

# Criminal Enforcement of Trade Secret Theft: Strategic Considerations for Canadian SMEs

Matt Malone

*“As IP theft remains hard for firms to detect, much less obtain legal redress for, their incentives are to rely more on their own efforts to conceal trade secrets and less on patents that entail public disclosure. New estimates suggest that trade secret theft is between 1% and 3% of GDP, meaning that the cost to the \$18 trillion U.S. economy is between \$180 billion and \$540 billion.”*

Report of the Commission on the Theft of American Intellectual Property  
(2017)  
The National Bureau of Asia Research

Many innovative small and medium enterprises (SMEs) face unique challenges in protecting their intellectual property (IP). Potential theft of trade secrets is a key feature of these challenges, which arises often in the context of disputes related to employee mobility. Despite the risks these challenges pose, SMEs often confront significant resource barriers in protecting themselves from trade secret theft. The passage of a recent criminal law by the Canadian federal government, section 391 of the *Criminal Code*, creates a powerful new tool for innovative SMEs to report, investigate, and prosecute theft of trade secrets. It also comes with specific considerations and risks that innovative SMEs should examine and contemplate. This article explores strategies for SMEs in Canada to use section 391 to protect their trade secrets, navigate the legal environment during theft of a trade secret, and remediate such theft.

## Introduction and Background

Many innovative SMEs have a fraught relationship with intellectual property (IP). Lacking adequate financial resources, the formalistic mechanisms of IP protection can act as both temporal and financial cost barriers to legal redress when IP theft occurs (OECD, 2010). Minimal recourse to legal resources also prevents these actors from executing an IP protection plan with the same sophistication as their larger commercial counterparts (Cabeca & Chaperot, 2017.) SMEs may also lack a nuanced understanding of IP and human resources law, and thus remain vulnerable to certain pitfalls when operating against larger, resource-rich competitors, especially across multiple legal jurisdictions (OECD, 2010; Brant & Lohse, 2013.). Although IP cannot supplement solid knowledge and business fundamentals, it can be disproportionately vital

to the promise of growth and success for SMEs (French, 2010; Friesike, 2011.) For many of them, IP is in fact the crown jewel of their enterprise. The success for these SMEs is “underpinned by effective exploitation of intellectual assets” (Brant & Lohse, 2013.)

In short, IP is a serious issue for SMEs, in particular, for innovative SMEs that have the potential to contribute to long-term technological innovation. These business entities generally prefer more informal methods of protecting their IP (Kitching & Blackburn, 2003.) The doctrine of “trade secrets”, which eschews formal registration, is a common type of legal protection for such companies, one that combines low cost with potential permanent duration in legal protection for technologies that are not susceptible to reverse engineering or public knowledge. Yet trade secrets have specific drawbacks related to the costs associated with

## Criminal Enforcement of Trade Secret Theft: Strategic Considerations for Canadian SMEs *Matt Malone*

their effective investigation and litigation in the case of theft. Various IP protection models have been established to address the IP needs of SMEs, such as IP clinics and pro bono programs (Cabeca & Chaperot, 2017). However, the limitations of these models have also been highlighted (Dahl & Phillips, 2018), given that they are often not well-equipped to respond to investigation and litigation, as trade secret theft requires.

Thus, tensions over IP can arise that create unique challenges for innovative SMEs regarding theft of their trade secrets. Disputes over theft of trade secrets have been growing in recent years (Almeling, et al., 2010). This appears to be particularly true in two contexts that SMEs are prone to encounter by their very nature. The first situation involves the hiring by a competitor of an employee from an innovative SME (or an employee leaving an innovative SME to start a directly competitive enterprise). In such scenarios, trade secret theft may occur as the employee deploys not only their unique skills and talents, but also makes use of trade secrets from the SME that they left. The second common situation pertains to mergers and acquisitions, where a SME may enter discussions with a larger company, only to find that confidential circumstances in the discussion were breached, resulting in the misappropriation of trade secrets. Of course, these scenarios are not exclusive. However, both scenarios place an innovative SME into a position and posture where it is necessary to prosecute trade secret theft. And both may not only be harmful to a SME, but potentially destructive to the business. In sum, the stakes of potential trade secret disputes where an innovative SME must prosecute trade secret theft are of critical significance for how their business is conducted.

