Federal Court Cour fédérale

~~**TOP SECRET**~~

Date: 20251216

Docket: C-1-24

Citation: 2025 FC 1978

Ottawa, Ontario, December 16, 2025

PRESENT: The Honourable Madam Justice Kane

BETWEEN:

IN THE MATTER OF an application by [...] 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 CYBER ESPIONAGE, CYBER SABOTAGE, and CYBER FOREIGN-INFLUENCED ACTIVITIES

REASONS

I. Background

[1] On February 16, 2024, the Court granted the application for a warrant pursuant to sections 12 and 21 to authorize the Canadian Security Intelligence Service [CSIS or the Service] to investigate threats to the security of Canada posed by cyber espionage, cyber sabotage and cyber foreign-influenced activities, referred to as "the cyber warrant". The warrant covered the period [...], to [...].

[2] The cyber warrant authorized the Service to intercept any communication destined to or originating from infrastructure associated with specific Internet Protocol [IP] addresses, [...], and any other infrastructure subject to an Order of this Court pursuant to Condition 3 of the

warrant. The cyber warrant also authorized the Service to obtain information [...] relating to the specified infrastructure.

[3] Condition 3 of the cyber warrant permits the Service to bring a supplemental application to this Court where the Service identifies additional infrastructure.

[4] On February 29, 2024, the Service filed a supplemental application pursuant to Condition 3 to execute powers with respect to newly identified infrastructure, in particular, infrastructure associated with [...] IP addresses [the Supplemental Application].

[5] Prior to the Court's determination of the Supplemental Application, Counsel for the Attorney General of Canada [AGC] advised that on March 1, 2024, the Supreme Court of Canada [SCC] had issued its decision in *R v Bykovets*, 2024 SCC 6 [*Bykovets*]. In *Bykovets*, a 5-4 decision, the majority of the SCC held that individuals have a reasonable expectation of privacy in their IP address, that IP addresses enjoy the protection of section 8 of the *Canadian Charter of Rights and Freedoms* [*Charter*], and that the police's request to a third party for Mr. Bykovets' IP address without a warrant violated his reasonable expectation of privacy. The minority found that Mr. Bykovets did not have a reasonable expectation of privacy in the IP address.

[6] In the Supplemental Application, the AGC's initial position was that the collection of the [...] IP addresses at issue was lawful, noting that the addresses were obtained prior to the issuance of *Bykovets*. Nonetheless, the AGC offered to provide further submissions.

[7] On March 6, 2024, the Court requested that the AGC make submissions on the impact of *Bykovets* on the Supplemental Application, and advised that the Court would appoint an *amicus curiae* [*amicus*] to do the same and that a reasonable timetable would be established for written submissions and an oral hearing. The Supplemental Application was held in abeyance pending the Court's consideration of the submissions.

[8] By Order dated April 15, 2024, the Court appointed Mr. Matthew Gourlay as *amicus*. As *amicus,* Mr. Gourlay has provided insightful analysis into the scope of *Bykovets* and its impact on the existing jurisprudence in the national security context, and on the particular issues on the Supplemental Application, including the AGC's alternative arguments.

[9] The AGC filed written submissions on June 14, 2024.

[10] The *amicus* filed written submissions on July 5, 2024.

[11] The AGC filed reply submissions on July 18, 2024.

[12] The dates initially and tentatively proposed for the oral hearing (August 14-15, 2024) were not feasible and the oral hearing was rescheduled.

[13] On September 23, 2024, the Court issued a Direction noting that the impact of *Bykovets* had been raised in other proceedings before the Court and the Court anticipated that this would continue. The Court also noted that the submissions of the AGC and *amicus* may be particularly relevant in the context of another proceeding (CSIS-24-22) and proposed that Justice Gleeson,

who has carriage of CSIS-24-22, co-preside at the oral hearing in C-1-24 although C-1-24 and CSIS-24-22 would remain independent applications.

