involved in trade secret offences, while the Crown will bear the responsibility of proving beyond a reasonable doubt that an offence was committed. Practically, the owner of the trade secret is in the best position to provide supporting evidence for any conviction, primarily through their systems, policies, and operations. Some law enforcement agencies also have tools and networks that may facilitate identification, tracking, containment, deterrence, and enforcement. Of course, criminal proceedings do not preclude civil proceedings.

Civil remedies in Canada

Remedies for the misappropriation of trade secrets (otherwise known as confidential information) are available in Canada. A handful of landmark Supreme Court of Canada decisions have set the following legal requirements that must be established on the balance of probabilities:

i. The information conveyed was confidential;
ii. The information was communicated in confidence; and
iii. The information was misused by the party to whom it was communicated.

Canadian courts have recognized that it is often hard to quantify the harm suffered as a result of misappropriation of a trade secret. As a result, many have taken an approach geared toward finding a broadly equitable result. This has often led to significant monetary awards.

In addition to monetary awards, a Canadian court may issue an injunction. When there is a serious issue to be tried, there will often be irreparable harm, and the balance of convenience favours granting an injunction. Recently, the Supreme Court confirmed a lower court decision granting an extraterritorial injunction, recognizing that the "internet has no borders."

THE SECRET OF MAINTAINING TRADE SECRET VALUE

1. Develop a trade secret policy and operational systems in order to:

i. Identify information that is a trade secret (that lends itself to being a trade secret and has value);
ii. Maintain the secret; and
iii. Provide evidence in support for criminal/civil proceedings.

2. Components of trade secret policy

Many components of a good trade secret policy support broader business planning, IP strategy, and data privacy/confidentiality compliance objectives, and may include:

i. A method for identifying and reporting on information that is valuable and ideally kept as a trade secret (as opposed to other forms of IP). What

information provides a business with a commercial edge? What information would impact the value of the business if known by others?

ii. Ensuring proper agreement/relationship management, such as standard confidentiality clauses and, to the extent permissible, non-compete provisions (see below). Also, identifying trade secret information obtained from third parties, isolating it, and limiting access and use in accordance with the agreement.

iii. Adopting proper document management, including labelling/classifying documents, establishing access/permission levels (limiting access to trade secrets or parts of them to certain employees/consultants, etc.), tracking and recording access, encryption, password protection, and physical lock and key methods (including limiting location for access, limiting downloading, printing, and the creation of copies).

iv. Training employees (as well as consultants and third-party partners, as applicable) on appropriate measures to keep trade secrets safe; professionally remind departing employees and applicable third parties of their continuing confidentiality obligations.

v. Ensuring physical security: sign-in/sign-out procedures, security officers, physical security systems.

Last, policies and procedures should not be static. Laws change, so business and commercialization plans and priorities need to change, too, along with the technology used to protect trade secrets. It's imperative for businesses to review the aforementioned on a regular basis.

3. Employment law

Until recently, Canadian employers were able to utilize non-compete clauses in employment contracts as a tool to limit the disclosure of trade secrets. However, in November 2021, Ontario passed Bill 27, *Working for Workers Act*, which prohibits the use of non-compete clauses in Ontario through an amendment to the *Ontario Employment Standards Act*. This prohibition does not apply to "executives"[5] nor in situations relating to a condition of purchase or sale of a business or part of a business, and the seller thereafter becomes an employee of the purchaser.

Although non-compete clauses are generally unenforceable in Ontario, they may be in other jurisdictions across Canada and internationally. Lawyers in the applicable jurisdictions should be consulted for clarification. Further, a non-compete clause does not preclude an employment contract that has continuing confidentiality obligations that survive the terms of employment. Conversely, as a hiring entity, it also does not preclude provisions that prevent an employee or contractor from using third-party confidential information or trade secrets.

When it comes to protecting trade secrets, investing in good policies, procedures, and security measures should be seen as not just the cost of doing business, but an investment in a valuable asset. That asset can ultimately help distinguish the unique products and services of a business, and should be closely monitored, guarded, and contained.

[***Anita Nador*** *is a Partner specializing in the protection, commercialization and regulatory planning of IP and resulting products primarily in the life sciences and chemical sectors. She is particularly distinguished for her ability to pair sophisticated IP experience with corporate transactional and regulatory law, to assist clients in achieving their commercial goals. Anita is a lawyer and a registered patent and trademark agent.*

Madison MacColl *is an Associate working in the advertising and product regulatory practice group. Her practice includes developing and implementing IP strategies and advising on regulatory Health Canada matters.*]

---

1 *Criminal Code* (R.S.C., 1985, c. C-46) , section 391(1)

2 *Criminal Code* (R.S.C., 1985, c. C-46) , section 391(2)

3 *Criminal Code* (R.S.C., 1985, c. C-46) , section 391(5)

4 *Criminal Code* (R.S.C., 1985, c. C-46) , section 391(4)

5 "Executive" means any person who holds the office of chief executive officer, president, chief administrative officer, chief operating officer, chief financial officer, chief information officer, chief legal officer, chief human resources officer or chief corporate development officer, or holds any other chief executive position.