Federal Court  Cour fédérale

Date: 20200619

Docket: DES-5-08

Citation: 2020 FC 715

Ottawa, Ontario, June 19, 2020

PRESENT: The Honourable Madam Justice Roussel

BETWEEN:

IN THE MATTER OF a certificate signed pursuant to subsection 77(1) of the *Immigration and Refugee Protection Act* [IRPA];

AND IN THE MATTER OF the referral of that certificate to the Federal Court of Canada pursuant to subsection 77(1) of the IRPA;

AND IN THE MATTER OF Mohamed HARKAT

REASONS FOR ORDER

ROUSSEL J.

I. Overview

[1] The Minister of Citizenship and Immigration and the Minister of Public Safety and Emergency Preparedness [Ministers] are asking the Court to vary the terms and conditions of Mohamed Harkat's release. They assert that Mr. Harkat has committed two (2) breaches by changing his email password without informing the Canada Border Services Agency [CBSA] and by deleting a number of his emails without their consent. In addition, they seek to clarify the

terms and conditions relating to Mr. Harkat's use of a mobile telephone and computer for employment purposes.

[2] Mr. Harkat opposes the Ministers' motion. He maintains that he has not breached the conditions imposed by the Court, at least not knowingly, and he seeks a further relaxation of his terms and conditions of release.

[3] For the purposes of the Ministers' motion, it is not necessary to provide a full account of the facts, procedural history and variations brought to Mr. Harkat's terms and conditions of release. It is sufficient to mention that Mr. Harkat is the subject of a security certificate under section 77 of the IRPA. The certificate was determined to be reasonable by this Court in 2010 (*Harkat (Re)*, 2010 FC 1241). The Supreme Court of Canada upheld that finding in 2014 (*Canada (Citizenship and Immigration) v Harkat*, 2014 SCC 37). Since Mr. Harkat's release from detention in 2006, this Court has reviewed and varied the terms and conditions of his release. The most recent review took place in November 2017 (*Harkat (Re)*, 2018 FC 62 [*Harkat 2018*]). For previous reviews, the reader should refer to *Harkat v Canada (Citizenship and Immigration)*, 2014 FC 1034 [*Harkat 2014*]; *Harkat v Canada (Citizenship and Immigration)*, 2013 FC 795 [*Harkat 2013*]; *Harkat (Re)*, 2009 FC 1008; *Harkat (Re)*, 2009 FC 241; *Harkat v Canada (Citizenship and Immigration)*, 2007 FC 416; and *Harkat v Canada (Minister of Citizenship and Immigration)*, 2006 FC 1105.

II. Analysis

A. *Breach of Conditions*

(1) Deletion of Emails Without Consent

[4] The Ministers allege that on June 12, 2018, an examination of Mr. Harkat's computer revealed that he had deleted a large number of emails without authorization from the CBSA. They submit that Mr. Harkat breached condition 7a) of the terms and conditions of release set out in Appendix "A" of my Order dated April 6, 2018 [Order]. This condition stipulates that "Mr. Harkat, or anyone on his behalf, shall not alter or delete from his computer any tracking information without the permission of the CBSA, including, but not limited to email, … sent, received or draft electronic mail".

[5] While Mr. Harkat admits to the deletion of emails, he maintains that he had the authority to delete them. In his testimony before the Court, he explained that it was his understanding, based on an email he received in December 2013, that he could delete his emails after the CBSA inspected his computer. In addition to this standing permission, he would also receive verbal authorization when he picked up his computer at the offices of the CBSA. When the CBSA did not inspect his computer for a while, an official from the CBSA would send him an email approximately every three (3) months authorizing him to delete emails up to a certain date.

[6] After reviewing the evidence of both parties, I am unable to conclude, on a balance of probabilities, that Mr. Harkat breached condition 7a) of his terms and conditions of release.

[7] The CBSA officer in charge of monitoring Mr. Harkat's conditions, Michel Connelly, indicates in his affidavit that "a review of Mr. Harkat's computer on June 12, 2018 revealed that he had deleted a number of emails" [my emphasis]. He then goes on to refer to an email sent to Mr. Harkat on June 21, 2018 advising him that the CBSA had conducted a "routine review of [his] email account" [my emphasis] and noticed that he had "deleted a large batch of emails (in the 'Recover Deleted Items' folder)".

[8] The difficulty with this evidence is that it does not indicate when the CBSA actually accessed Mr. Harkat's email account. This information is particularly relevant since Mr. Harkat's emails are not stored on his computer, as he does not use a dedicated email software product [email client] such as Microsoft Outlook. Instead, Mr. Harkat accesses his email account through his computer's web browser. To monitor this account, the CBSA uses Mr. Harkat's username and password to log in remotely.

[9] It appears from the evidence that Mr. Harkat brought his computer to the CBSA for inspection on May 7, 2018, and he picked it up the next day. When he got home, he "cleaned" his computer and deleted certain emails. If the CBSA only accessed Mr. Harkat's email account when it reviewed the image of the computer in June, as opposed to when he brought the computer to the CBSA for inspection in early May, it is possible that Mr. Harkat had already deleted the emails by the time the CBSA accessed his email account.

[10] I find there are too many gaps in the Ministers' evidence that leave too many questions unanswered. To begin with, there is insufficient evidence establishing with any certainty how

and when the CBSA provided authorization to Mr. Harkat in the past. In addition, there is no objective documentary evidence demonstrating the breach. The witnesses who appeared before me had no personal knowledge of the facts, and they could not provide any additional information on the breach. There is also no evidence of the scope and magnitude of the breach. Even if I had found that there was a breach, I would be unable to determine the appropriate consequence, given that I cannot assess the seriousness of the breach.

[11] I also note the testimony of Mr. Connelly, during which he indicated that he could not recall any unauthorized deletions of emails before this alleged incident. This is an important consideration given that Mr. Harkat has had an email account for several years.

[12] Finally, I cannot ignore the answer provided by Mr. Connelly when asked on cross-examination how he found out that Mr. Harkat had deleted some emails. He responded as follows:

> […] avec l'assistance de notre bureau chef de notre section, on est arrivé à la conclusion qu'il y avait une possibilité qu'il avait effacé ses courriels.
>
> Alors j'ai envoyé l'information à Mme et M. Harkat concernant la possible infraction.
>
> [TRANSLATION]
>
> … with the assistance of our section's head office, we concluded there was a possibility he had deleted his emails.
>
> So, I sent Ms. and Mr. Harkat the information concerning the possible infraction.
>
> (Transcript of Proceedings, Vol 1 at 44:7-17)
>
> [Emphasis added.]

[13] Even if Mr. Harkat has admitted to deleting some of his emails, I am not persuaded that a breach actually occurred given the words used by Mr. Connelly, which only refer to the "possibility" of a breach occurring, and given the lack of detailed evidence on the issue.

(2) Password Change

[14] The Ministers allege that Mr. Harkat breached the terms and conditions of his release by failing to advise the CBSA of a change in the password to his email account.

