IN THE SUPREME COURT OF BRITISH COLUMBIA

Citation: *Skycope Technologies Inc. v. X.L.,*
2024 BCSC 1885

Date: 20240830
Docket: S246016
Registry: Vancouver

Between:

Skycope Technologies Inc.

Plaintiff

And

X.L.

Defendant

Before: The Honourable Madam Justice Sharma

Oral Reasons for Judgment

(*In Camera*)

Counsel for the Plaintiff:	B. Duong H. Cook D. Wotherspoon R. Hamoni, Articled Student
Place and Date of Trial/Hearing:	Vancouver, B.C. August 30, 2024
Place and Date of Judgment:	Vancouver, B.C. August 30, 2024

[1] This is the written version of judgment delivered orally on August 30, 2024. Edits have been made to improve grammar and style and to add references to case law. Edits also include clarification to or addition of facts, identified by content in italics and enclosed in square brackets. Nothing about the analysis or conclusions has been altered. In addition, the defendant is identified by initials pursuant to an order I granted on October 10, 2024. Because of that Order, I also delayed publication of this judgment for seven days after distribution to the parties to ensure counsel could seek further alterations in order to be consistent with the anonymization order, or protect information sensitive to national security interests.

[2] **THE COURT:** This is an application brought *ex parte* on an urgent basis for an *Anton Piller* order. The plaintiff also seeks to have the hearing and reasons delivered *in camera* and applies for an interim injunction and sealing order.

[3] The circumstances why these other measures are being sought and why I am granting them will be explained in due course. I will state at the outset that there are facts about this case that make it somewhat unusual, and those explain, in part, why I agreed to conduct the hearing and deliver judgment *in camera*. I refer to the evidence in this matter that carries potential implications on Canada's national security interests.

[4] I acknowledge the assistance of counsel who were forthright and candid in complying with their duty when seeking an *ex parte* order to provide full and frank disclosure, including identifying potential arguments that the defendant might have raised had he been here to oppose the orders. I also confirm that I have had time to fully review the application record.

FACTS

The Plaintiff

[5] The plaintiff is in the anti-drone technology business. It develops and markets technology aimed at detecting, identifying and neutralizing drones which enter unauthorized airspace. This is its core business.

[6] In order to be able to detect a new model of drone, the plaintiff first obtains a model of it, records its radio frequency data and analyzes the structure of the signals. The analysis involves research to detect and identify unique properties and features or “fingerprints”. This process is described in one of the affidavits by analogy: the process involves figuring out what language the drone uses to communicate with its remote controller.

[7] This signal analysis methodology took the plaintiff years to develop through trial and error. Skycope has successfully detected a large number of drone “languages” through this process, creating what it calls a drone library, which is one of its main assets. The plaintiff values and guards not only the end result of all of the years of research that it did, which includes the drone library, but also the process it developed. It asserts that confidentiality is essential to its business.

[8] In his affidavit, Hamidreza Boostanimehr, the plaintiff’s chief executive officer (the “CEO”), described in general terms drones and their common commercial, industrial and potential harmful uses. He also described how drones are controlled by remote controllers through radio frequency signals or “protocols”. He explained that each drone model’s protocol is either standard or unique. In addition, protocols of different models may be similar in the same way that, for instance, French is similar to Spanish in that they have a common root language, or protocols could be very different in the way that Chinese and French are extremely different.

[9] The CEO deposed that the two largest manufacturers of drones use unique, proprietary protocols.

[10] He also described how the plaintiff developed technology to detect what specific model of drone enters a particular airspace, and how they crack these protocols. He explained that at the time the company was developing this technology, it was novel, and he described the time and effort it took to develop it.

[11] Once a drone’s protocol is detected, a device can be created to transmit signals that essentially jams the drone. The plaintiff's key hardware in that regard is

called SkyEye. In addition, once a model of a drone's protocol has been detected or cracked, it is added to the plaintiff's drone library. That is a key asset, and it is kept strictly confidential. The CEO deposed that he believes the plaintiff has the largest drone library in the market, making it an industry leader and distinguishing it from many competitors.

The Defendant

[12] The defendant has been employed by the plaintiff since 2018. He is a member of the team that conducts wireless research and development.