[14] The AGC provided the *amicus* and the Court with relevant decisions of provincial and superior courts regarding the impact of *Bykovets* on police practices regarding the receipt or collection of IP addresses as those decisions became available and has continued to do so.

[15] On October 15, 2024, the Court convened a hearing with both Justices Kane and Gleeson presiding, which focused on the legal issues relevant to both C-1-24 and CSIS-24-22. On October 22, 2024, the Court convened a hearing on only C-1-24 to, among other things, receive the evidence of the affiant and the submissions of counsel for the AGC and *amicus* on the Supplemental Application.

[16] On October 23, 2024, the Court granted the Supplemental Application pursuant to Condition 3 of the cyber warrant upon finding that the [...] IP addresses at issue did not attract a reasonable expectation of privacy and did not engage section 8.

[17] The [...] IP addresses at issue included addresses reasonably believed to relate to foreign nationals outside Canada without a recognized nexus and to Canadian victims of attacks by those hostile foreign actors. These IP addresses do not attract a reasonable expectation of privacy and therefore, the Service lawfully collected the addresses without a warrant pursuant to section 12 as a non-intrusive collection activity.

[18] Although the Supplemental Application was determined on this basis, the AGC urged the Court to consider their alternative arguments supporting the collection of the [...] IP addresses at issue and to provide guidance for other scenarios that may arise where the collection of the infrastructure (IP addresses) could engage a reasonable expectation of privacy. The *amicus* disagreed, arguing that the Court should determine the Supplemental Application on the facts presented and on the basis that there was no reasonable expectation of privacy, and cautioned against addressing the AGC's alternative arguments in the absence of a factual record.

[19] The Court indicated that it would consider whether to address the alternative arguments and would issue reasons at a later date. The Court's reasons follow and address the primary argument and the alternative argument with respect to the [...] IP addresses at issue.

[20] A summary of the Court's findings is set out at paragraph 223.

II. The cyber warrant

[21] The cyber warrant, at paragraph 1, authorizes the Director and any employee of the Service acting under the Director's authority to intercept any communication destined to or originating from: (a) "infrastructure associated with the following IP addresses, [_..._] and then sets out the specific IP addresses, [_..._]"; and (b) "any other infrastructure subject to a Federal Court order issued in accordance with Condition 3" [emphasis added].

[22] "Infrastructure" is defined as "any computer, electronic data storage medium, network, Internet-based account or Internet services account that was compromised, attempted to be compromised or is being used by a cyber-actor".

[23] The cyber warrant was issued initially identifying specific IP addresses and other infrastructure. The affidavit filed in support of the application for the warrant, sought pursuant to sections 12 and 21, explained why the infrastructure is believed to be associated with cyber espionage, cyber sabotage and cyber influenced activity and how the infrastructure was identified. The affiant also provided oral evidence in support of the application. The Court was satisfied that the cyber warrant was required to enable the Service to investigate, within or outside Canada, threats to the security of Canada posed by cyber espionage, cyber sabotage and cyber foreign-influenced activities.

[24] Condition 3 of the cyber warrant provides:

> Where pursuant to paragraph 1 (b), the Director General or their designate has identified infrastructure, for the purpose of executing this warrant, a supplemental application shall be brought to the Court, without delay, to seek an order to execute the warrant powers in respect of the identified infrastructure.

[25] Pursuant to Condition 3, CSIS submitted the Supplemental Application to the Court identifying additional infrastructure—more specifically, [...] IP addresses.

[26] The affidavit filed in support of the Supplemental Application describes how the infrastructure was identified and obtained by CSIS [...] ([...] IP addresses are victims of the cyber actors; [...] IP addresses are hostile foreign actors). CSIS also conducted non-warranted queries of the IP addresses using open-source tools to identify the general location and assignment of a number to the IP addresses.

[27] The affiant provided further information at the oral hearing. In a nutshell, most of the IP addresses were provided by other agencies ([...]). CSIS did not proactively seek the IP addresses. The collection of the IP addresses occurred prior to the decision in *Bykovets*.