[15] In his affidavit, Mr. Connelly states that, on October 29, 2018, the CBSA attempted to log in to Mr. Harkat's email account but was unable to do so. On November 8, 2018, counsel for the Ministers wrote to Mr. Harkat's counsel requesting the password. On November 20, 2018, Mr. Harkat's counsel responded that there had been no changes to Mr. Harkat's password. On December 4, 2018, the CBSA wrote directly to Mr. Harkat, as the CBSA was still unable to access his email account. On that date, Mr. Harkat provided Mr. Connelly with the new password. The next day, Mr. Harkat confirmed the new password. On December 7, 2018, in a folder labelled "Garbage" in Mr. Harkat's email account, the CBSA discovered an email from Microsoft stating that Mr. Harkat's password had been changed on September 28, 2018 at 9:24 p.m.

[16] The Ministers argue that Mr. Harkat's failure to advise the CBSA of the password change prevented them from reviewing Mr. Harkat's emails for a period of approximately sixty (60) days. As a result, they are asking the Court to require Mr. Harkat to access his email only through an email client such as Microsoft Outlook or Mozilla Thunderbird, rather than his

current method using a web browser. An email client will provide the CBSA a better level of protection in its monitoring of Mr. Harkat's emails.

[17] In response, Mr. Harkat acknowledges there was a password change. However, he maintains that it was not a breach of his conditions because he did not change it intentionally. His evidence is that after the tornado in the National Capital Region in September 2018, he had problems with his computer. On September 26, 2018, he advised the CBSA he would bring them his computer for an inspection, and then he would have it repaired at a local business. He brought his computer to the CBSA on September 27, 2018 and picked it up the next day. Before taking his computer for repair, he logged out of his email account so that the technicians at the store would not be able to see his emails. Since the repair shops were too busy, he returned home and tried to log into his email account. He tried to enter his password three (3) times, only to be locked out of his account. He testified that he remembers receiving a message asking him whether he had forgotten his password. The telephone then rang and he received a security code to enter and reset his password. As he did not want to change his password, he entered the same one.

[18] Mr. Harkat claims that he did not realize he had changed one of the letters in the password from uppercase to lowercase. He explained that the change in case did not raise an issue for him because he kept his email account logged on, and, therefore, he did not need to remember his password. He only realized the password had changed when he received an email from the CBSA in early December 2018, in which Mr. Connelly told him that Microsoft had sent an email, which was in the "Garbage" folder, indicating that the password had been changed.

The same day, Mr. Harkat sent an email to Microsoft complaining that he had not changed his password.

[19] Mr. Harkat claims that he did not read the email from Microsoft confirming the password change. The email in question was still marked as unread when he checked his "Garbage" folder. Mr. Harkat explained that he had created the "Garbage" folder to store emails he wanted to delete while waiting for the CBSA's permission to delete them.

[20] The three (3) digital forensic investigators who appeared before me, which included Mr. Harkat's own expert, unequivocally stated that password changes do not happen by accident. A user can only change an online account password by logging into the account and changing the security settings, or by using the "I forgot my password" recovery function accessible from the login screen. Mr. Harkat's digital forensic expert, Stephen Ellwood, also testified that there may be some confusion in changing a password. A non-technical person may not understand the importance of uppercase and lowercase characters when setting a password, which may cause the person to think that the password is the same.

[21] I can understand that Mr. Harkat may not have realized initially that he had changed his email password if he was not required to log onto his email account because it remains continuously logged in on his computer. However, when he and his wife became aware that the password he had given the CBSA did not work, he should have tried to determine the cause of the problem. He could have logged off and attempted to re-enter his account, at which time he would have realized that his old password was not working. He could have double-checked

which password the CBSA were using or brought his computer in for inspection. If he had consulted his "Garbage" folder, he would have seen the unopened email from Microsoft on September 28, 2018 indicating the password change. Even if the password change was inadvertent, Mr. Harkat could have been more proactive in attempting to resolve the issue.

[22] I also note that the information relating to Mr. Harkat locking himself out of his email account and receiving a call from Microsoft was never communicated to the CBSA, and it does not appear anywhere in his affidavit or in his wife's affidavit. This information only came to light during his oral testimony.

[23] While Mr. Harkat may not have intended to change his password, the fact remains that he did so without informing the CBSA. Therefore, I must conclude that he has breached condition 7c) of his terms and conditions of release. This condition required him to provide the CBSA with any password necessary to access any part of his computer. This includes the password to his email account. I will address the consequences of this breach later in these reasons.

(3) InPrivate Browsing

[24] Before leaving the issue of the breach of conditions, it is important to note an additional alleged breach that the Ministers have since abandoned. When this matter initially came before the Court, the Ministers were only alleging the two (2) breaches above. Then, after the Ministers filed their motion record, Mr. Harkat's counsel was provided a copy of an affidavit sworn by Carl Létourneau in late March 2019. Mr. Létourneau is a digital forensic investigator employed with the CBSA. In his affidavit, he stated that, as a result of his forensic investigation and

analysis of the internet artifacts on Mr. Harkat's hard drive, he believed that Mr. Harkat had used the "InPrivate Browsing" feature of Internet Explorer, in violation of his terms and conditions of release. After receiving a copy of the affidavit, Mr. Harkat's counsel indicated she would consent to the filing of this late affidavit, provided she could cross-examine the affiant and obtain her own expert report, to which the Ministers agreed. On April 24, 2019, the CBSA provided a digital forensic image of Mr. Harkat's hard drive to his counsel to allow his expert to examine it.

[25] The Ministers amended their motion record on July 4, 2019. They included two (2) affidavits sworn by Mr. Létourneau on the issue of the alleged "InPrivate Browsing" breach, one dated March 25, 2019 and a second dated June 28, 2019. In these affidavits, Mr. Létourneau explained the "InPrivate Browsing" feature, its purpose, the footprint it leaves behind and how one can retrace its use using digital forensic tools.

[26] On August 23, 2019, Mr. Harkat filed his responding motion record, which included a report from Mr. Ellwood, his own digital forensic expert. Mr. Ellwood concluded there was no evidence that the laptop had been used to perform "InPrivate Browsing" using Internet Explorer. Rather, it was his view that a misunderstanding of Internet Explorer's "Automatic Crash Recovery" feature had led the CBSA investigators to an inaccurate conclusion.

[27] After reviewing the Ministers' motion materials as well as Mr. Harkat's responding motion record, I issued a direction to the parties that the Ministers' motion would proceed orally and that the Court would hear from the forensic investigators. Five (5) days before the scheduled hearing, the Ministers filed a reply record. It included a will-say statement from Mr. Létourneau

and a copy of the digital forensic report he had originally prepared and relied upon to conclude there was a breach. This new information caused Mr. Ellwood to prepare several videos simulating Mr. Harkat's computer to dispute the findings reached by Mr. Létourneau. After reviewing the videos and the findings advanced by Mr. Ellwood, the Ministers informed the Court on October 7, 2019 that, while their digital forensic investigator had found traces of browsing artifacts consistent with "InPrivate Browsing", he could no longer confirm with certainty whether this feature had been used by Mr. Harkat or the computer's previous owner. As a result, the Ministers advised that they were abandoning this alleged breach and their request for partial forfeiture of the cash bond deposited into Court.

[28] While I do not intend to comment any further on this alleged breach, I must say that it is unfortunate that the Ministers' reassessment of their position did not come earlier in the proceedings. In total, two and a half (2.5) days of hearings were devoted to the examination and cross-examination of three (3) digital forensic investigators. If Mr. Létourneau's report had been attached to his affidavit sworn on March 25, 2019 instead of being introduced through his will say on September 13, 2019, it is likely that this issue would have been resolved before the hearing began on September 18, 2019, which would have resulted in a shorter hearing.