[13] On August 16, 2024, the defendant told the plaintiff that he was resigning. At that time, he only stated that he was pursuing new opportunities. In a reply email, the CEO asked to speak to him to see if there was anything the company could do to keep him on as an employee. The CEO and the defendant had a meeting on August 19, 2024, and the defendant identified financial renumeration as a main reason that he was leaving.

[14] The amount of money the defendant would be making [*approximately 50% more in the new position, tax free*] raised a concern in the CEO’s mind given what he understood the defendant would be doing at his new opportunity. [*The CEO deposed that amount of money for a wireless researcher, his current role at Skycope, seemed high and unrealistic*]. This caused the CEO to ask the defendant if he would be joining another company involved with anti-drone technology. The CEO asked this question because the plaintiff had a dispute with a former employee which resulted in litigation, so the CEO was alive to the possibility of an employee starting a new company or going to a competitor.

[15] The manner of how the defendant responded to that inquiry raised further suspicion because his answer was slightly evasive or vague. The defendant stated he was leaving for a company that was not an anti-drone company “in the way they represented themselves”. The CEO deposed that gave him pause immediately.

[16] The CEO also recounted how, within the last year, he was concerned that the defendant was using a note-taking application called “Obsidian” to log progress on files. In that conversation the defendant mentioned how he would upload his notes to a cloud server so that they could be accessible anywhere. That was flagged immediately by the CEO as a potential security risk, and he told the defendant to stop doing that.

[17] This particular evidence is important. The company had an existing concern regarding a potential breach of the employment contract by the defendant due to his insufficient precautions to safeguard the confidential information even before knowing about his plan to go to a new job. I am not making a specific finding that he did breach his employment contract. Instead, I am saying there is evidence that supports why a concern was raised. It also shows the seriousness with which the plaintiff guards its confidential information and the extent of its vigilance about it.

[18] Given the suspicion raised by this past conversation, the CEO, with another employee, decided to log into a company computer that they knew the defendant frequently used. It was accessible using one of the company's standard passwords. In my understanding, it was a workstation that any employee of the company would be able to access.

[19] In his affidavit the CEO details how it was part of his job to monitor the work of members of the wireless research team that the defendant was on. [*As such, the CEO directly managed the defendant, and the team held bi-weekly meetings where tasks were delegated, progress was reviewed, and plans were made. The team’s work process and results were documented internal to Skycope, and is confidential. The internal documentation, as well as internal messaging tool used by Skycope, allowed the CEO to monitor the defendant’s work and his contribution to Skycope’s projects.*]

[20] Upon logging into that work computer, they saw that the note-taking application, Obsidian, was there. The CEO deposed that he believed it contains source code that appeared to be reproduced from the drone library, as well as data

and key findings about various protocols. He could not understand why those items would be in these Obsidian notes, and that is relevant when I come to talking about the test for an *Anton Piller* order.

[21] However, upon accessing that computer, the CEO also noticed that the defendant was logged into his personal Gmail account. That means that they did not have to input an email or password because the email application was already open. Without entering any search terms, they were able to see that the defendant had exchanges with a company called BeamTrail, which is located in Abu Dhabi. I will come back to the significance of that later, but the fact that they did not enter search terms, in my respectful view, shows that there was at least some acknowledgement of the possible need for caution in accessing what might be termed more personal information. I am not making that finding, but I note the CEO was alive to that issue.

[22] What became apparent to the CEO by looking at the email account was that on at least two occasions, the defendant had disclosed information documenting the process of how two proprietary drone protocols were cracked, and he did so in an apparent process of being interviewed for a new job. One disclosure was to someone at BeamTrail, and BeamTrail is regarded as a competitor of the plaintiff. The emails revealed that he accepted a job with BeamTrail in mid-July. I am referring to the facts that are set out in the notice of application, paragraphs 16 to 18, and I confirm this is supported by the affidavit evidence that has been filed. I also will address later the fact that BeamTrail is located in the United Arab Emirates (UAE), which raises potential national security issues.

[23] The CEO deposed that he saw that the defendant had entered source code that appeared to have been reproduced from the drone library in Bitbucket [*a database that contains the drone library in a password-protected folder, which only members of the wireless research team have access*], as well as data and key findings about various protocols in his notes. They also saw a Dropbox folder for Obsidian, as well as Obsidian vault. The CEO believed these files may contain source code that should properly only be stored in the drone library on Bitbucket, as

well as data and key findings about various protocols that should only be stored on the plaintiff's Google drive. He also indicated that the Dropbox account featured a list of devices that may have in the past, or could currently, access that account.