[28] As noted above, given the broad principles enunciated in *Bykovets* regarding the reasonable expectation of privacy in an IP address, the Court sought further submissions to assess whether the passive collection of the [...] IP addresses by CSIS was lawful.

III. Overview of Positions

A. *The AGC's position*

[29] The AGC's primary position is that there was no reasonable expectation of privacy in the [...] IP addresses at issue. The AGC submits that if the Court agrees with their primary submission, concurred in by *amicus,* i.e., that to the extent that the [...] IP addresses are reasonably believed to relate to foreign nationals outside Canada without a recognized nexus or to Canadian victims of attacks by those hostile foreign actors, the IP addresses do not attract a reasonable expectation of privacy; section 8 of the *Charter* is not engaged. Therefore, CSIS lawfully collected the IP addresses pursuant to section 12 as non-intrusive collection activity and this is sufficient for the Court to grant the Supplemental Application.

[30] Alternatively, the AGC submits that section 12 of the *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 [*CSIS Act*] provided the authority to collect the IP addresses on the reasonable grounds to suspect standard because it is a minimally intrusive search. In the further alternative, the AGC submits that the IP addresses could be retained by applying the

balancing test established in the *En Banc* decision (*Canadian Security Intelligence Service Act (Re)*, 2020 FC 616 [*En Banc*]).

[31] The AGC asks the Court to address their alternative arguments, particularly the argument that IP addresses that attract a reasonable expectation of privacy can be collected (including by a direct request) by CSIS without a warrant pursuant to section 12 as a minimally intrusive form of search, because this is a recurring issue requiring resolution.

[32] The AGC also raises related issues, including whether IP addresses lawfully collected can be used or "enriched".

B. *The Amicus' position*

[33] The *amicus* agrees that the Supplemental Application can be granted on the facts as presented; no one's section 8 rights were implicated or at risk.

[34] The *amicus* submits that hostile foreign actors with no *nexus* to Canada do not have section 8 rights and do not have a reasonable expectation of privacy in their IP address.

[35] Although Canadian victims of cyber attacks by the hostile foreign actors do have section 8 rights, their voluntary provision of their IP address, or the receipt by CSIS of their IP address from others in the course of an investigation into cyber espionage does not engage the victims' section 8 rights. The *amicus* agrees that a victim of a cyber attack would likely welcome CSIS's efforts to thwart the attack.

[36] The *amicus* distinguishes the facts in the Supplemental Application noting that there was no request by CSIS for the IP addresses from other circumstances where CSIS may seek to proactively obtain an IP address, including from a Canadian internet service provider [ISP]. The *amicus* submits that in these other circumstances, *Bykovets* would apply. The *amicus* submits that such a search would be more than minimally intrusive and would require a warrant.

[37] The *amicus* submits that this Court should focus on the facts in the Supplemental Application and should not address the AGC's alternative arguments in the absence of a factual basis to do so.

[38] However, if the Court considers the AGC's alternative argument, the *amicus* disagrees that section 12 of the *CSIS Act* provides CSIS with the authority to seek an IP address. The *amicus* submits that *Bykovets* cannot be relied on as authority for the proposition that a reasonable suspicion standard is sufficient to seek an IP address and that by analogy, section 12 provides CSIS with the authority.

IV. The *Bykovets* decision and its interpretation and application to date

A. *The Supreme Court's decision*

[39] In *Bykovets*, the SCC found that the police violated Mr. Bykovets' rights by obtaining his IP address from a third-party payment processing company without judicial authorization. The SCC found that given the potential of the IP address to reveal the user's internet activity and their identity, an IP address attracts a reasonable expectation of privacy. The SCC concluded that

a request by the state for an IP address is a search under section 8 of the *Charter* and requires prior judicial authorization.