This article addresses the challenges faced by SMEs in navigating these tensions by examining a powerful new instrument for the enforcement of IP rights that stands to supplement the inherent resource shortcomings of SMEs in Canada – namely, section 391 of the Criminal Code. Section 391 offloads from SMEs who experience trade secret and confidential information theft the investigatory and prosecutorial responsibilities associated with seeking legal redress for these harms, and allocates these responsibilities to the state. In doing so, it provides a significant instrument in the defense and remediation of Canadian IP theft. At the same time, significant risks and specific considerations are involved in seeking assistance from law enforcement authorities when making a complaint under the aegis of section 391, which this article probes. Finally, this article provides

practical advice to SMEs in Canada seeking to file a complaint under section 391.

### The New Section 391 of the Criminal Code of Canada

Given the resource obstacles noted above, innovative SMEs have historically tended not to be predisposed to seek legal redress when trade secret theft occurs. However, the federal government recently revised the *Criminal Code of Canada* to provide an important new tool for innovative SMEs that experience trade secret theft: section 391. This new section sets forth that “[e]veryone commits an offense who, by deceit, falsehood or other fraudulent means, knowingly obtains a trade secret or communicates or makes available a trade secret” (Crim. Code, sec. 391). Section 391 defines a trade secret as “any information that is not generally known in the trade or business that uses or may use that information; has economic value from not being generally known; and is the subject of efforts that are reasonable under the circumstances to maintain its secrecy” (Ibid). Further clarification is given to note that information is not a trade secret when it was “obtained by independent development or by reason only of reverse engineering.”

The main elements of an offence under section 391 include:

- The defendant obtained, communicated, or made available a trade secret;
- The defendant knowingly acted by deceit, falsehood or other fraudulent means; and
- The information was a trade secret.

Section 391 was passed as part of an omnibus bill implementing the USMCA (effective since July 1, 2020), which required that all signatory parties “shall provide for criminal procedures and penalties for the unauthorized and willful misappropriation of a trade secret” (USMCA, art. 20.71). At the time of signing the USMCA, the United States of America already had a similar provision on the books in the *Economic Espionage Act*, which criminalizes economic espionage by a foreign entity, as well as commercial theft of trade secrets by a private party (U.S. Code, Title 18§ 1832 et seq). Although Canada has had economic espionage as a criminal offense on the books for years, under the auspices of the *Security of Information Act*, it had lacked

## Criminal Enforcement of Trade Secret Theft: Strategic Considerations for Canadian SMEs *Matt Malone*

an equivalent offense to the commercial theft of trade secrets between private actors where there was no foreign economic espionage element. Section 391 of the *Criminal Code of Canada* now fills this legal vacuum, though to the present date of writing this paper, section 391 has not yet been used in Canada.

### Significance of Section 391

What section 391 promises to do for innovative SMEs is not insignificant. It offers them investigatory and prosecutorial powers from the federal government to address instances of theft of trade secrets, providing them with resources that were previously only available to larger commercial actors that already possessed them. In doing so, section 391 gives innovative SMEs an opportunity to level the legal playing field.

In the past, the only available recourse for innovative SMEs in cases of trade secret theft were civil law remedies, such as filing for a breach of confidence, breach of fiduciary obligations, or breach of contract. This was resource-intensive to investigate and successfully litigate. In tackling a breach of confidence, courts in Canada always enjoyed “ample jurisdiction to fashion appropriate relief out of the full gamut of available remedies, including appropriate financial compensation”, which it was believed would put “the confider in as good a position as it would have been in but for the breach,” as well as the option of filing for injunctions (Cadbury, 1999.)

However, disputes over a breach of confidence pose practical challenges for SMEs as a legal instrument. If a dispute goes to court, one concern for SMEs is dealing with judges that are potentially incapable of understanding the technological and scientific issues at hand without the aid of expensive expert analyses to assist them. Moreover, the fact-intensive nature of trade secret disputes renders the remedies in such matters somewhat unpredictable. Because such disputes turn on factual questions (for example, defining the trade secret and the alleged misappropriation), discovery and litigation can drag on well past the summary judgment. All these factors breed uncertainty – and come with high legal costs. In sum, a breach of confidence is a resource-intensive form of legal protection that does not easily invite innovative SMEs to avail themselves of the law. Section 391 removes these resource burdens and presents far fewer resource obstacles, making the responsibilities of investigation and prosecution incumbent on the state.