[24] In his affidavit, the CEO discussed a PowerPoint slide presentation that the defendant shared with BeamTrail. Significantly, he identified information in that presentation regarding one particular drone protocol which Skycope received in confidence from the Department of National Defence. The presentation shared with BeamTrail included the defendant's conclusions about the type of signal that the drone protocol uses, and it matched a conclusion that was referenced in progress notes that the company kept from March 2023. There was a slide identifying a particular tool that is typically used to identify protocols that did not work in this instance, followed by the slides stating, "My solution," which showed how the defendant successfully worked around that.

[25] These very specific examples in that document match progress that was logged during a very specific task when the team was working to crack the code of a particular drone.

National Security Concerns

[26] The plaintiff's technology has potential national security implications in many respects. One way is that it received confidential information from the Department of National Defence relating to one of the products alleged to have been part of the information that the defendant disclosed to BeamTrail.

[27] Furthermore, it is public knowledge that the plaintiff has participated in a Government of Canada program initiated by, and of interest to, the military. The program was to test the ability to successfully jam particular types of drones. The plaintiff company performed well, achieving a 100% success rate. It has published that on its website, no doubt as a marketing effort, but it had to get the published content on its website vetted and approved by the Department of National Defence given the security implications.

[28] What is important about this is that it is public knowledge that the anti-drone technology is of significant interest to the military. Because of this known military utilization of drones, the CEO deposed that the plaintiff pays close attention to sanctions imposed by the Canadian government dealing with commercial relationships with foreign entities and state actors. In particular, he deposed that recent events, [*such as a news article alleging that a Russian university had acquired the plaintiff's technology, which required the plaintiff to refute its involvement; as well as the Government of Canada ordering the plaintiff's competitor to cease operations after conducting a national security review*], reinforced his view that vigilance is required by the company in the conduct of its business. That is because, if their technology ends up in the wrong hands, it could mean serious financial penalties. However, he also expressed the concern regarding damage to Canadian interests in the larger geopolitical way.

[29] With respect to BeamTrail, the plaintiff has adduced evidence that it is likely a subsidiary of a much larger Emirate company, Edge Group. It is also notable that the plaintiff sold a SkyEye to BeamTrail in August 2022.

[30] Some of the following information may not be direct, but I am satisfied that it is appropriate in the unique circumstances to rely on what might be hearsay evidence. In my view, there are sound reasons to do so. The information comes from a business consultant who is not subject to employment confidentiality terms. The CEO explained how he considered it imprudent to get an affidavit from that person given the confidentiality surrounding everything else. That person happens to be the main point of contact between the plaintiff and BeamTrail.

[31] In any event, I am satisfied on the evidence that at one time the plaintiff understood that BeamTrail was interested in buying only the software from the plaintiff. That is not something the plaintiff would do. As explained, the plaintiff does not sell its software as a standalone product. It sells devices, like the SkyEye, and those devices have proprietary software encrypted and imbedded within them. While I understand it would not be impossible, it would be extremely difficult to reverse

engineering the software or any of the other proprietary information if one had the hardware. It is likely the case, however, that if one had the software, it would be slightly less difficult to reverse engineering.

[32] In any event, the CEO deposed that he believes BeamTrail was interested in getting the software in order to take advantage of the drone library to input that into its locally developed hardware. There is evidence before me that it expressed an interest in getting the software as a standalone product on more than one occasion.

[33] This brings me to the expert report that was adduced in evidence. I am satisfied that that report comes from an expert who is qualified to give opinion evidence on foreign threat activities, actors and risks relative to Canadian persons, organizations or corporations, and sensitive technology as they operate in Canada and abroad. He also consulted, without disclosing any confidential aspects of this case, with other people that agreed with his opinion who had expertise in areas regarding national security, among other things.

[34] The expert's opinion was based on his experience and knowledge, as well as open-source material. He made a number of relevant findings. I do not intend to read all of them out.