B. *Review of the Terms and Conditions of Release*

[29] In my last review of Mr. Harkat's terms and conditions of release, I indicated that I accepted the legal framework set out by my predecessor in *Harkat 2014* at paragraph 7 and in *Harkat 2013* at paragraphs 25 to 27 (see also *Charkaoui v Canada (Citizenship and Immigration)*, 2007 SCC 9 at paras 108-109, 119). I also set out a non-exhaustive list of factors

to be considered in determining whether Mr. Harkat's release poses a danger to the security of Canada and, if so, whether that danger can be neutralized through the impositions of terms and conditions (*Harkat 2018* at para 39). Ultimately, I concluded that the conditions were disproportionate with the danger posed by Mr. Harkat and that they should be attenuated.

[30] Neither counsel for the Ministers nor Mr. Harkat argued extensively on the factors that I should consider in the context of this motion. For the most part, I find that they remain unchanged (*Harkat 2018* at paras 42-66), with certain exceptions.

[31] To begin with, on October 2, 2018, a senior delegate of Immigration, Refugees and Citizenship Canada [Minister's Delegate] determined, pursuant to paragraph 115(2)(*b*) of the IRPA, that Mr. Harkat should not be allowed to remain in Canada based on the nature and severity of the acts he committed. Mr. Harkat is seeking judicial review of that decision in Court File IMM-5330-18. That proceeding is ongoing and its finality remains uncertain at this time.

[32] Additionally, unlike in the last review, Mr. Harkat has not complied with all of the terms and conditions of his release. The Ministers have demonstrated that Mr. Harkat has breached one of his conditions. The existence of the breach raises issues of trustworthiness and credibility, both of which are essential considerations in reviewing the appropriateness of the terms and conditions of release (*Harkat 2013*).

[33] As in the past, the passage of time favours the relaxation of the conditions. The Ministers have not presented any evidence that Mr. Harkat has been involved in any threat-related activity

since my last review. The fact that the opinion of the Minister's Delegate is based on the nature and severity of the acts committed by Mr. Harkat in the past, as opposed to the danger he poses to Canada today, supports the conclusion that the danger posed by Mr. Harkat continues to be situated at the lower end of the spectrum.

[34] In this context, I will now examine the changes and clarifications proposed by the parties.

(1) Mobile Telephone for Employment Purposes

[35] In my last review of Mr. Harkat's terms and conditions of release, I allowed him to use a mobile telephone for employment purposes, subject to the following conditions:

> i. the employer-provided mobile telephone could not have internet connectivity;
>
> ii. Mr. Harkat was required to provide a written undertaking that the mobile telephone would be used for employment purposes only, and any unauthorized use would result in a breach of conditions;
>
> iii. Mr. Harkat was required to advise his employer of this condition and ask his employer to report any unauthorized use to the CBSA;
>
> iv. Mr. Harkat was to provide his employer with the name and number of the contact person at the CBSA and provide the CBSA with the name and number of his work supervisor.
>
> (*Harkat 2018* at para 87)

[36] Mr. Harkat provided his signed undertaking regarding the use of the mobile telephone for employment purposes on April 13, 2018.

[37] According to the evidence, Mr. Connelly contacted Mr. Harkat's work supervisor by telephone on April 26, 2018 to verify that the conditions were being respected. Mr. Harkat's supervisor indicated that she preferred that he communicate with her in writing. Mr. Connelly sent the supervisor an email the next day asking for confirmation that Mr. Harkat had advised her of his conditions regarding the use of a mobile telephone at work, the make and model of the telephone provided to Mr. Harkat, and confirmation that the mobile telephone did not have internet connectivity. Mr. Harkat's supervisor did not respond to the email. Mr. Connelly resent the same email on May 15, 2018. Mr. Harkat's supervisor responded the same day that she was not bound by the Order.

[38] The Ministers contend that since the Order required Mr. Harkat to provide the CBSA the name and number of his work supervisor, it implicitly permitted CBSA employees to verify compliance with the terms of the undertaking. They consider that the supervisor's comments amount to a breach of the Order.

[39] The Ministers are asking that condition 4r) of the terms and conditions, which governs Mr. Harkat's use of a mobile telephone for employment purposes, be amended to include the following:

> (i) Additionally, Mr. Harkat will need to advise the CBSA as to whether or not he will be taking the mobile phone home to his residence, or whether the mobile phone will remain at his workplace; the make and model of the mobile telephone he is required to use for employment purposes (and update the CBSA with this information if he uses a different mobile phone).
>
> (ii) Mr. Harkat will also be required to advise his employer of this condition and ask his employer to report any unauthorized use to the CBSA. Mr. Harkat's employer will

> be required to sign an acknowledgment that Mr. Harkat has advised them of the conditions and that it will report any unauthorized use to the CBSA.

[40] Mr. Harkat disagrees with the Ministers' interpretation of the Order, and he asserts that he has abided by all of its terms and conditions. In his view, there is nothing in the Order requiring him to provide the make and model of the employer's telephone or obliging his employer to answer the CBSA's questions. There is also no evidence that he has ever breached this condition.

[41] I am concerned by Mr. Harkat's failure to abide by the spirit of the Order. In my view, much of the disagreement between the parties could have been avoided if Mr. Harkat had simply informed the CBSA of the make and model of the mobile telephone. Also, in emails dated August 19 and 22, 2019, Mr. Harkat's supervisor eventually confirmed to Ms. Harkat that the mobile telephone did not have internet connectivity, that she was aware of the conditions, and that she would report any breach. These emails were filed as exhibits to the affidavit of Ms. Harkat, which was included in Mr. Harkat's motion record. It is unfortunate that Mr. Harkat did not obtain this information earlier and communicate it to the CBSA.

[42] Despite my concerns, I am not prepared to order that Mr. Harkat's current employer or any future employer sign an acknowledgment that Mr. Harkat has advised them of the conditions regarding the mobile telephone. To do so would undoubtedly make it difficult for Mr. Harkat to obtain employment.

[43] While Mr. Harkat may wish to have a mobile telephone with internet connectivity for employment purposes, I am not prepared to agree to this change. Mr. Létourneau testified that when one has a telephone with internet connectivity, it would be possible to install applications while at work, log into various accounts, and communicate with others. Then, at the end of the business day, the employee could delete the applications and communications. The employer would not know that the employee had initiated a communication and, unless the CBSA can inspect the telephone, it will not be able to know either. This concern exists with internet access over cellular data networks or over Wi-Fi networks.

[44] To the extent that the make and model number of the mobile telephone will inform the CBSA of the mobile telephone's capabilities, including internet connectivity and storage technology, I am prepared to hold that Mr. Harkat must advise the CBSA of the make and model number of the mobile telephone. However, I have not been persuaded that it is necessary for Mr. Harkat to inform the CBSA whether he will be taking the employer-provided mobile telephone home.