[40] The minority decision disagreed and found that Mr. Bykovets did not have a reasonable expectation of privacy and that the police did not need judicial authorization before asking the payment processor for the IP addresses in order to determine the ISP associated with them. The minority noted that their conclusion did not foreclose the possibility that someone may have a reasonable expectation of privacy on different facts.

[41] By way of background, the police were investigating fraudulent online purchases from a liquor store. The police contacted the payment processing company for online sales, obtained the IP addresses used for the purchases and then obtained a production order to compel the ISP to disclose subscriber information. The police then used the subscriber information to seek and execute search warrants.

[42] Mr. Bykovets challenged the request by police to obtain his IP addresses from the payment processing company, arguing that it violated his right against unreasonable search and seizure under section 8.

[43] The SCC noted that the IP address is the “key to unlocking” a user’s internet activity and ultimately their identity, and as such, attracts a reasonable expectation of privacy. Section 8 protects the online privacy of Canadians, and must protect their IP addresses (at para 28).

[44] At paras 60-70, the SCC explains the rationale for finding that IP addresses attract a reasonable expectation of privacy given the potential to be correlated with other online information, which may reveal a great deal of information about a user "touching directly on the intimate details of the lifestyle and personal choices of an individual", and that judicial pre-authorization to obtain the IP address is required.

[45] The SCC stated at para 60:

> The Crown suggests that an IP address is useless without a *Spencer* warrant. Respectfully, I cannot agree. First, as the link that connects specific Internet activity to a specific location, an IP address may betray deeply personal information, even before police try to link the address to the user's identity. Second, activity associated with the IP address can be correlated with other online activity associated with that address available to the state — with particularly concerning consequences when coupled with access to third-party-held information. Finally, an IP address can set the state on a trail of Internet activity that leads directly to a user's identity, even without a *Spencer* warrant. The instances when an IP address may betray biographical core information are not all captured by *Spencer*. In light of these three points, which I elaborate below, access to IP addresses without judicial pre-authorization poses intense privacy risks, and IP addresses attract a reasonable expectation of privacy.

[46] The SCC first noted that "the activity associated with the IP address can itself be deeply revealing, even before any attempt to determine identity" (at para 61) and that "[o]ther online activities can reveal information that goes directly to a user's biographical core" (at para 63).

[47] The SCC then noted that "[s]econd, the specific activity associated to the IP address by the search can be correlated with other online activity associated to that IP address" (at para 64) and explained at para 65:

> Without the protection of s. 8, nothing prevents the state from pre-emptively collecting IP addresses and comparing that user's IP address against their database. Further, and significantly, the scope of information that an IP address can reveal is enormous if correlated against information held by a third party.

[48] The SCC added, at paras 68-69, that "link by link, an IP address can set the state on a trail of anonymous Internet activity that leads directly to a user's identity", that IP addresses are "the first 'digital breadcrumbs' on the user's cybernetic trail", and that these "breadcrumbs may establish an Internet user's entire daily, weekly, or even monthly online activity, leading to an electronic roadmap of the user's cybernetic peregrinations... Like the computer in *Reeves*, an IP address provides the state with the means that can lead them to a trove of personal information" [citations omitted].

[49] The SCC summed up at para 70:

> Consequently, an IP address may betray an intensely private array of information, touching directly on the intimate details of the lifestyle and personal choices of an individual user (*Marakah*, at para. 32; *Spencer*, at para. 27).

[50] The SCC acknowledged that the privacy interests must be weighed against safety and that the police need tools to investigate online crime, noting the harm to victims, in particular, to children. Despite the acknowledgement, the SCC found that prior judicial authorization was required, noting at paras 85-86:

> [85] In my view, however, requiring that police obtain prior judicial authorization before obtaining an IP address is not an onerous investigative step, and it would not unduly interfere with law enforcement's ability to deal with this crime. Where the IP address, or the subscriber information, is sufficiently linked to the commission of a crime, judicial authorization is readily available and adds little to the information police must already provide for