[35] He was asked to advise on security risks arising from foreign threats to individuals or businesses operating in the UAE, including technology or aerospace sector with military applications. While he opined that the security risk is considered low to medium for corporations and persons operating in the UAE generally, the security risk is considered medium to high when operating in the technology or aerospace sector with military applications depending on the specific technology for military application. He stated that if the technology pertains to drone warfare, the security risks would tend to be at the higher end, and that clearly applies in this particular case.

[36] The second question had a much longer response. He was asked to provide a threat assessment laying out the particular security risk in the circumstances of an

assumed set of facts, which I will not read out. What is important are a number of his findings and conclusions. I am not going to articulate all of them, but will focus on the findings and opinions that I consider to be important.

[37] The defendant graduated from an institution in China that had well-known links to the state's security agency. As such, the expert opined his position with the plaintiff would likely be well-known to China. The defendant's public profile on LinkedIn confirms that he is engaged in drone technology.

[38] BeamTrail is believed to have a parent company, Edge Group, which is a military and defence contractor in the UAE. Edge Group has publicly stated its willingness to supply products to Russia, and it is known to be in the drone supply business. It likely possesses significant cyber capabilities. The Edge Group has publicly stated its willingness to support Chinese and Russian defence entities through trade.

[39] The UAE has been actively engaged in evading sanctions regarding Russia according to open-source reporting. Given Russia's current war with Ukraine and the wide use of drones, Russia would likely have a keen interest in acquiring anti-drone technology. There is no extradition treaty between the UAE and Canada.

[40] The expert commented that even if the defendant had no intent to further disclose proprietary information, there is a large Russian and Chinese intelligence presence in the UAE and they would be interested in acquiring sensitive data such as the type to which the plaintiff had access. The expert expressed a view that the agencies could easily use inducements or leverage in an "accommodating operational theatre" like the UAE against potential employees in order to encourage their cooperation.

[41] He mentioned that the UAE is home to several terrorist groups that would be keen to acquire anti-drone technology. He noted that the defendant is a Chinese citizen, and that China has passed laws that may compel Chinese citizens, including

Chinese-Canadians, to share intelligence with state actors, thus allowing them to directly collect or share information.

[42] All of the foregoing gives context to the type of security concerns that may arise.

[43] The expert then gave his specific opinion. He assessed the future working/living context in the UAE to be a high security risk to the defendant given his knowledge of the technology, and the UAE entity's knowledge that he may be able to access or provide critical sensitive information. I am not going to read out the rest of the bullets in his report because of the sensitivity of that information However, they are all highly relevant to all of the issues before me.

***ANTON PILLER* ORDER**

[44] The test is well-known: (1) the plaintiff must demonstrate a strong *prima facie* case; (2) the damage to the plaintiff or the defendant's alleged misconduct, potential or actual, must be very serious; (3) there must be convincing evidence that the defendant has in its possession incriminating documents or things; and (4) it must be shown that there is a real possibility that the defendant may destroy such material before the discovery process can do its work: *British Columbia (Attorney General) v. Malik*, 2011 SCC 18 at para. 29. The purpose of an order is for the preservation of evidence that arises from the inherent jurisdiction of this Court: *Malik* at para. 31.

[45] The Supreme Court of Canada has confirmed that the court can make an order for the detention, custody and preservation of property that is subject to a proceeding, or where a question may arise that the property is subject to a proceeding. An *Anton Piller* order includes the court authorizing persons to enter upon any land or building in order to detain, take custody or preserve evidence. They are granted typically *ex parte* to ensure that a defendant cannot circumvent the court's process by being forewarned and making relevant evidence disappear. That is why it is so important that the applicant provide full and frank disclosure, and, as I have said, I am satisfied that has occurred here.

[46] Many cases have been reported where an *Anton Piller* order has been granted to deal with employees who are leaving an employer where they may have breached a duty of confidence: *Peters & Co Limited v. Ward*, 2015 ABCA 6; *Teledyne Dalsa, Inc. v. BinQiao Li*, 2014 ONSC 323; *Johnson v. Helo Enterprises Inc.*, 2012 ONSC 5186; *FLS Transportation Services Limited v. TRAFFIX Group Inc.*, 2024 BCSC 1078 [*FLS Transportation*].

[47] The plaintiff fairly acknowledges some aspects of this case that are worthy of the court's scrutiny. First, once the plaintiff had a suspicion that the defendant had potentially breached confidence or was potentially going to work for a competitor, it accessed his Gmail account which is personal to him. The plaintiff acknowledges that this could give rise to an equitable argument based on the plaintiff not having clean hands. It also points out that this is potentially a concern about breach of the defendant's privacy.

