Tips for Preserving Trade Secrets in the Age of Virtual Meetings

October 19, 2020

By Victor Krichker, Justin Philpott and Paige Newman

The COVID-19 pandemic has fundamentally altered the way business is conducted. Face-to-face meetings have moved online via popular videoconferencing platforms, such as Zoom™ and Cisco Webex™. It is a trend that shows no signs of slowing. This massive shift to videoconferencing can present a number of challenges to businesses that own valuable trade secrets. When determining whether to grant trade secret protection, Canadian courts weigh the measures taken by the trade secret owner to protect the secrecy of their information. With insufficient protective measures in place, the trade secret owner risks losing their lawsuits. In an article published last year, we provided trade secret owners with a list of measures that can be put in place to protect the secrecy of their information. In this article, we provide an updated set of measures geared to avoiding the trade secret pitfalls associated with videoconferencing.

Unlike patents, trademarks and copyright that are protected by federal statutory regimes in Canada, trade secrets are not granted statutory protection by Canadian federal law. Instead, companies primarily rely on the common law in Canada for remedies for trade secret theft and other misappropriation, and typically pursue these remedies in the provincial courts by suing for breach of confidence. In an action for breach of confidence, the onus is on the plaintiff to prove that the misappropriated information was confidential and that the information was communicated in confidence[1]; in other words, the plaintiff must demonstrate that the information was in fact a secret and that the individual(s) who misappropriated this information knew it was a secret.

In the recent U.S. decision *Smash Franchise Partners, LLC v Kanda Holdings, Inc. [Smash]*, the court was dissatisfied with the measures taken by the plaintiffs to protect the information disclosed during Zoom meetings. The plaintiffs organized recurring Zoom meetings as a way to discuss franchising opportunities. Among the topics discussed were the plaintiff's business strategy, pricing models, current territory, the identity of certain customers, and growth opportunities. However, these Zoom meetings were open to anyone who had the meeting ID. All of the subsequent Zoom meetings used the same meeting ID, and none required a password. Further, many participants had not signed a non-disclosure agreement (NDA). These factors led the court to conclude that the information disclosed by the plaintiff during their many Zoom meetings was non-confidential in nature. In effect, the plaintiffs failed to show the court that the misappropriated information they were claiming to be confidential was treated any differently than non-confidential information.

The *Smash* decision is a timely warning to trade secret owners. It demonstrates the perils of insufficiently protecting one's confidential information while using videoconferencing platforms. While there are differences between U.S. and Canadian trade secret law, the U.S. court's analysis in *Smash* is comparable to how a Canadian court would weigh the protective measures taken by a trade secret owner in a videoconferencing context. The following protective measures stand out:

- Require the participants of each videoconference to enter a password[2]
- Vary meeting passwords from videoconference to videoconference so that individuals are only allowed to enter the videoconference they are authorized to join (e.g. if the same meeting password is used for all meetings, having access to that one password can allow an individual to join every videoconference[3])
- Use the "waiting room" feature provided by many videoconferencing platforms to screen videoconference participants (e.g. have the meeting organizer verify the identity of the participants before allowing them into the "meeting room")[4]
- Take attendance of everyone in the videoconference before it begins[5]

- Remove individuals from the videoconference who are not authorized to participate[6]
- Disable the recording feature of the videoconference platform so that participants are prevented from recording the videoconference[7]
- Request that employees working away from the office are not in a public space while participating in videoconferences where confidential information is disclosed[8]
- Continually identify the disclosed information that is considered confidential to all participants in each videoconference[9]
- Require all individuals to return a signed NDA before any videoconference in which confidential information is to be disclosed[10]
- Provide the information needed to connect to the videoconference only to those who have returned a signed an NDA[11]
- Explicitly indicate which information is intended to be confidential within the NDA (e.g. an NDA that stipulates that all of the disclosed information is confidential is not as strong as one that explicitly sets out the specific type(s) of information considered confidential)[12]

Many of the protective measures in the list above involve using safety features that are built into many videoconference platforms. If the *Smash* decision is any indication, not using these standard safety features can severely impact the plaintiff's ability to demonstrate that sufficient protective measures were in place.

Key Takeaways

The objective of implementing measures to protect the secrecy of confidential information is twofold. First, they provide practical value by guarding against the misappropriation of the information in the first place. Second, in the event of a dispute, they demonstrate to the court that sufficient measures were taken to preserve the confidential nature of the information. Courts are unlikely to order monetary damages or grant an injunction for misappropriated information if the plaintiff is unable to demonstrate that they had taken sufficient measures to protect their trade secrets.

Whether your business relies on videoconferencing or not, the key takeaway is the same. If you want the court to enforce the misappropriation of your trade secrets, then you need to treat your trade secrets like secrets. In a videoconferencing context, the non-exhaustive list above provides several measures that a Canadian court may view favourably when determining if misappropriated information possesses the necessary "quality of confidence" to be considered a trade secret[13] It should go without saying that the more vigorous the protective measures in place, the greater the likelihood that a court will find that this condition is met.

---

1 *International Corona Research Ltd v Lac Mineral Ltd*, [1989] 2 SCR 574 at 635-36, citing Coco v AN Clark (Engineers) Ltd, [1969] RPC 41 at 47 (Ch).

2 *Smash Franchise Partners, LLC v Kanda Holdings, Inc., 2020 Del. Ch. LEXIS 263 (Del. Ch. August 13, 2020).*

3 *Ibid*.

4 *Ibid*.

5 *Ibid*.

6 *Ibid*.

7 https://www.law.com/therecorder/2020/05/21/whos-watching-hidden-dangers-to-trade-secrets-from-video-conferencing/

8 *Stonetile (Canada) Ltd v Castcon Ltd*, 2010 ABQB 392 (CanLII) at para 26

9 *Ibid*.

10 *Supra* note 2.

11 *Ibid*.

12 *Supra* note 8 at paras 28-9.

13 *GasTOPS Ltd v Forsyth*, 2009 CanLII 66153 (ON SC) at para 124, aff'd 2012 ONCA 134.