[45] Consequently, condition 4r) will be amended to include the following underlined passage:

> 4. …
>
> r) … To the extent Mr. Harkat is required to have a mobile telephone for employment purposes, Mr. Harkat will be required to provide a written undertaking that the mobile telephone will be used for employment purposes only, with the exception of calls to and from his wife, and any unauthorized use will result in a breach of conditions. <u>Additionally, Mr. Harkat will need to advise the CBSA of the make and model of the mobile telephone he is required to</u>

> use for employment purposes (and update the CBSA with this information if he uses a different mobile telephone). Mr. Harkat will also be required to advise his employer of this condition and ask his employer to report any unauthorized use to the CBSA. Mr. Harkat will provide the employer with the name and number of the contact person at the CBSA and provide the CBSA with the name and number of his work supervisor.
>
> …

(2) Use of a Computer for Employment Purposes With Internet Access

[46] In November 2017, Mr. Harkat sought permission to use a computer with internet connectivity for employment purposes. I agreed with Mr. Harkat that the restrictions regarding the use of technology for employment purposes, such as the internet, made it difficult for him to find full-time employment. I noted that Mr. Harkat had complied with his conditions of release since his release in 2006 and that, in order to fully embrace the values of his adopted country, it was important that he be given the opportunity to obtain gainful employment.

[47] While the Ministers were amenable to relaxing this condition, they opposed the request for "blanket approval" due to the possibility of unmonitored and anonymous communications. They suggested that each request be dealt with on an individual basis, and they agreed that the CBSA's approval should not be unreasonably withheld.

[48] I therefore indicated in my reasons that I was inclined to allow Mr. Harkat the right to use a computer, including the internet, for employment purposes, subject to certain limitations. Upon review by the parties, the condition was worded as follows:

7. …

…

i) With the CBSA's consent, Mr. Harkat may use a desktop computer or laptop computer with internet connectivity if required by his employer for work purposes only. The parties shall identify in advance the types of technologies Mr. Harkat can use. Upon Mr. Harkat contemplating employment, he shall inform the CBSA of the name of his prospective employer, the duties he will be required to perform, the technology he will be required to use and have access to in the course of his employment, including the internet, the use he will make of it, and the number of hours a week he will be required to use it. Upon notification by Mr. Harkat, the CBSA shall consider Mr. Harkat's prospective employment without delay and respond to him in a diligent and expeditious manner. If the parties are unable to reach a consensus, they may come to the Court for a determination. In all cases, Mr. Harkat will be required to sign an undertaking that any use of the technology or the internet will be for employment purposes only and any unauthorized use shall constitute a breach of his conditions. Mr. Harkat will also be required to advise his employer of this condition and ask his employer to report any unauthorized use to the CBSA. Mr. Harkat will provide the employer with the name and number of the contact person at the CBSA and provide the CBSA with the name and number of his work supervisor.

…

[49] The Ministers now seek to have this term removed from the terms and conditions for several reasons. They argue that Mr. Harkat has committed two (2) serious breaches of the terms and conditions imposed by this Court, both related to his personal use of the internet. Also, Mr. Harkat's employer has, to date, demonstrated that it does not intend to cooperate with the CBSA. The Ministers submit that a term that requires the cooperation of a third party, when the

third party has demonstrated that it will not cooperate with the CBSA, is not a term or condition that can be enforced.

[50] The Ministers have failed to persuade me that Mr. Harkat should not be allowed to use a computer with internet connectivity for employment purposes.

[51] As I indicated in my last review, I can think of very few types of employment that require no form of technology or the use of the internet. I also believe that frustration can result from one's inability to secure gainful employment. It can affect a person's mental health, which in turn can lead to other issues and problems. Indeed, the Supreme Court of Canada has affirmed the significance of internet access as an "increasingly indispensable component of everyday life" (*R v KRJ*, 2016 SCC 31 at para 54).

[52] I have very little evidence on the specific conditions of Mr. Harkat's employment and his access to a computer with internet connectivity. During the hearing, Mr. Harkat's counsel submitted that when Mr. Harkat works the night shift at his current job, no one is there to supervise him, so, in theory, he could use the nearby computer if he wanted to access the internet. She suggested that the Court either trusts him or it does not.

[53] If Mr. Harkat is required to use a computer with internet connectivity in his current employment, I believe that one option to resolve this issue would be to allow Mr. Harkat to bring his personal laptop computer to work, providing it does not contain a solid-state drive [SSD]. The evidence provided by the Ministers' digital forensic investigators is that the presence of an

SSD in Mr. Harkat's computer would interfere with the evidentiary value of the data imaged for inspection. An SSD performs a number of system functions that will delete certain data used for forensic analysis. Because SSDs tend to have lower capacities than traditional hard drives, an SSD also increases the likelihood that data will be overwritten. Once the data is overwritten, it may not be recoverable later.

[54] There is conflicting evidence on the record as to whether Mr. Harkat's computer already contains an SSD. Jeremy Fernando, the other digital forensic investigator who testified on behalf of the Ministers, states in his affidavit that he was advised and believes that Mr. Harkat obtained an SSD in August 2017. His evidence is consistent with the evidence of Mr. Connelly's predecessor, who swore an affidavit and testified during Mr. Harkat's last review. However, Mr. Létourneau testified as follows:

> Q. With respect to the kind of computer that Mr. Harkat has, do you know if it's an SSD or a platter?
>
> A. It's a spinning drive.
>
> Q. So it's a platter computer?
>
> A. Yes.
>
> (Transcript of Proceedings, Vol 2 at 248-249)

[55] Mr. Létourneau is responsible for imaging Mr. Harkat's computer and analyzing the images. During cross-examination on his affidavit, he explained that one of the first things he does when he receives Mr. Harkat's computer is to look at the type of hard drive in the computer. As he is the best-placed person to know what type of storage device is in Mr. Harkat's computer,

I will assume that he is correct and that Mr. Harkat does not currently have an SSD in his personal computer.

[56] Allowing Mr. Harkat to use his personal laptop computer for employment purposes will permit the CBSA to monitor his use of the computer while at work through its existing inspection procedures. The CBSA cannot do this with respect to the employer's computer.

[57] If Mr. Harkat's computer already contains an SSD, he will not be permitted to bring it to work because, based on the evidence before me, I am concerned that the increased usage would increase the risk of data being overwritten.

[58] In the event that Mr. Harkat is required to use an employer's computer with internet connectivity for work purposes, either in his current employment or in future employment, the condition will remain the same, except that Mr. Harkat must also provide the following information to CBSA:

- the name of the prospective employer;
- the duties he will be required to perform;
- the technology he will be required to use and have access to in the course of his employment, including the make and model of the computer, his access to the internet, the use he will make of it, the number of hours a week he will be required to use it;
- the programs he will be required to use to complete his work;
- whether he will be required to use email;
- whether his computer use will be monitored or supervised;

- the employer's policy with respect to personal use of the computer;

[59] While I understand that this list of required information may appear overwhelming at first glance, it is important because it allows the CBSA to evaluate whether issues might arise. Given the confrontational relationship between the parties, it is necessary to include as much information as possible to avoid a "back and forth" situation. When Mr. Harkat will be contemplating the use of technology with internet connectivity for employment purposes, full information should be provided at the outset to avoid unnecessary delays in the CBSA's evaluation process.

[60] In keeping with the need for early resolution, the CBSA will also be required to consider the information provided by Mr. Harkat and provide a response to him within three (3) business days. While no specific time limit was mentioned in the previous Order, it appears from the evidence that it took the CBSA from May 24 to June 13, 2018 to advise Mr. Harkat that it had refused his request to use a computer with internet connectivity at work.