[48] However, the defendant had logged onto his personal email account and his Dropbox account on a work computer to which only employees had access. That is, he signed onto those accounts and did not log out. Therefore, logging onto the common computer, those applications were essentially open. It is arguable that he left his private information essentially in plain view, assuming that it was private. That tempers—possibly to a great extent—any privacy interest he may have had.

[49] I am also aware of the case law and academic commentary suggesting that employees have a diminished right of privacy when using work computers: *York Region District School Board v. Elementary Teachers' Federation of Ontario,* 2024 SCC 22 at para. 103; Steven M. Penney, "The Digitization of Section 8 of the Charter: Reform or Revolution?", 2014 67 *Supreme Court Law Review* 505, 2014 CanLIIDocs 33331 at 518–19.

[50] Another aspect that is worthy of scrutiny is the more invasive nature of the remedies that are sought, in that electronic devices will essentially be seized and kept until further court order rather than simply copied. For many of the reasons I have already outlined in the facts, I am satisfied that this is appropriate in this

particular case. However, it is important to identify that it does increase the defendant's privacy interests at stake and justifies careful scrutiny about how these terms are carried out and what arguments that the defendant might have been able to raise in opposition. I am satisfied that those concerns have been adequately met and are justified in this particular case.

Strong *Prima Facie* Case

[51] In this instance, the draft notice of civil claim alleges breach of confidential information as well as breach of a contractual duty (in the defendant's employment contract) to maintain confidence of the work product.

[52] The test for breach of confidence is set out in Justice Iyer's decision in *Skycope Technologies Inc. v. Jia*, 2023 BCSC 1288 [*Jia*] at paras. 116–128. I will not repeat that here.

[53] It is helpful to note that Justice Iyer talked about the difference between know-how, which is generally not protected by confidence, and information that may be protected by the common law remedy of breach of confidence. I note in particular paragraph 134 where she stated that the plaintiff had not given examples of particular calculations, simulations or experimentations for specific drones carried out to develop technology and what particular employees might have learned through their employment.

[54] The passage is helpful because, in contrast, the CEO's affidavit in this case detailed how the information in the impugned evidence that the defendant has likely disclosed is confidential. Specifically, the affidavit explained how the defendant's description of how he cracked a very specific drone's protocol came from the methodology that was used at the plaintiff company. It is actually tied to particular reports and monitoring (through progress reports) that was done. It is quite detailed and very specific.

[55] I also note that the defendant has an employment contract with the plaintiff. Clause 17(b) of that contract sets out the obligations of confidentiality. It requires him

to maintain strict confidentiality of “confidential information”—a broadly defined term—and not to use or disclose it except during the employment and only as required to carry out the employment, not to use or disclose it for personal benefit or anyone else's benefit, and to take all precautions to prevent unauthorized access or use or disclosure or reproduction of confidential information.

[56] Clause 16 of that contract defines “confidential information”, and its scope is very broad. It includes, among others: things; research and development information; material; technologies and works which include discoveries, developments, ideas and concepts; studies and analyses and reports. The identical provision was discussed in *Jia* at paras. 191–192.

[57] At common law, in order for information to be confidential to ground a claim for breach of confidence, it must be inaccessible, have a quality of originality or uniqueness and not simply be in the nature of know-how. However, the threshold to meet this test is low, and it requires a contextual analysis: *Jia* at paras. 118-119.

[58] Given the facts that I have reviewed above, I am satisfied that there is a strong *prima facie* case based on the wording of the contract and the obligations in it. The disclosure of the presentation, on its own, presents a strong *prima facie* case. In addition, I note the affidavit evidence that the defendant potentially uploaded the source code to Dropbox through his Obsidian notes.

[59] I add to that that BeamTrail is potentially a threat to Canadian interests, and that it has previously expressed interest in getting the software. There is the potential that, having been unsuccessful at doing so directly, employing the defendant is their way of getting around that. In other words, there is at least some indication that one might be able to draw an inference that that is how they have gone about getting confidential information.