> a *Spencer* production order. For example, under s. 487.015(1) of the *Criminal Code*, R.S.C. 1985, c. C-46, a production order for information relating to a specified transmission of a communication is available if there are reasonable grounds to *suspect* that an offence has been or will be committed. Police often apply for and obtain multiple authorizations to protect different territorial privacy interests. The same is true to protect informational privacy.
>
> [86] On balance, the burden imposed on the state by recognizing a reasonable expectation of privacy in IP addresses pales compared to the substantial privacy concerns implicated in this case. Law enforcement will need to demonstrate enough grounds to intrude on an individual's privacy but, in the age of telewarrants and around-the-clock access to justices of the peace, this burden is not onerous. Police engaging in legitimate investigatory activities can readily establish the requisite constitutional grounds. Recognizing that an IP address attracts s. 8 protection will not thwart police investigations involving IP addresses; rather, it aims to make sure police investigations better reflect what each reasonable Canadian expects from a privacy perspective *and* from a crime control perspective.

[51] The SCC summarized their rationale at para 90:

> [90] Thus, viewed normatively, s. 8 of the Charter ought to extend a reasonable expectation of privacy to IP addresses. They provide the state with the means through which to obtain information of a deeply personal nature about a specific Internet user and, ultimately, their identity whether or not another warrant is required. An IP address plays an integral role in maintaining privacy on the Internet. It is the key to unlocking an Internet user's online activity and the key to identifying the user behind online activity. Given these serious privacy concerns, the public's interest in being left alone should prevail over the relatively straightforward burden imposed on law enforcement. Recognizing a reasonable expectation of privacy in IP addresses would ensure that the veil of privacy all Canadians expect when they access the Internet is <u>only lifted when an independent judicial officer is satisfied that providing this information to the state will serve a legitimate law enforcement purpose.</u>
>
> [emphasis added].

[52] In concluding, the SCC reiterated that "the request by the state for an IP address is a search under s.8 of the *Charter*" (at para 92 [emphasis added]).

B. *The key findings in Bykovets*

- Section 8 protects the online privacy of Canadians, and must protect their IP addresses.

- An IP address is the crucial link between an internet user and their online activity (at para 28). Given the potential of the IP address to reveal the user's internet activity and their identity, an IP address attracts a reasonable expectation of privacy. A request by the state for an IP address is a search under section 8 of the *Charter*.

- A search occurs where the state invades a reasonable expectation of privacy. An expectation of privacy is reasonable where the public's interest in being left alone by the government outweighs the government's interest in intruding on the individual's privacy to advance its goals, notably those of law enforcement. Competing factors inform the determination of a reasonable expectation of privacy: (1) the subject matter of the search; (2) the claimant's interest in the subject matter; (3) the claimant's subjective expectation of privacy; and (4) whether the subjective expectation of privacy was objectively reasonable (at para 31).

- Whether a subjective expectation of privacy is objectively reasonable is determined taking into account the totality of the circumstances (at paras 44-45).

- Defining a reasonable expectation of privacy is an exercise in balance. On the facts in *Bykovets*, the balance weighed in favour of extending a reasonable expectation of privacy to IP addresses. The intensely private nature of the information an IP address may betray strongly suggests that the public's interest in being left alone should prevail over the government's interest in advancing its law enforcement goals (at paras 71-72).

- Although the police need investigative tools to address online crime, prior judicial authorization is required to seek an IP address and seeking such authorization would not be onerous (at paras 84-85). The SCC noted the availability of production orders pursuant to subsection 487.015(1). The SCC also noted that "[l]aw enforcement will need to demonstrate enough grounds to intrude on an individual's privacy but, in the age of telewarrants and around-the-clock access to justices of the peace, this burden is not onerous" (at para 86 [emphasis added]).

C. *The interpretation and application of Bykovets by provincial and superior courts (criminal context)*

[53] As noted above, the AGC submitted case law interpreting and applying or distinguishing *Bykovets.* A brief summary of this and more recent jurisprudence of which the Court is aware is described below.