Another significant change in the law is that section 391 alters the constitutive elements and punishments for theft of trade secrets. A breach of confidence is a three-part test that requires a party bringing forward an allegation of trade secret theft. The party must prove: 1) the subject matter at hand had a quality of confidence to it, 2) that it was imparted in circumstances obliging confidence, and 3) that it has been the subject of an unauthorized use to the detriment of the party who originally communicated it in confidence (Coco, 1969; Lac Minerals, 1989). If a party can prove these elements, it can generally obtain damages and/or an injunction. However, proving “unauthorized use” is a challenging standard. On the other hand, Section 391 only has an “intent” requirement that combines with a guilty act of “knowingly obtain[ing] a trade secret or communicat[ing] or mak[ing] available a trade secret” (Crim. Code, sec. 391). Finally, there is a difference in the resulting penalties with the new code. Whereas a breach of confidence may have brought a winning party damages and/or an injunction, liability under section 391 comes with punishment of committing an indictable offense bearing “imprisonment for a term not exceeding 14 years”, or summary conviction for which the penalty is a fine of not more than \$5,000 or term of imprisonment not exceeding six months or both (Ibid; Crim. Code, sec. 787).

Given the obstacles to prosecution presented by a breach of confidence case, many Canadian companies have instead historically litigated trade secret theft in the United States, if they could find some kind of nexus with that jurisdiction. In the United States, unlike in Canada, the federal government and nearly every state have statutes that permit private parties to bring a cause of action against other private parties. The federal statute provides a different and lower standard than the breach of confidence in Canada (U.S. Code, Title 18 §1832 et seq.). The same is true of US state-level statutes (UTSA, s. 1). Perhaps for this reason, many Canadian companies often avail themselves of American rather than Canadian law. For example, in 2018 Bombardier Aerospace filed suit against Japan's Mitsubishi Heavy Industries Ltd. for theft of trade secrets related to certifying regional jets. The underlying theft occurred in Quebec. But Bombardier did not file in Quebec or even in Canada. Rather, it filed in the Western District of Washington, the location of Aerospace Testing Engineering & Certification Inc., a third-party working with Mitsubishi on the certification of a 90-seat regional jet (Layne, 2020.) The case was notable for Bombardier's strategic decision not to file in Canada (and not to avail the

## Criminal Enforcement of Trade Secret Theft: Strategic Considerations for Canadian SMEs *Matt Malone*

company of home turf advantage), but rather instead to go on the offensive against theft of trade secrets in a less familiar foreign jurisdiction.

### Methodology

Having canvassed the IP challenges facing SMEs and the changes wrought by section 391, this article suggests that section 391 of the *Criminal Code* addresses many of these challenges. The article now proffers practical considerations, insights, and tools for SMEs that may consider or benefit from enforcing their legal rights under the auspices of section 391. Given the challenges for SMEs to protect their IP, and the significance of section 391, this paper reflects on two main strategic considerations: 1) strategic considerations that SMEs should take when deciding whether or not to lodge a complaint under the auspices of section 391, and, 2) if they decide on making a formal complaint, clear guidelines as to how it can be articulated, documented, and filed (along with preparatory steps that a SME should take if it decides to do so). In both of these areas, the article presents a comparative analysis with similar statutory laws in the United States, as well as practical litigation events in recent years as a way to understand legal trends.

### Examining the Strategic Implications of Section 391

The Canadian federal government has not yet given indication of what types of matters it intends to prosecute under section 391. But if the American example provides any lessons, innovative SMEs suspecting that theft has occurred under the auspices of a foreign actor will likely have the most success in convincing the federal government to take up prosecution. In the United States, prosecutorial guidelines advise government attorneys that are considering to file charges under the *Economic Espionage Act*, that “[t]he criminal enforcement of IP rights plays a critical role in safeguarding U.S. economic and national security interests ... our national security interests can be undermined by foreign and domestic competitors who deliberately target leading U.S. industries and technologies to obtain sensitive trade secrets that have applications in defense, security, or critical infrastructure” (Pros’g IP Crimes, 2020).

In the United States, the announcement of a “China Initiative” in December 2018, which sought to oppose Chinese misappropriation of intellectual property, coincided with a spike in prosecutions under the

*Economic Espionage Act* (China Initiative, 2018). The U.S. Department of Justice noted that 60 per cent of all trade secret theft cases brought during this time had “at least some nexus to China” (China Initiative, 2018; Morton, 2019). Although some observers may be inclined to view such actions as a particular obsession of current President Trump’s administration, it is notable that in 2011 President Obama’s administration released a document on the *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, which laid the groundwork for the future China Initiative, including the appointment of specialist attorney generals at each of the 97 U.S. Attorney Offices to prosecute theft of trade secrets (Administration Strategy, 2013).