Serious Damage, Actual or Potential, to the Plaintiff

[60] The plaintiff was fair to identify two routes in the case law. One is the judicial approach looking at the nature of the claim itself in assessing the degree of damage:

FLS Transportation at para. 16. There is also an Alberta case that talks about damage to the plaintiff in that not granting the order would make it impossible for them to prove the case: *Peters* at para. 22. The plaintiff asserts that both routes apply in this case, and I agree.

[61] The disclosure of confidential information, on its own, could potentially and seriously damage the plaintiff's business interests. I refer specifically—although it was in the different context of interim injunctions—to Justice Macintosh's statement as quoted by Justice Stephens in *Concrete Cashmere Ltd. v. Lo*, 2023 BCSC 1502 at paras. 11–12. It is notoriously difficult for a plaintiff to prove, in a way measurable by damages, how the release of confidential information does harm. I am, however, satisfied that in this particular case the affidavit is compelling in describing that.

[62] Additional factor in this particular case is the potential for damages to the reputation of the plaintiff company. It is known to be working in the field of interest to the military. It is known to operate in a field where the government has sanctions on commercial enterprises related to states not friendly to Canada. The plaintiff included a CBC report that a Russian entity potentially obtained confidential technology of the plaintiff. The article illustrates that the Canadian government takes that extremely seriously. It is then not difficult to understand that if this sort of thing happens again—where it is known that confidential information from the plaintiff has gone into the hands of a company associated with an unfriendly state—that the plaintiff company may come to be seen as unreliable which would severely affect its reputation and its business interest.

[63] I also note the potential harm to the defendant himself or other employees, in that they may be subject to attempts at manipulation by states or unsavory actors wanting access to the technology and confidential information.

[64] I am satisfied that this step has been met.

Convincing Evidence that the Defendant Possesses Incriminating Documents or Things

[65] In my review of why this case meets a strong *prima facie* case and of the facts, I am satisfied this step has been easily met.

[66] I will clarify that it is not necessary here to make a finding, an inference or assume that there was malicious intent on behalf of the defendant. As counsel explained, it might be that he simply wanted to impress his potential new employer, or he might have wanted to get a leg-up when he started his job, and to do either, he wanted to illustrate his skills. Even if one could find that there was no malicious intent, that is essentially irrelevant to whether there has been a breach of confidentiality and a breach of the employment contract. It is also immaterial to the potential risk to national security and his potential exposure to attempts at manipulation which would arise regardless of his intention or his knowledge of his breach.

[67] I am satisfied that step has been met.

Real Possibility of Destruction

[68] I am satisfied this step has been met, but acknowledge the difficulty in this case given that one cannot discern from these facts whether the defendant had malicious intent or knowledge that disclosure of the information was in breach of his contract. It is not a leap, however, to infer he had some concern that he was in breach given his ambiguous response to question about the company for which he was going to work. In any event, it is highly likely that if the defendant has advance notice of the lawsuit and the plaintiff seeking reimbursement for its legal costs and the other sanctions sought, he would be tempted to try and destroy the evidence to show that he had not done anything wrong.

[69] Even if the defendant was merely careless in what he did, or that he did not know he was breaching confidentiality—which is hard to imagine but not impossible—given the severity of the potential sanctions being sought against him, he would be highly motivated to remove incriminating evidence, not only to protect

his position, but potentially to save himself from the embarrassment or shame of what he had done.

[70] I should also add that there is some basis in this particular case upon which a reasonable inference could be drawn that he actually had knowledge. I am not making that finding. It is only to indicate that it supports a conclusion that there is a real possibility he might destroy the information.

[71] For all of those reasons, I grant the *Anton Piller* order.

INTERIM INJUNCTION

[72] As noted, the plaintiff also sought an interim injunction requiring both the cessation of any further use or disclosure of confidential information. The three-step test for interim injunction is well-known from *RJR-MacDonald Inc. v. Canada (Attorney General)*, [1994] 1 S.C.R. 311, 1994 CanLII 117. I agree that the first step of whether a serious question to be tried is met by my previous discussion about the *Anton Piller* order, and I will not repeat that.

[73] I am also satisfied that the second step of whether irreparable harm will occur is met. One can presume irreparable harm from the breach of confidentiality agreements: *EnWave Corporation v. Dehydration Research, LLC*, 2022 BCSC 637 at paras. 105–106 [*EnWave*]. I agree that applies here. I also note my previous comments about the potential harm to the reputation of the company, given that it is operating in the military sphere and in the atmosphere of sanctions.