[61] If the parties are unable to reach an agreement, they may seek a determination by the Court. Before they do so, I encourage them to attempt an alternative form of dispute resolution, either privately or with the assistance of the Court.

[62] Finally, for the same reasons that I provided concerning the use of a mobile telephone for employment purposes, I am not prepared to order that Mr. Harkat's employer, whether current or future, sign an acknowledgement that Mr. Harkat has advised them of the conditions regarding

his use of a computer with internet connectivity. To the extent the parties reach an agreement on Mr. Harkat's use of technology with internet capabilities, it will be sufficient for Mr. Harkat to sign an undertaking that any use of the technology or the internet will be for employment purposes only and any unauthorized use will constitute a breach of his conditions. Mr. Harkat will also be required to advise his employer of this condition and ask his employer to report any unauthorized use to the CBSA. Mr. Harkat will provide the employer with the name and telephone number of the contact person at the CBSA, and he will provide the CBSA with the name and telephone number of his work supervisor.

(3) Variations Relating to Mr. Harkat's Use of His Computer

[63] The Ministers seek a number of adjustments to the conditions relating to Mr. Harkat's computer use. They can be regrouped into the following categories: (a) computer hardware; (b) social media websites and applications; (c) internet browsers; and (d) email accounts.

(a) *Computer Hardware*

[64] The CBSA wants the authority to approve the make and model of Mr. Harkat's personal computer in advance. It is also requesting the addition of a condition stipulating that Mr. Harkat's desktop or laptop computer not contain an "[SSD], flash SSD, hybrid drive or flash storage devices". The CBSA made this request in the last review, but I denied it on the basis that there was insufficient evidence to justify this condition.

[65] As I explained above, the Ministers' digital forensic investigators provided evidence that an SSD in Mr. Harkat's computer would interfere with the evidentiary value of the data imaged

for inspection. Because they tend to have lower capacities than traditional hard drives, SSDs present more opportunities for data to be overwritten and rendered unrecoverable. The capabilities for recovering data are better with a traditional hard drive because deleted data are often left intact on the disk platter.

[66] Since I will be permitting Mr. Harkat to bring his computer to work, it is important that the data related to his use of the computer not be overwritten. Therefore, I am granting the Ministers' request that Mr. Harkat's computer not contain a flash storage device, including an SSD, flash SSD, or hybrid drive. I will not be granting their request that the CBSA must approve the make and model of Mr. Harkat's computer in advance, as they have failed to convince me that this condition is necessary.

(b) *Social Media Websites and Applications*

[67] The second category of changes requested by the Ministers relate to Mr. Harkat's use of social media websites or applications. The CBSA asks that Mr. Harkat's access to social media websites or applications, such as Facebook and Twitter, and to websites or applications that facilitate online video chat, such as Skype, be subject to the following conditions:

(i) he may obtain only one (1) account per respective website or application;

(ii) he must obtain CBSA approval before creating an account on any websites or applications that facilitate online video chat, other than Skype;

(iii) he shall provide the username, password and any updates thereof to the CBSA immediately upon setting up an account;

(iv) he shall consent to the CBSA, or any person designated by it, having access to his accounts without notice;

(v) he shall not alter or delete records of activity or records of communication on any websites or applications;

(vi) he may only access Skype using the desktop application, and he must ensure that his Skype settings are such that all chat and call history are set to be saved forever;

(vii) he must notify the CBSA of the names and Skype addresses of individuals with whom he wishes to communicate, one month in advance of engaging in such communication, though such notice need only be given once with respect to the same individual; and

(viii) Mr. Harkat shall not participate in any communication over these websites or applications over which he can claim solicitor-client or litigation privilege.

[68] The Ministers submit that there are limits to the CBSA's ability to supervise communications over the internet and over social networks. Given the rapid and constantly evolving nature of technology and social networking services, the Ministers submit that restricting Mr. Harkat's use of social media is necessary to allow the CBSA to meaningfully execute its supervisory role.

[69] In response, Mr. Harkat argues that restricting his use of social media is unnecessary and unjustified. He contends that the Court can only impose conditions for a reason, and the Ministers present none to justify these increased measures.

[70] I disagree. When this matter came before me in September 2019, the Ministers were alleging that Mr. Harkat had breached three (3) of his conditions of release. The Ministers have since abandoned their allegations surrounding the "InPrivate Browsing" feature on his computer, and I have found there is insufficient evidence to demonstrate that Mr. Harkat deleted emails without the authority of the CBSA. Nevertheless, the fact remains that Mr. Harkat did breach one of his conditions of release.

[71] Although the danger associated with Mr. Harkat has diminished over time and is situated at the lower end of the spectrum (*Harkat 2018* at paras 50-51), conditions continue to be necessary to neutralize this danger. The CBSA is responsible for ensuring that Mr. Harkat is complying with the terms and conditions of his release. Meanwhile, consumer technology is evolving quickly, and it is becoming increasingly difficult to monitor his technology use. Social media accounts also make it even easier for someone to communicate undetected. According to Mr. Fernando, it is very easy to alter or delete communications over such accounts, or to bypass the CBSA's monitoring capabilities without leaving a trace.

[72] The CBSA already has remote access to Mr. Harkat's email account. It has been monitoring his communications to ensure that he is not communicating with persons who might be engaged in threat-related activities. Like Mr. Harkat's email account, social media accounts are internet-based and have communication capabilities. Refusing to grant the CBSA access to Mr. Harkat's social media accounts when it already has access to his email account would not only be inconsistent, but it would allow Mr. Harkat to redirect his communications to channels that would otherwise be unmonitored.

[73] For these reasons, I am prepared to grant the Ministers' request with respect to paragraphs (i) to (vi) and (viii) above. Regarding paragraph (vii), I find the Ministers' request to be unreasonable. They have not demonstrated why it would be necessary for Mr. Harkat to notify the CBSA of the names and Skype addresses of individuals with whom he wishes to communicate.

(c) *Internet Browsers*

[74] The third category of changes the Ministers seek relates to his use of an internet browser. They ask that Mr. Harkat only be permitted to use the Internet Explorer web browser, and that he not be permitted to install any other web browsers on his computer. They are also asking that all existing or preinstalled browsers be uninstalled from his computer.

[75] Based on the evidence before me, the Ministers have failed to persuade me that the restriction they are seeking is justified.

[76] According to Mr. Létourneau, from a digital forensics standpoint, Internet Explorer is the best browser option to monitor compliance with Mr. Harkat's conditions because it leaves the best forensic footprint. The "InPrivate Browsing" feature of Internet Explorer leaves better artifacts on the hard drive because of the way it caches browsing activity. As a result, the Ministers argue that restricting Mr. Harkat's usage to this browser will make it easier for the CBSA to detect future "InPrivate Browsing" incidents, and the impact of this restriction on the user experience is negligible.

[77] During the hearing, I asked Mr. Létourneau how Internet Explorer compares to Microsoft Edge. His response was that they were "kind of very similar" and that it was "just the way the history – the data is stored". He added that he had not had the chance to test Microsoft Edge. With respect to other browsers, such as Google Chrome and Mozilla Firefox, he testified they were more secure and left less of a footprint because they overwrite data at a certain point, thus making it more difficult for the CBSA to review the history. He testified that imaging Mr. Harkat's computer more frequently, such as every month instead of every three (3) months, as allowed under the current conditions, would reduce the risk of the information being overwritten. However, from a workload perspective, he added that such a schedule would "be a nightmare" because it would require him to work 24 hours a day.

