Federal Court  Cour fédérale

~~**TOP SECRET**~~

Date: 20190201

Docket: CSIS-28-18

Citation: 2019 FC 141

Ottawa, Ontario, February 1, 2019

PRESENT: The Honourable Mr. Justice Fothergill

BETWEEN:

IN THE MATTER OF AN APPLICATION BY [redacted] FOR WARRANTS PURSUANT TO SECTIONS 12 AND 21 OF THE *CANADIAN SECURITY INTELLIGENCE SERVICE ACT*, RSC 1985, c C-23

AND IN THE MATTER OF ISLAMIST TERRORISM – [redacted]

REASONS FOR ORDER

I. Overview

[1] On October 16, 2018, I issued a series of warrants pursuant to ss 12 and 21 of the *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 [*CSIS Act*] in furtherance of an ongoing investigation by the Canadian Security Intelligence Service [CSIS or the Service] into Islamist terrorism and a named individual. Two of those warrants authorize the Director of CSIS

and any employee of the Service acting under his authority to install, maintain, remove [redacted] "any thing" on a computer or portable communications device in order to intercept communications and obtain information. This technique is commonly described as installing an "implant" on a device.

[2] In effect, a collection implant enables the Service to covertly receive a copy of what a subject of investigation [redacted] on a computer or portable communications device [collectively, device]. The Service also uses implants to conduct remote searches of devices and obtain information including, but not limited to, images, documents, e-mail messages, [redacted] Collection from an implant is done on an ongoing basis without the user's knowledge.

[3] Counsel representing the Attorney General of Canada acknowledged that certain powers sought in the warrants are novel, and could raise questions regarding compliance with the *Canadian Charter of Rights and Freedoms*[1] [*Charter*], and the privacy rights or interests of persons who could be affected by their exercise. The Court convened an oral hearing to hear from counsel for the Attorney General, the CSIS employee who applied for the warrants, and two additional affiants.

[4] The Court also appointed a security-cleared *amicus curiae*. The *amicus curiae* was given access to relevant documents, and was offered the opportunity to cross-examine all affiants and make submissions orally and in writing. The Court directed the *amicus curiae* to present his

[1] Part 1 of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

considered and professional opinion regarding the legal and other issues raised by the application. The *amicus curiae* was not obliged to adopt an adversarial position if he did not consider this to be necessary or justified.

[5] After hearing from the affiants, reading the materials filed, and considering the submissions of counsel for the Attorney General of Canada and the *amicus curiae*, I concluded that the requirements of s 21(2)(a) and (b) of the *CSIS Act* were met and the warrants should be issued with minor modifications. These are the reasons for that decision.

II. New Powers Sought

[6] Before installing an implant on a device, the Service seeks to identify the device used by the subject of its investigation. This is typically accomplished by recourse to human sources, surveillance, interviews, cell-site simulators, or requests to domestic or foreign law enforcement and intelligence agencies. It may also be facilitated by the interception of communications and information obtained from communications service providers. If the subject of investigation [redacted] CSIS may seek the assistance of the Communications Security Establishment to conduct the investigative steps authorized by the warrants.

[7] When performing a remote installation of an implant, the Service first collects preliminary information in order to confirm that the implant is being installed on a device that belongs to or is used by the subject of investigation. The new powers sought in the warrants are

intended to reflect the practical reality that the Service may not be able to determine, prior to installing an implant, whether the device belongs to or is used by the subject of investigation.

[8] The warrants authorize employees of the Service to remotely install an implant on any device that is [redacted] by the subject of investigation; [redacted] by the subject of investigation. [redacted]

[9] Depending on the kind of implant used, the Service may require an Internet warrant to be in force. The Internet warrant authorizes the Service to intercept communications destined to or originating from an Internet services account [redacted] a subject of investigation.

[10] Where an implant is remotely installed on a device [redacted] a survey of the device is performed prior to intercepting communications and obtaining the information described in the warrants. The survey information may include: [redacted] operating system information, device make and model, network addresses, [redacted]

[11] Other information may also be obtained at the survey stage in order to protect the security of the implant: [redacted]

[12] Depending on whether the Service is operating pursuant to a portable device warrant or a general intercept and search warrant, a designated Service employee reviews the survey information and determines whether the device is (a) a portable device owned, leased or used by the subject of investigation; or (b) a computer holding information that may be obtained pursuant to the general intercept and search warrant. If the device falls within one of these two categories, then the survey information is retained and the interception and collection from the device commences. If the device does not fall within one of these two categories, then the survey information is destroyed as soon as reasonably practicable, but no later than six months from the date it was obtained.

[13] If the device is neither owned nor leased by the subject of investigation, but the designated Service employee has reasonable grounds to believe that it is used by the subject, then the Regional Director General may authorize interception. Survey information which may assist the Regional Director General's exercise of this responsibility may be retained for this purpose. Due to the exigencies of the investigation, the determination is usually made quickly.