[74] It is notable that courts typically find that this step is more easily met when someone has breached a negative covenant, which is the case here: *Global Internet Management v. McLeod et al*, 2003 BCSC 652 at para. 82. I also note that there is a stipulation in the contract that breach of confidence amounts to irreparable harm entitling the plaintiff to an injunction, which is compelling but not determinative: *Enwave* at paras. 104–105.

[75] Turning then to the third step of whether balance of convenience favours the granting of the relief, I am satisfied that it is also met. The CEO has provided an undertaking as to damages, and given the nature of the company, I am satisfied that is sufficient. It is clear that the defendant took steps to alter the *status quo*. I find that there is a very strong case here on a *prima facie* basis about the breach of confidence, and that also favours granting the order.

[76] It is significant in this particular case that the potential harm from the disclosure of information is not limited only to the plaintiff. I also have evidence of the potential harm to Canada's national security interests if BeamTrail passes the information along to states that are contrary to Canadian interests, as well as the potential that the defendant himself may be subject to attempts by foreign agencies to manipulate him or to compel him to provide further information.

[77] The plaintiff said that the defendant is not impeded from going to his new employment, simply that he cannot breach his contractual obligations. It may be that he is no longer of interest to the company if these events come to light. If that is the case, with respect, that would only be because of his breach of confidential information in the first place.

[78] Therefore, it is clear to me that the balance of convenience favours granting the injunction.

SEALING ORDER

[79] Lastly, the parties ask for a sealing order. I am mindful of the test from *Sherman Estate v. Donovan*, 2021 SCC 25 at para. 38. This Court is vigilant to protect the openness of the court process, and not interfere with it lightly. However, I find, in the interests of justice, particularly given the national security implications contained in the evidence, it is appropriate to enter into this hearing and these reasons *in camera*.

[80] That reasoning and that rationale underly why I also find it is appropriate to grant a sealing order. The public interest in this case is not only the protection of

confidential information that I find is essential to the plaintiff's business, but we have the unique aspect of potential risk of harm to Canadian national interests. That is sufficient, in my respectful view, to grant a sealing order.

[81] I am thankful to counsel who elucidated some of the concerns that I raised about ensuring there will be some method to come back and discuss the necessity for that sealing order in breadth and duration, even if the plaintiff does not immediately have a comeback order. I am not making that order. I trust counsel will take my remarks to heart, and I appreciate their cooperation in that regard.

TERMS OF THE *ANTON PILLER* ORDER

[82] The only other thing to address is the orders, which I now sign. I note on the record with regard to the *Anton Piller* order, that I approve of certain things that are not standard. Typically, in cases with electronic devices, there is an order that they are taken and mirror images produced and returned. In this particular case, however, I have granted an order that authorizes them to be kept for a time, subject to the supervising solicitor in this unique situation. Another cellphone or other devices will be given to the defendant, and incoming private communications will be forwarded.

[83] This is quite unusual. However, I am satisfied that it is necessary in this particular case based on everything that I have said.

[84] I also note that the plaintiff will be going to the defendant’s home to carry out the terms of the order. I am aware that the defendant has a family. I am satisfied that the plaintiff has been careful to think about the impact of implementing this order on his family, in that they will try to execute it at a time when the children will not be there. I expressed a concern about the potential for how other devices will be looked at. The children are very young—it is doubtful that they have highly sensitive personal information on individual electronic devices. It is, however, within the realm of the supervising solicitor with the plaintiff there to look at devices and to come to a determination whether it may contain confidential information, and if it may, to allow further examination of it.

[85] In other words, I am satisfied that the plaintiff has given thought to these issues. I trust that the supervising solicitor will act as an officer of the Court and be vigilant to the concerns that may arise from the unusual aspects of this case.

[86] I also expressed a concern about the necessity of producing a transcript, not only of the proceedings but of my reasons and doing so quickly. That, of course, is in order to give the defendant notice of what has happened in his absence. It is unclear to me, given the sealing order, what would need to be done logistically for that to happen. Given the urgency of the situation, I exercise my discretion in my inherent jurisdiction to order the transcript of the proceedings, as well as my reasons, to be produced on an expedited basis without the necessity of any further court order.

"Sharma J."