[78] Since Internet Explorer and Microsoft Edge leave a similar footprint, I do not see why Mr. Harkat cannot use Microsoft Edge. As for the other browsers, I understand that there may be circumstances where Mr. Harkat may want to use them for compatibility reasons. For instance, certain websites may not operate correctly in particular browsers. The evidence is these other browsers do leave forensic footprints, even if they are not optimal for forensic examination. To the extent Mr. Harkat wishes to use these other browsers on a regular basis, he will have to accept that the CBSA will likely want to inspect his computer more often. As it stands, the evidence demonstrates that the CBSA is not availing itself of its right to inspect Mr. Harkat's computer every three (3) months. Indeed, in the last few years, they have waited a year between inspections.

[79] In addition to the restriction relating to his use of an internet browser, the Ministers also seek the right to contact Mr. Harkat's internet service provider [ISP] to obtain a report on his internet activity. They also ask the Court to order Mr. Harkat to consent to the CBSA, or any person designated by it, obtaining these records from his ISP.

[80] In my view, this request is unfounded and unsupported by the evidence. When the Ministers have reasonable grounds to request a report on Mr. Harkat's internet activity, they may seek judicial authorization from a designated judge of this Court.

(d) *Email Account*

[81] The last category of changes sought by the Ministers relates to Mr. Harkat's email account. They ask that Mr. Harkat be allowed only one (1) email account under the following conditions:

(i) The email account must be web-based;

(ii) Mr. Harkat shall not access his email through a web browser. He shall only access his email through an email client such as Outlook or Thunderbird, set up on his home computer. Whichever email client is used, it is prohibited to configure it to allow access to any chat applications;

(iii) Mr. Harkat shall provide the email address, username and password to CBSA immediately upon setting up the email account. Mr. Harkat must provide the CBSA with any updates to his email account immediately upon making any changes;

(iv) Mr. Harkat shall consent to CBSA, or any person designated by it, having access, without notice, to his email account, including his full and correct password at all times;

(v) Mr. Harkat must ensure that no one else, except for him and the CBSA or agents of the CBSA, have access to his account;

(vi) Mr. Harkat shall not alter or modify any sent or received emails and he shall not delete any sent, received, or drafted emails without express permission in writing from CBSA officials;

(vii) Mr. Harkat shall not participate in any email communication over which he can claim solicitor-client or litigation privilege.

[82] In my view, the conditions under paragraphs (i) and (iii) to (vii) do not constitute a significant change from the current situation. Mr. Harkat's email account is already web-based and the CBSA has access to his email address, username and password. Mr. Harkat is required to provide the CBSA any passwords required to access any part of his computer. I have already indicated that this includes his email account. His current conditions also prevent him from altering or modifying any sent or received emails, and he is not permitted to delete any sent, received or drafted emails without express permission in writing from CBSA officials.

[83] The most significant change requested by the Ministers is that Mr. Harkat only be able to access his email account through an email client like Microsoft Outlook or Mozilla Thunderbird.

According to the Ministers, an email client would provide a level of protection for the CBSA officials to monitor Mr. Harkat's emails.

[84] The evidence of the Ministers' digital forensic investigators is that the CBSA's digital forensic software tools can download certain cloud content, but the information it retrieves is not as extensive as what can be retrieved from an analysis of the disk image. The CBSA's ability to extract online data is limited to those files which are live, meaning that it cannot recover deleted items from "cloud sources". When someone accesses their email account through a web browser, they can alter or delete messages while leaving little to no trace. According to Mr. Fernando, it is highly unlikely that the CBSA's examination tools would be able to trace the altered or deleted messages, let alone even indicate whether a communication has been deleted or altered.

[85] On the other hand, if an individual accesses his or her email account through an email client, such as Microsoft Outlook or Mozilla Thunderbird, it is much more difficult for the individual to alter or delete email messages without leaving a trace. This is because an email client is typically configured to store messages locally on the user's computer. An email client can also be configured to leave messages intact on the email server while disabling functions that would delete messages for clean-up or drive storage purposes. This would facilitate the CBSA's access to Mr. Harkat's email account through its existing inspection process.

[86] Mr. Ellwood suggested that the CBSA could achieve similar results using a retention policy called a "litigation hold". He also indicated that the CBSA could be the administrator of

the associated email account that Mr. Harkat could then use. According to Mr. Ellwood, a litigation hold would be inexpensive and relatively easy to do.

[87] Given that the two (2) breaches alleged against Mr. Harkat relate to the use of his email account, I find that the Ministers' request is not only justified but also reasonable. Because Mr. Harkat's emails would be stored locally on his computer until further review by the CBSA, an email client would avoid potential problems in the future and protect Mr. Harkat from unfounded allegations of breach of conditions. As the Ministers did not indicate a preference between Microsoft Outlook and Mozilla Thunderbird, I will leave the choice to Mr. Harkat.

[88] As for the Ministers' request to limit Mr. Harkat to one (1) email account, I am not persuaded that this restriction is justified. I can think of several reasons why a person would want to have more than one (1) email account. For instance, the person may use a secondary account to divert unsolicited emails away from their primary account. A person may also have another account through their employer or their educational institution. If Mr. Harkat decides to use additional email accounts, I am satisfied that the CBSA's concerns will be attenuated provided that Mr. Harkat shares his account credentials and the other stated conditions apply to each of his email accounts. Mr. Harkat will be restricted to a maximum of three (3) email accounts.

(4) Other Ongoing Issues Raised by Mr. Harkat

[89] Aside from the changes examined above, Mr. Harkat is proposing changes relating to his use of a mobile telephone, the location where he may use his laptop, his computer inspections,

his reporting conditions, his travel outside of the National Capital Region, the people who reside with him and the CBSA's surveillance.

(a) *Mobile Telephone*

[90] Mr. Harkat is proposing that he be permitted to have a mobile telephone for his personal use. He would not store solicitor-client information on the telephone, and he would make it available for inspection by the CBSA at reasonable intervals. The current "mobile telephone" conditions would continue, including the requirements that Mr. Harkat (1) must not permit any other person to use his mobile telephone; (2) must provide the CBSA with the name of the service provider, the telephone number and passwords to access the telephone; (3) must consent to the CBSA, or any person designated by it, obtaining and monitoring the toll records of voice calls and text messages from the service provider; and (4) must consent to the CBSA obtaining any Court order that may be required in order to obtain these toll records.

[91] The Ministers submit that there is no basis to support this request given the alleged breaches. Mr. Harkat has had permission to use a mobile telephone for personal use since 2014, based on orders issued by Mr. Justice Simon Noël dated October 31, 2014 and January 16, 2015. In addition, at the last review in November 2017, Mr. Harkat advised the Court that he was not seeking any changes to the terms and conditions associated with a mobile telephone for personal use. The Ministers submit that if Mr. Harkat wishes to begin using a mobile telephone for personal use, he can do so in accordance with condition 4 of the terms and conditions.