The existence of a national security dimension is not the only factor that will go into whether a country’s federal government will prosecute such theft. The U.S. Department of Justice has created guidelines for economic espionage that specifically identify the following “discretionary factors” in determining whether or not to bring forward charges: “(a) the scope of the criminal activity, including evidence of involvement by a foreign government, foreign agent or foreign instrumentality; (b) the degree of economic injury to the trade secret owner; (c) the type of trade secret misappropriated; (d) the effectiveness of available civil remedies; and (e) the potential deterrent value of the prosecution” (DOJ Manual, 2018). One notable Canadian practitioner of trade secret law recently opined that the federal government should develop similar prosecution policies to these, as a form of guidance to actors in the private sector (Courage, 2020).

These considerations aside, in Canada there are several important risks inherent in reporting theft of trade secrets to law enforcement. Although law enforcement has powerful investigatory and prosecutorial tools (and at no cost to the reporting party), reporting trade secret theft as a crime has potential downsides. Some of these are ancillary, such as potential bad publicity, while others are more essential, including the loss of control over proceedings when law enforcement assumes control to investigate and the Crown (i.e., government attorneys) prosecutes. Delays can also be a major issue. As even the Supreme Court of Canada noted in *R. v. Jordan* (2016): “a culture of complacency towards delay has emerged in the criminal justice system” (*R. v. Jordan*, 2016). Given that time is often a crucial consideration for innovative SMEs – including being one of the reasons in the first place that they resort to “trade secret” status for assets, rather than going for patents, which require a

## Criminal Enforcement of Trade Secret Theft: Strategic Considerations for Canadian SMEs *Matt Malone*

lengthy registration process – such attitudes may discourage SMEs from seeking out the assistance of law enforcement and the Crown.

A supplementary concern is the confidentiality of the proceedings. As noted above, one concern of trade secret litigation is that it can thwart the discovery process during litigation (i.e., the period when parties in a lawsuit make available to one another all relevant evidence). Such can occur if the discovery process were used not to locate and prove instances of misappropriation, but rather to locate trade secrets themselves, as a fishing expedition. Another major concern for SMEs is that, in Canadian government-led prosecutions, the Crown has specific disclosure obligations. As in the United States, where confidentiality is not wholly guaranteed in light of the 5th Amendment and *Brady* obligations, in Canada legal precedent requires that “the Crown is under a general duty to disclose all relevant information” to the defense (R. v. Stinchcombe, 1991). Additionally, innovative SMEs may reasonably doubt the Crown’s ability to safeguard and keep information confidential. For example, in 2019 it was revealed that the RCMP’s Director General of National Intelligence was arrested (case still ongoing) on charges of allegedly communicating confidential information (Tunney, 2020). Similarly, in 2020 the Revenue Canada website was subject to a notable data breach (Patel & Ling, 2020).

Finally, although it is an obvious point, a further important consideration for an innovative SME when considering to ask the federal government to prosecute trade secret theft is confirming the existence of trade secrets. Such lawsuits can sometimes be used by companies as battering rams to discourage innovation—something courts seek to discourage through measures like cost and fee awards in civil cases. Although this consideration may not entirely translate to the criminal law, filing a false report carries significant penalties (Crim. Code, s. 140). Thus, somewhat similar dynamics play out as in cost and fee awards. A prerequisite of most civil litigation is that the trade secrets at the heart of the dispute be identifiable, so as to allow a court to assure that the dispute is not meritless (and also that the dispute is not, in fact, just a strategy to force a party to disclose their trade secrets through litigation techniques like the discovery process). It also allows the defense to proffer defenses, such as reverse engineering or public knowledge. Thus, any entity contemplating litigation should confirm that their claim has a solid good faith basis before filing the complaint.

Further, a party is more likely to obtain the support and interest of law enforcement authorities if the allegation of misappropriation of trade secrets is specific and narrow, rendering the complaint more easily susceptible to verification (as opposed to a making a kind of laundry list accusation).