[14] The warrants also authorize [redacted] using what is referred to as a [redacted]

[redacted] A survey is not required for [redacted] because a determination has already been made that the implant has been installed on a device belonging to or used by a subject of investigation.

[15] In addition, the warrants authorize the [redacted] of a device belonging to a third party where the Service installs an implant on a device which is subsequently determined at the survey stage to be unconnected to the target of investigation. The warrants permit the Service to [redacted] the third party's device that will enable CSIS to distinguish it from the device belonging to or used by the subject of investigation. Once installed, the [redacted] As this information does not relate to a subject of investigation, it is destroyed as soon as reasonably practicable, but no later than six months from the date it was obtained.

[16] While much of the information obtained at the survey stage will reveal little or no core biographical information about the individual who owns or uses the device, some of it may. Depending on [redacted] may disclose sensitive personal information. [redacted]

III. Issue

[17] The legal issue raised by these warrant applications is whether the safeguards proposed by the Service during the survey stage are sufficient to protect the *Charter* and privacy rights or interests of innocent third parties whose personal information may be collected during the remote installation of an implant on a device.

IV. Analysis

[18] The installation of an implant on a device is authorized under standard provisions of warrants that permit the interception of communications, the acquisition of information and images, and the tracking or geolocation of a subject of investigation. The Service has previously sought to intercept communications or obtain information from a device by remotely installing an implant. This technique, including the use of a survey stage to identify the correct device, was explained to the Court during an *en banc* presentation on December 15, 2017.

[19] In the course of the *en banc* presentation, Chief Justice Paul Crampton expressed the view that a survey stage should be mandatory before full data collection using an implant can begin. This is the first time the Court has been asked to consider the language of the new warrant condition.

A. *General Principles*

[20] The Court may grant a warrant enabling CSIS to collect information and intelligence under s 12 of the *CSIS Act* only when the requirements of s 21(2) are met. The Court must be satisfied, *inter alia*, that a warrant is required to investigate a threat to the security of Canada, and that other investigative measures have been tried and have either failed or are unlikely to succeed. The Federal Court of Appeal observed in *Atwal v Canada*, [1988] 1 FC 107 at paragraph 37 that "it will be generally less practically possible to be specific, in advance, in authorizations to intercept private communications under the [CSIS] Act than under the Criminal Code."

[21] A search pursuant to a CSIS warrant may be unreasonable and contrary to s 8 of the *Charter* if it is not carried out in a reasonable manner. This may be because the issuing justice failed to limit the breadth of the authorization, or because the persons carrying out the search failed to adhere to minimization principles in executing the warrants (*Canada (Attorney General) v Huang*, 2018 FCA 109 at para 28).

[22] There is a high expectation of privacy in a computer or a cell phone. As the Supreme Court of Canada held in *R v Vu*, 2013 SCC 60 at paragraphs 40 to 44, it is difficult to imagine a more intrusive invasion of privacy than a search of these devices. Personal computers store immense amounts of information, some of which may touch the "biographical core of personal information". In addition, computers contain information that is automatically generated, often without the knowledge of the user, and a computer may retain files and data long after users

think they have been deleted. When connected to the Internet, computers serve as portals to an almost infinite amount of information that is shared between different users and is stored almost anywhere in the world. Similarly, a computer that is connected to a network may allow police and intelligence agencies to obtain access to information on other devices.

[23] In *R v Marakah*, 2017 SCC 59 at paragraph 37, the Supreme Court of Canada remarked that electronic conversations are capable of revealing a great deal of personal information. Preservation of a "zone of privacy" in which personal information is safe from state intrusion is the very purpose of s 8 of the *Charter*. This zone of privacy extends beyond one's own mobile device. It can include electronic conversations in which one shares private information with others. It is reasonable to expect these private interactions, and not just the contents of a particular cell phone at a particular point in time, to remain private.

B. *Remote Searches*

[24] A remotely installed implant may enable CSIS to intercept [redacted] the installation of an implant on a device that is used by or belongs to an innocent third party is a real possibility. If the [redacted] is associated with a public place, such as an Internet café, it becomes highly likely.

[25] The *amicus curiae* informed the Court that Canadian jurisprudence addressing the legal implications of remotely installed implants is sparse. He referred the Court to the following

excerpt from Gerald Chand and Susan Magotiaux, *Digital Evidence: A Practitioner's Handbook* (Toronto: Emond Professional, 2018) at page 47:

> What about when the state wants to access data on a computer without actually entering the place where the computer is located? More creative methods of remote data access are yet to be comprehensively considered in Canada courts, though there have been attempts in the United States for state actors to seek judicial authorization for offsite access through the use of programs delivered covertly to a target machine.