[54] In *R v Leger*, 2024 NBKB 72 (CanLII) [*Leger*], the New Brunswick Court of King's Bench found that the Royal Canadian Mounted Police's [RCMP] receipt of the accused's IP

address from the United Kingdom National Crime Agency [UK NCA] did not engage the section 8 rights of the accused; there was no state action and no search.

[55] The court observed at para 44 that the focus of the SCC's decision in *Bykovets* "is on the actions of the police authority in seeking out the information rather than receiving the information unprompted", unlike the facts before the court. The court concluded at para 45:

> [45] The facts of this case do not engage section 8 of the *Charter*, or the principles set out in *R v Bykovets*, The RCMP did not take investigative steps or seek out information to identify the IP address ultimately linked to Leger. Rather the UK NCA provided the RCMP a username, TOX ID, and IP address located in Canada used for sharing and discussing child exploitation material on a particular date. There was no search conducted by the RCMP to obtain Leger's IP address.

[56] In *R v Prys*, 2024 ABCJ 166, the Alberta Court of Justice found that section 8 does not apply to the mandated reporting of child sexual abuse activity in a foreign jurisdiction. The IP address was voluntarily provided by Dropbox, a United States [US] organization.

[57] The court concluded that the production order and search warrant were both lawfully granted, explaining at para 12:

> [12] From all of the above, I find that s 8 of the Charter has no application to the mandated reporting of detected instances of online child sexual abuse activity in a foreign jurisdiction, including the voluntary reporting of IP addresses associated with such activity. When NCMEC forwards an IP address to police in Canada without a request by law enforcement, this is simply a means of reporting a crime so that police may then obtain the appropriate judicial authorizations to investigate suspected child sexual exploitation in their jurisdiction. As per the Alberta Court of Appeal in R v King, 2021 ABCA 271, I find that when information is provided to the police by a third party without an active request,

> the police are entitled to receive and review it, and there is no search or seizure by the state which engages s 8 of the Charter.

[58] In *R v Pengelly*, 2024 SKKB 192 [*Pengelly*], the Saskatchewan Court of King's Bench found that the voluntary provision of the IP address by the National Center for Missing and Exploited Children [NCMEC] (a private US organization) to the police is not a search by a state actor in Canada and does not engage section 8. The court explained at para 57 that NCMEC's voluntary assistance in detecting child pornography does not engage the *Charter*; the receipt by the police of a complaint from NCMEC and the use of a public search engine to geo-locate and identify the Communication Service Provider [CSP] did not engage Mr. Pengelly's reasonable expectation of privacy. Therefore, the initial investigatory steps taken by the police, including asking the ISP whether it had subscriber information (i.e., not asking it to provide that information) did not require prior judicial authorization nor did this result in a breach of the accused's right to be free from unreasonable search and seizure (at paras 58-60).

[59] In *R v Cofell*, 2024 ONSC 7151 [*Cofell*], the Ontario Superior Court of Justice found that the provision of the IP address by the Child Protection System [CPS], a US organization, to the police does not constitute state action, is not a search and does not engage section 8 (at para 149). Alternatively, if the use of the CPS information had constituted state action, the court found that the accused did not have a reasonable expectation of privacy based on an analysis of the totality of the circumstances, including that he was involved in file sharing and his IP address was publicly available (at para 176).

[60] Other decisions of superior and provincial courts have also found that the passive receipt of an IP address by the police does not engage section 8.

[61] In *R v Hillier*, 2024 NLSC 161, the Supreme Court of Newfoundland and Labrador found that the accused's IP address was never requested by Canadian authorities but voluntarily provided by NCMEC to Canada's National Child Exploitation Crime Centre and therefore involved no direct state action against the accused's right to privacy under section 8 (at paras 68-71, 75). The court further noted that the *Charter* has no extraterritorial jurisdiction or application over the actions of foreign regulatory agencies, including how and what evidence they gather (at paras 68, 71).