### Responding to Trade Secret Theft with Section 391

Despite the existence of section 391, the Canadian federal government has thus far provided little guidance to victims of trade secret theft. Section 391 has not come accompanied with meaningful guidance as to how companies, and in particular, innovative SMEs – may avail themselves of the law. This differs markedly from the situation in the United States, where the Department of Justice published (2013) *Reporting Intellectual Property Crime: A Guide for Victims of Copyright Infringement, Trademark Counterfeiting, and Trade Secret Theft*. This DOJ guideline urges victims of trade secret theft to fill out a victim checklist with many useful instructions, including:

- Background and contact information
- Description of the trade secret
- General physical measures taken to protect the trade secret (including the existence of confidentiality and non-disclosure agreements, computer infrastructure descriptions, document controls, and employee controls)
- Description of the theft of trade secrets
- Background on whether civil proceedings have been filed (Rep’g IP Crime, 2013)

This checklist then instructs victims to provide a copy to a federal law enforcement official (Ibid). Helpfully, the checklist also includes reproductions of the language of relevant legal provisions. The Canadian federal government does not offer such guidelines, but now that the underlying criminal law is effectively the same, an innovative SME that has been the victim of trade secret theft can borrow the DOJ checklist and use it to conduct their forensic analysis of trade secret theft. Upon completion of the report, they can provide it to the RCMP or a police force jurisdiction where the innovative SME is located, in the same way that they would report any criminal offense. In addition to such measures, basic

## Criminal Enforcement of Trade Secret Theft: Strategic Considerations for Canadian SMEs *Matt Malone*

steps should be taken once an SME becomes aware of a trade secret theft to preserve evidence, in particular any records that have monitored the transmission of data and tracked employees that may document the theft.

Finally, although this paper has focused on measures from the perspective of taking a defensive posture towards IP, which is relevant for a SME suffering theft of trade secrets, such entities should also be alert to the concern that section 391 may be mobilized against them. As one practitioner noted: “Disputes between companies and their departing employees or former business collaborators can also be very polarized and intense, making it further difficult to judge the facts well enough at the outset to decide whether to lay charges” (Courage, 2020). Thus, companies should undertake careful measures to avoid potential theft to their trade secrets, including through employee training on best practices handling any information that may be susceptible to such designation.

### Conclusion

Section 391 is a powerful instrument for SMEs in Canada to protect their IP. It makes up for many resource deficiencies that they experience, in particular vis-à-vis their larger competitors. However, recourse to section 391 comes with specific advantages and disadvantages that this paper has laid out for SMEs to contemplate. Further, this paper has provided practical advice for initiating a complaint under section 391.

Innovative SMEs should take seriously the important measures they put in place to protect their trade secrets. Routine audits are an important way for such companies to think on a regular basis about how they govern and restrict access to information, including what employment policies they have in place, and how employees are trained to protect such information. Business measures like this are of central importance in court. While these prophylactic measures can go a long way in preventing the misappropriation of trade secrets, in the event that something is stolen, they also form important pillars in building a case for prosecution by helping harness evidence to build a persuasive legal narrative. If theft of a trade secret occurs, a SME should undertake immediate steps to preserve whatever evidence of it they have available to them.

This article addressed the challenges that Canadian SMEs face in protecting their IP due to resources

deficiencies. It focused on a recent solution to these deficiencies presented by section 391 of Canada’s *Criminal Code*. It took into account considerations for SMEs when turning to this new legal protection, including advantages and drawbacks to enforcement, and devised a practical suggestion of utilizing the checklist prepared by the DOJ as a tool to report relevant information to the RCMP, or police force in another jurisdiction (or even simply to make a record for themselves) in the event of trade secret or confidential information theft. Going forward, in addition to the federal government developing tools that are specifically designed for SMEs to assist effective enforcement, further research will be needed to examine the ways in which such enforcement should be structured, expanded, and also limited to maintain a robust innovation environment in Canada.

### References

- Almeling, D.S., Snyder, D.W., Sapoznikow, M., McCollum, W.E., & Weader, J. 2010. A Statistical Analysis of Trade Secret Litigation in Federal Courts. *Gonzaga Law Review*, 45:2: 291-334.
- Brant, Jennifer, and Lohse, Sebastian. 2013. Enhancing Intellectual Property Management and Appropriation by Innovative SMEs. International Chamber of Commerce. *Innovation and Intellectual Property Research Paper No. 1*.
- Cabeca, John, and Chaperot, Ivan. 2017. SMEs and Patents in the United States. *Les Nouvelles - Journal of the Licensing Executives Society*, Volume LII, No. 4.
- Cadbury Schweppes Inc v FBI Foods Ltd. 1999. 1999 *CanLII 705* (SCC) at para 61, 167 DLR (4th) 577.
- Canada. *Criminal Code*, RSC. 1985, c C-46, s. 391.
- Canada. *Criminal Code*, RSC. 1985, c C-46, s. 787.
- Canada. *Security of Information Act*, R.S.C., 1985, c. O-5, s. 19.
- Coco v. A.N. Clark (Engineers) Ltd. 1969. *R.P.C. 41* (Ch.).
- Courage, Noel. 2020. *The Past and Future of Canada’s Criminalization of Trade Secret Theft – Part II*. March 3, 2020. Bereskin and Parr.
- Dahl, Cynthia, and Phillips, Victoria F. 2018. Innovation and Tradition: A Survey of Intellectual Property and Technology Legal Clinics. *Clinical Law Review*, 25:95.