[92] During my last review, I indicated that since Mr. Harkat was no longer seeking to have access to a mobile telephone with internet connectivity, condition 4 would remain the same, subject to a few modifications. I also provided that the parties could return to Court when Mr. Harkat was ready to possess a SIM card mobile telephone with internet connectivity, at which point I would expect Mr. Harkat to demonstrate why he requires a mobile telephone with internet connectivity, how he intends to use it and for what purposes. As for the Ministers, I indicated that I would expect them to adduce evidence demonstrating how the examination of internet usage on a mobile telephone differs from that of a computer, whether particular models have greater storage capacity and what type of supervision would be required to accommodate the use of a mobile telephone with internet connectivity.

[93] The Ministers' evidence is that it is difficult to monitor mobile telephone usage. Mobile telephones generally hold less data than personal computers and, as such, deleted data is more likely to be overwritten on a mobile telephone than on a personal computer. The ability to recover deleted data is more limited on a mobile telephone because both the amount of data that can be retrieved and the window of time in which it can be retrieved are narrower. The Ministers did not provide any evidence on whether particular models have greater storage capacity or on what type of supervision would be required to monitor Mr. Harkat's usage effectively.

[94] Mr. Harkat's wife provided written testimony that her husband wishes to continue to use the mobile telephone provided by his employer, which does not have internet connectivity, because he needs it for his work and to communicate with her. He would also like permission to

use other mobile or landline telephones in order to report to the CBSA or in case of an emergency while travelling.

[95] Mr. Harkat testified that he has tried many places to obtain a “simple phone”, but he claims it is impossible to find a mobile telephone without internet connectivity that can be activated by a service provider.

[96] I am inclined to grant Mr. Harkat’s request to have access to a mobile telephone with internet connectivity for a number of reasons. First, I agree with Mr. Harkat that the evolving nature of consumer technology is making it harder and harder to find a mobile telephone without internet connectivity, whether over cellular data networks or Wi-Fi networks. Second, even if Mr. Harkat’s current employer is able to confirm that the telephone they provide does not have internet connectivity, the CBSA has no control over that telephone. It cannot inspect that telephone, and it appears that Mr. Harkat is not the sole user of the telephone. Third, the CBSA will have access to Mr. Harkat’s social media and other online accounts in order to monitor his communications. Fourth, the CBSA will continue to monitor his emails, and the new condition that he use an email client on his computer will facilitate this monitoring. Finally, his ability to use a personal mobile telephone with internet connectivity would be subject to a number of conditions, to be determined, to ensure that the CBSA is able to monitor the mobile telephone effectively. In fact, Mr. Harkat’s counsel indicated in her submissions that her client would be willing to have the telephone inspected on a weekly basis, if necessary.

[97] As the evidence has demonstrated, there are a number of factors that can influence or affect the CBSA's ability to monitor a mobile telephone. Accordingly, prior to obtaining the mobile telephone, Mr. Harkat must provide the CBSA the make and model number of the mobile telephone he intends to use, its storage capabilities, the name of the service provider, and details of the wireless plan he intends to use. Within five (5) business days of receiving this information, the CBSA must inform Mr. Harkat of the frequency at which inspections will be required to ensure that data is not overwritten. At the same time, the CBSA will indicate what conditions are required to monitor Mr. Harkat's use of the telephone beyond those proposed by Mr. Harkat at page 58 of his motion record. If the parties are unable to agree on the frequency of inspections and the conditions of use, they may seek the assistance of the Court.

[98] Until then, subject to my comments in the preceding paragraph, the conditions regarding Mr. Harkat's use of a mobile telephone for personal use will remain unchanged. For greater certainty, this does not affect the amendment to condition 4r), discussed above, which governs his use of a mobile telephone for employment purposes. The Ministers have also suggested two (2) other variations (conditions 4t) and 4u)), but these do not appear to be relevant until Mr. Harkat wishes to use a mobile telephone for personal use with internet connectivity.

(b) *Laptop*

[99] Mr. Harkat asks the Court to remove the words "at his residence" at the beginning of condition 7 of the terms and conditions so that he may use his laptop outside of his home.

[100] In my last review, the Ministers objected to Mr. Harkat's request to use the laptop outside his home because the CBSA would not be able to monitor and ensure that Mr. Harkat is not engaging in unauthorized or improper communications. In my reasons, I indicated that if Mr. Harkat wished to use the laptop outside his home, he should be prepared to demonstrate why he needed to do so. I also indicated that the CBSA should be prepared to demonstrate, with sufficient detail, why Mr. Harkat's request could not be accommodated.

[101] Mr. Harkat's submissions on this review did not explicitly address this issue. Moreover, little evidence was presented to satisfy the instructions provided in my last review. Although I have decided to allow Mr. Harkat to use his personal computer laptop while at work, I am not prepared to make other exceptions at this time. Therefore, the words "at his residence" will remain in condition 7.

(c) *Computer Inspections*

[102] The Ministers were originally seeking to increase the frequency of Mr. Harkat's computer inspections from every three (3) months to every month. However, on October 15, 2019, the Ministers amended their application in light of their inability to demonstrate that Mr. Harkat had used the "InPrivate Browsing" feature of Internet Explorer. In so doing, they abandoned their request for monthly inspections.

[103] Meanwhile, Mr. Harkat is seeking to reduce the frequency to every six (6) months.

[104] I cannot grant Mr. Harkat's request to reduce the frequency of inspections. The CBSA must be able to effectively monitor Mr. Harkat's computer use, especially given the evolving nature of consumer technology, together with his now-expanded access to different web browsers and online accounts. For these reasons, the condition relating to the frequency of inspections will remain at three (3) months.

(d) *Reporting Conditions*

[105] In my last review, Mr. Harkat's reporting requirements were reduced from reporting to the CBSA every two (2) weeks to once a month on a day and at a time as determined by a representative of the CBSA. The condition also provided that the reporting requirements could be reduced by the CBSA without seeking the permission of the Court.

[106] Mr. Harkat seeks to amend this condition so that he will only be required to report to the CBSA once every three (3) months.

[107] As I have no evidence on the frequency of the reporting and how it is working, I am not prepared to vary this condition.

(e) *Travel*

[108] In my last review, I expanded the window of opportunity for Mr. Harkat to travel anywhere in Ontario and Quebec without having to notify the CBSA. I was of the view that a window of seventy-two (72) hours was both proportionate and reasonable given Mr. Harkat's

past compliance with his conditions and the minimal risk associated with relaxing this condition. This gave Mr. Harkat and his family more flexibility in their outings by allowing them to visit friends and family on long weekends without the stress of having to report daily to the CBSA, particularly where there are no telephones readily available, such as when they visited the cottage of Ms. Harkat's sister.

[109] Mr. Harkat is now asking the Court to allow him to travel within Ontario and Quebec for up to one hundred and twenty (120) hours without having to notify the CBSA. In her affidavit, Ms. Harkat states that the change in 2018 was very positive for them and their entire family, and she identifies the places where they have travelled as a result. While the change has been positive, she explained in her testimony that she has family in northern Quebec but, because of the distance, they lose a day to drive there and another to drive back. She also stated that her family has timeshares in Ontario where they would like to travel.

[110] The Ministers take the position that further relaxation of the conditions is not warranted due to the breaches.