[26] In "Modern Technology and Privacy Rights: Leading Canadian and U.S. Case Law", (Ontario Bar Association, 2013), Assistant Crown Attorney Brock Jones refers to a case in which parole authorities were denied a warrant to search for breaches of a long-term supervision order. Mr. Jones offers the following comments at page 8:

> The government's reliance on an IP address associated to emails sent and received from the presumed "target computer" lends itself to potential pitfalls. The person(s) sending the emails in question may have used "spoofing" software to disguise their true IP address, and therefore the installation of the Trojan software could target innocent computer users and their computers. The computer in question could also be in a public space such as a café or library. Installation of the spyware would potentially capture many innocent persons utilizing the computer for innocent purposes. The government's application would also permit real-time video surveillance via the computer's webcam. As such, the government must apply for a wiretap authorization, not a warrant. Future applications must address the court's concerns before a warrant would issue. [Emphasis added]

[27] *In re Warrant to Search a Target Computer at Premises*, 2013 WL 1729765 at pages 3 and 4, United States Magistrate Judge Stephen W.M. Smith of the District Court for the Southern District of Texas, Houston Division, refused an application for a warrant to target a computer

remotely. While the ruling must be understood within the unique legal context of that jurisdiction, Judge Smith asked a number of questions that are potentially germane to the present case:

> This "method" of software installation is nowhere explained. Nor does the Government explain how it will ensure that only those "committing the illegal activity will be ... subject to the technology." What if the Target Computer is located in a public library, an Internet café, or a workplace accessible to others? What if the computer is used by family or friends uninvolved in the illegal scheme? What if the counterfeit email address is used for legitimate reasons by others unconnected to the criminal conspiracy? What if the email address is accessed by more than one computer, or by a cell phone and other digital devices? <u>There may well be sufficient answers to these questions, but the Government's application does not supply them</u>. [Emphasis added]

[28] In "Beware of Government Agents Bearing Trojan Horses", Akron Law Review: Vol. 48: Iss. 2, Article 4 at pages 345 to 347, Assistant Professor Brian Owsley of Texas Tech University Law School suggests that concerns of this nature may be addressed through a prior authorization process, and by putting protocols in place. In particular: (a) investigators must be barred from keeping third party information that is unrelated to the investigation; (b) investigators must distinguish between information that is relevant to the subject of the investigation on the targeted computer and non-relevant materials, such as personal photos and financial information that does not evidence any criminal activity; and (c) hard copies of irrelevant materials must be destroyed, and any electronic records must be deleted.

C. *Minimization Protocols*

[29] The destruction of data seized from innocent third parties is one way to limit the invasiveness of an electronic search, but it is not the only one. The warrant itself may minimize intrusion into the *Charter* rights and privacy interests of third parties.

[30] In *R v Thompson*, [1990] 2 SCR 1111 [*Thompson*], the Supreme Court of Canada considered a "resort to" clause in an authorization to intercept private communications. The clause would authorize the police to monitor communications from a location the target may "resort to", in this case a pay telephone available to the public. Justice John Sopkina said the following at paragraphs 113 and 114:

> In any authorization there is the possibility of invasion of privacy of innocent third parties. For instance a wiretap placed on the home telephone of a target will record communications by other members of the household. This is an unfortunate cost of electronic surveillance. But it is one which Parliament has obviously judged is justified in appropriate circumstances in the investigation of serious crime.
>
> In my view, in some cases the possibility of invasion of privacy of innocent persons may become so great that it requires explicit recognition along with the interests of the investigation of crime. A "resort to" clause creates just this possibility if among the places resorted to are telephones frequently used by the general public or other such places. I do not mean to suggest that there should be a constitutional prohibition of intercepting communications at places frequented by the public; in that case drug importing conspiracies could virtually insulate themselves from perhaps the only effective investigative technique against them merely by using public places to conduct their business.

[31] The Supreme Court did not find the "resort to" clause to be unlawful under the relevant provisions of the *Criminal Code*, and the authorizations were found to be valid. However, given the extent of the invasion of privacy authorized, a total absence of any protection for the public created a potential for carrying out searches and seizures that were unreasonable. Justice Sopinka explained at paragraph 119:

> Interceptions which were made pursuant to these authorizations, which were simply fishing expeditions and not based on reasonable and probable grounds for believing the target would be utilizing the pay telephones at the time, were, in my opinion, unreasonable. In most instances, it would be preferable to have actual physical surveillance of the public telephone to ensure that it is being used by the target. This is said to be normal police practice. I am, however, in agreement with Martin J.A. and Professor Stanley A. Cohen that to make this an absolute requirement would impose too heavy a burden on Canadian law enforcement officials.