## Criminal Enforcement of Trade Secret Theft: Strategic Considerations for Canadian SMEs *Matt Malone*

- French, D.J. 2010. Why Intellectual Property Will Not Save the Canadian Economy. *Open Source Business Resource*.  
<http://timreview.ca/article/396>
- Friesike S. 2011. Profiting from Innovation by Managing Intellectual Property. *PhD thesis*. University of St. Gallen.
- Kitching, John, and Blackburn, Robert A. 2003. Innovation, Intellectual Property and Informality: Evidence from a Study of Small Enterprises and Some Implications for Policy. *University of Illinois at Urbana-Champaign's Academy for Entrepreneurial Leadership Historical Research Reference in Entrepreneurship*.
- Lac Minerals Ltd v International Corona Resources Ltd. 1989. 2 SCR 574, 1989 SCJ No 83.
- Layne, Nathan. 2018. Bombardier sues Mitsubishi jet program over trade secrets. *Reuters*.
- Macdonald, Stuart and Lefang, Bernard. 2003. Worlds Apart: Patent Information and Innovation in SMEs. *University of Illinois at Urbana-Champaign's Academy for Entrepreneurial Leadership Historical Research Reference in Entrepreneurship*.
- Morton, Mindy. 2019. *Why Companies Should Care about Increasing Criminal Enforcement of Trade Secret Theft*. Procopio LLP.
- Obama, Barack. 2013. President of the United States. *Administration Strategy on Mitigating the Theft of Trade Secrets*. February 2013.
- OECD. 2010. *Innovative SMEs and Entrepreneurship for Job Creation and Growth: 'Bologna + 10' High-Level Meeting on Lessons from the Global Crisis and the Way forward to Job Creation and Growth*. OECD Publishing, Paris.
- Patel, Raisa and Philip Ling. 2020. CRA shuts down online services after thousands of accounts breached in cyberattacks. *CBC News*.
- R. v. Jordan. 2016. SCC 27 (CanLII) at para. 40, [2016] 1 SCR 631.
- R. v. Stinchcombe. 1991. 1 CanLII 45 (SCC), [1991] 3 SCR 326.
- United States Department of Justice. 2013. *Reporting Intellectual Property Crime: A Guide for Victims of Copyright Infringement, Trademark Counterfeiting, and Trade Secret Theft*. Computer Crime and Intellectual Property Section.
- Tunney, Catherine. 2020. New charges claim RCMP official 'intentionally' shared operational information back in 2015. *CBC News*.
- Uniform Law Commission. *Uniform Trade Secrets Act*, s. 1, para. 2.
- United States-Mexico-Canada Agreement*, art. 20.71.
- United States Code. *Title 18 §1832 et seq.*
- United States Department of Justice. 2018. *Attorney General Jeff Session's China Initiative Fact Sheet*.
- United States Department of Justice. 2018. *China Initiative*.
- United States Department of Justice. 2015. *Prosecuting Intellectual Property Crimes*. 4th Ed. Office of Legal Education for United States Attorneys.
- United States Department of Justice. 2018. *Department of Justice Manual*: Section 9-59.100.

### About the Author

Matt Malone is a Canadian-trained lawyer with an interest in law and technology. He has practiced trade secret law in Silicon Valley for several years. Prior to that, he worked at the Centre for International Governance Innovation, Bombardier Aerospace, and the Centre for Intellectual Property Policy. His research has been published in various peer-reviewed journals, including *The Advocates' Quarterly*, *Canadian Class Action Review*, and *Canadian Intellectual Property Review*.

Citation: Malone, M. 2020. Criminal Enforcement of Trade Secret Theft: Strategic Considerations for Canadian SMEs. *Technology Innovation Management Review*, 10(11): 40-46.  
<http://doi.org/10.22215/timreview/1402>



Keywords: Trade secrets, confidential information, criminal law, enforcement, economic espionage, Small and medium-sized enterprises