[111] Despite finding that Mr. Harkat breached one of his conditions relating to the use of his computer, I have no evidence that Mr. Harkat has misused the expanded travel condition. I find his reasons compelling and, therefore, I am prepared to grant him an additional twenty-four (24) hours to travel within Ontario and Quebec without having to notify the CBSA. This will give Mr. Harkat two (2) full days to visit his wife's family, after accounting for travel time.

(f) *Residence*

[112] Mr. Harkat is proposing to eliminate the requirement that other occupants of his home sign an agreement to let the CBSA access the residence. Aside from Ms. Harkat, there are currently no other occupants, and there is no plan to add other occupants.

[113] Under the terms and conditions of release, all other occupants of the residence or any new occupant shall sign a document, in a form acceptable to counsel for the Ministers, agreeing to abide by its terms. It appears that Mr. Harkat is asking that only his wife, currently the only other occupant of the residence, be required to sign the document.

[114] I am not prepared to remove this condition. If there are no plans to add occupants, no inconvenience is caused to anyone. If the Harkats decide to add other occupants, the CBSA has an interest in ensuring that these occupants agree to abide by the conditions of Mr. Harkat's release.

(g) *Surveillance*

[115] In my last review, I indicated that I had concerns regarding the degree of intrusiveness of the CBSA's physical surveillance and the absence of any framework to review and ensure that any physical surveillance is conducted in the least intrusive manner possible. The CBSA agreed to review its monitoring process to ensure that the proper balance is maintained between the risk posed by Mr. Harkat and the need to ensure that the terms and conditions are being respected. I urged the CBSA to adopt a monitoring process devoid of arbitrariness, which ensures

proportionality, guidance and periodic reviews. I also stipulated that Mr. Harkat's terms and conditions be amended to explicitly address the issue of monitoring.

[116] The current condition on surveillance reads as follows:

> 20. The CBSA's surveillance of Mr. Harkat shall be conducted in the least intrusive manner possible and should not be disproportionate with the danger posed by Mr. Harkat. The CBSA shall ensure its officers are provided guidance on the timing and manner of physical surveillance, and that periodic reviews of the appropriateness of the monitoring measures is undertaken;

[117] Mr. Harkat is now requesting that the CBSA only engage in surveillance to address a real and subsisting danger posed by him. He also requests that the CBSA be required to report to the Court once a year on (1) its efforts to provide guidance on the timing and manner of physical surveillance and (2) on its periodic reviews of the appropriateness of monitoring measures.

[118] Mr. Connelly provided evidence on the manner in which the CBSA conducts its surveillance. He testified that the CBSA had reduced the frequency and duration of surveillance. He also indicated that the CBSA had established a monitoring framework for surveillance.

[119] Ms. Harkat testified that she believed that the CBSA conducted surveillance on average two (2) to three (3) times a week. Mr. Harkat testified that it was more like three (3) times a month. His testimony is more consistent with the monthly monitoring summary provided by the CBSA to Mr. Harkat's counsel and to the Court.

[120] In my last review, I accepted that monitoring is necessary to ensure that Mr. Harkat is complying with the terms and conditions of his release. It appears from the evidence that the CBSA may have construed this statement as an obligation to conduct surveillance. That is not the case. Monitoring can come in many forms, physical surveillance being only one. For example, Mr. Harkat's computer use is monitored through the inspection of his computer and remote monitoring of his email account. In the case of physical surveillance, it may act as a deterrent against doing or hiding a prohibited activity, but its purpose should be related to a specific activity that Mr. Harkat is prohibited from doing or required to do under his terms and conditions of release. In every case, surveillance should be conducted in the least intrusive manner possible, and it should not be disproportionate with the danger posed by Mr. Harkat. I would also recommend that any future surveillance be conducted, to the extent possible, in such a way as to avoid further stigmatizing Mr. and Ms. Harkat with their family, friends and neighbours.

[121] That being said, I am not persuaded that surveillance should be limited to only those situations where its purpose is to address a real and substantive danger posed by Mr. Harkat, as his counsel argued. While I recognize that surveillance may be intrusive, I reiterate that it is an unfortunate consequence of being the subject of a security certificate.

[122] I am not prepared to allow the changes proposed by Mr. Harkat, including the one which would require the CBSA to report its monitoring measures to the Court on an annual basis. However, in future reviews, I will expect the CBSA to present detailed evidence on its efforts to ensure that its monitoring measures are conducted in the least intrusive manner possible and

remain proportionate to the danger posed. To the extent possible, such evidence should also be made available to Mr. Harkat's counsel.

(5) Informal Resolution

[123] During their submissions, counsel suggested that a mechanism be put in place whereby some of the disputes between the parties could be better resolved in a non-litigious manner. According to Mr. Harkat's counsel, there were meetings initially with the CBSA to set up a framework for how these proceedings would unfold. She also indicated that, in another security certificate case in which she was involved, the judge had arranged for some form of arbitration or mediation where the parties would speak "off the record". This was very effective, in her opinion. In her view, a similar approach would not be a problem in this case, and she suggested that such an approach could be adopted either with the Court's assistance or by the parties first trying to resolve outstanding issues amongst themselves.

[124] I commend counsel for recognizing that many issues could be resolved proactively if the parties were able to discuss them outside of an adversarial context. I am of the same view. The parties are encouraged to resolve their differences through less costly and non-confrontational processes, which could include private mediation, court-assisted mediation or other form of dispute resolution.

III. Conclusion

[125] On the basis of the foregoing reasons, I conclude that the adjustments discussed above are sufficient to neutralize the danger Mr. Harkat presents and are proportional to the risk he poses. The remaining terms and conditions remain unchanged.

[126] Following receipt of these reasons, the Ministers will have ten (10) days to draft the new terms and conditions of Mr. Harkat's release from detention, consistent with the determinations in these reasons, and submit them to Mr. Harkat's counsel for approval. If the parties are unable to agree on the wording of the draft revised terms and conditions, they may report back to the Court for a determination. Once approved by the parties and the Court, the revised terms and conditions will become a schedule to an order to be issued by the Court at a later date. The revised terms and conditions will take effect on the signing of that order. The Ministers will immediately take whatever steps are necessary to give effect to the new terms and conditions.

[127] The parties are invited to submit serious questions of general importance pursuant to section 82.3 of the IRPA. They shall have ten (10) days to do so and an additional five (5) days to comment on the questions submitted, if any.

"Sylvie E. Roussel"
Judge

Ottawa, Ontario
June 19, 2020

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	DES-5-08
STYLE OF CAUSE:	IN THE MATTER OF a certificate signed pursuant to subsection 77(1) of the *Immigration and Refugee Protection Act* and IN THE MATTER of Mohamed Harkat
PLACE OF HEARING:	HELD IN PERSON IN TORONTO (ONTARIO) AND BY VIDEOCONFERENCE FROM OTTAWA, (ONTARIO)
DATE OF HEARING:	SEPTEMBER 18, 19, 20, 2019 OCTOBER 15, 16, 2019
REASONS FOR ORDER:	ROUSSEL J.
DATED:	JUNE 19, 2020

APPEARANCES:

Barbara Jackman	FOR MOHAMED HARKAT
Nadine Silverman Kevin Spykerman	FOR THE MINISTERS

SOLICITORS OF RECORD:

Jackman, Nazami & Associates Barristers & Solicitors Ottawa, Ontario	FOR MOHAMED HARKAT
Attorney General of Canada Ottawa, Ontario	FOR THE MINISTERS