[32] Although *Thompson* was decided almost three decades ago when the Internet was still in its infancy, the principle remains valid and applicable here. Minimization conditions in a warrant may not be required in every case, but they may be required in some cases depending on the extent of the potential invasion of the privacy of innocent third parties.

[33] More recently, the Supreme Court of Canada decided in *Vu* that a warrant was needed to explicitly authorize the search of a computer. The police could not rely on a warrant to search the residence from which the computer was seized.

[34] The Supreme Court in *Vu* proposed, in effect, to treat computers as if they were a separate place of search necessitating distinct prior authorization. However, Justice Thomas

Cromwell was not persuaded that s 8 of the *Charter* requires that the manner of searching a computer always be spelled out in advance. He reached this conclusion for two reasons. First, the manner of search in a criminal investigation is generally reviewed after the fact, which is better suited to developing new rules about how searches should be conducted than the *ex parte* procedure by which warrants are issued. Second, requiring search protocols to be imposed in advance of the search would add significant complexity and practical difficulty at the authorization stage. Attempts to impose search protocols during the authorization process risk creating blind spots in an investigation, undermining the legitimate goals of law enforcement that are recognized in the pre-authorization process. These problems are magnified by rapid and constant technological change.

[35] While search protocols may not be constitutionally required in all cases, authorizing justices must assure themselves that the warrants they issue fulfil the objectives of prior authorization. They also have the discretion to impose conditions to ensure they do. Justice Cromwell observed that an authorization might include directions concerning the manner of search. He did not foreclose the possibility that our developing understanding of computer searches and changes in technology may make it appropriate to impose search protocols in a broader range of cases in the future (*Vu* at para 62).

[36] The *amicus curiae* notes that there are a number of important differences between the use of warrant powers by the police and those employed by CSIS. One of the rationales provided by Justice Cromwell in *Vu* for not requiring search protocols in all warrants was that the reasonableness of the search was best examined after the fact. However, very few warrants

issued to the Director of CSIS are examined after the fact, in large measure because they are unlikely to result in criminal charges. Justice Cromwell's concern about complexity and inadvertently limiting the effectiveness of investigation does not arise here. The affiants have proposed a workable protocol which is currently being used on an informal basis.

[37] Given the extent of the potential invasion of the privacy of innocent third parties, the Attorney General of Canada and the *amicus curiae* agree that minimization conditions are required in warrants that authorize the remote installation of implants on devices. The *amicus curiae* has proposed that, consistent with the Chief Justice's recommendation at the *en banc* presentation on December 15, 2017, the survey stage be made mandatory before full data collection commences. He also recommends that the data obtained at the survey stage be strictly limited to the categories described in paragraphs 10 and 11 of these Reasons for Order.

[38] With these modifications, I am satisfied that the searches to be conducted under warrants requested by the Director of CSIS are reasonable. The search protocols are sufficiently robust to safeguard the *Charter* and privacy rights or interests of innocent parties. The warrants should therefore be granted.

V. Conclusion

[39] The warrants that authorize the remote installation of an implant on any device, including one that belongs to or is used by an innocent third party, may only be issued with the following search protocols:

1. Where an implant is remotely installed on a device [redacted] a survey of the device must be performed prior to intercepting communications and obtaining the information described in the warrants.

2. The data obtained at the survey stage must be limited to those described in paragraphs 10 and 11 of these Reasons for Order.

3. A designated Service employee must review the data obtained at the survey stage and determine whether there are reasonable grounds to believe that the device is (a) a portable device belonging to or used by the subject of investigation; or (b) a computer holding information that may be obtained pursuant to a general intercept and search warrant.

4. If either condition 3(a) or (b) is met, then the survey information may be retained and full interception and collection from the device may commence.

5. If neither condition 3(a) or 3(b) is met, then the survey information must be destroyed as soon as reasonably practicable, but no later than six months from the date it was obtained. No further use of the survey information may be made.

"Simon Fothergill"
Judge

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	CSIS 28-18
STYLE OF CAUSE:	IN THE MATTER OF AN APPLICATION BY [redacted] FOR WARRANTS PURSUANT TO SECTIONS 12 AND 21 OF THE CANADIAN SECURITY INTELLIGENCE SERVICE ACT, RSC 1985, c C-23 AND IN THE MATTER OF ISLAMIST TERRORISM – [redacted]
PLACE OF HEARING:	OTTAWA, ONTARIO
DATE OF HEARING:	SEPTEMBER 25, 2018
REASONS FOR ORDER:	FOTHERGILL J.
DATED:	FEBRUARY 1, 2019

APPEARANCES:

Stéphanie Dion Andrew Cameron	FOR THE APPLICANT
Ian Carter	*AMICUS CURIAE*

SOLICITORS OF RECORD:

Attorney General of Canada Ottawa ON	FOR THE APPLICANT
Bayne Sellar Ertel Carter Ottawa ON	*AMICUS CURIAE*