[62] In *R v Munro*, 2025 SKKB 20, the Saskatchewan Court of King's Bench found that section 8 of the *Charter* was not engaged when the accused's IP address was obtained by private actors (CPS) and voluntarily shared with law enforcement; there was no request made by law enforcement, and therefore no search (at paras 44-45).

[63] In *R v Tate*, 2025 BCSC 1462 [*Tate*], the Supreme Court of British Columbia found that section 8 was not engaged when police obtained the IP address of an accused that was publicly available online, as there was no reasonable expectation of privacy in that IP address. As such, there was no search or seizure when the police obtained that information from the CPS or used it as the foundation for their investigation (at para 130).

[64] In *R v Brazeau*, 2024 ONCJ 611 [*Brazeau*] and *R v Done*, 2025 ONCJ 326 [*Done*], the Ontario Court of Justice found that the passive receipt by police of the accused's IP address details was not a search and did not engage the constitutional protection of section 8, and therefore the police were not required to seek judicial authorization to passively receive such information nor after the fact (*Brazeau* at paras 18-23; *Done* at paras 38-43). The same was

found by the Provincial Court of British Columbia in *R v Cagoco* (BCPC, Courtenay, No 44265-1, November 1, 2024 [unreported], cited in *Cofell* at paras 115-116).

[65] There are a few superior and provincial court decisions that have taken a different approach (*R v Asantarajah*, 2025 ONSC 1377; *R v Daniels*, 2025 ONSC 344; *R v Currie*, 2024 BCPC 175), but these have been distinguished or rejected in the above-noted jurisprudence (see *Tate* at paras 93-94, 123-129; *Done* at paras 81-82; *Cofell* at para 152).

[66] All of the cases to date, of which the Court is aware, that have interpreted, applied, or distinguished *Bykovets* have addressed the role of the police in criminal investigations, primarily in the context of the prosecution of child pornography offences. In *Bykovets*, the SCC noted the need to balance privacy interests against "the legitimate interest in the need for safety and security" (at para 84) and acknowledged the seriousness of online child pornography, yet still found that prior judicial authorization was required, but that seeking such authorization would not be onerous. The lower courts, applying or distinguishing *Bykovets*, have focused on the manner in which the IP addresses were obtained by the police, including where the IP addresses originated, and whether, in the particular circumstances, there was a reasonable expectation of privacy in the first place. The courts have found that law enforcement agencies passively receiving IP addresses from foreign agencies and non-state actors do not engage section 8 rights; this is not state action.

[67] In *Leger* and *Pengelly*, the practice of relying on open-source tools to enrich an IP address provided to law enforcement was accepted (*Leger* at paras 51-55; *Pengelly* at para 58).

In *Tate*, the court also found that neither the receipt nor use of the IP address amounted to a search (at para 130).

V. The AGC's position

[68] The AGC acknowledges that the specific issue on the Supplemental Application is whether CSIS lawfully collected the [...] IP addresses. The AGC submits that the collection was lawful.

[69] The AGC emphasizes that the SCC did not consider whether IP addresses of section 8 rights holders attract a reasonable expectation of privacy outside of the specific factual context in *Bykovets*, where a Canadian police service requested the IP address from a Canadian third-party provider. The AGC notes that the factual context in *Bykovets* differs from the factual context underlying the Supplemental Application and from other contexts where CSIS collects IP addresses.

[70] The AGC advances three arguments and asks that the Court consider all.

[71] The AGC's primary position is that the passive receipt by CSIS of the [...] IP addresses does not engage section 8 of the *Charter*.

[72] The *amicus* agrees with this primary position, as does the Court, and the Supplemental Application was granted on this basis. The submissions of the AGC and *amicus* are nonetheless included in the Court's reasons, for completeness.

A. *No reasonable expectation of privacy; section 8 is not engaged*

[73] The AGC explains that the collection of the [...] IP addresses does not engage section 8.

[74] With respect to the [...] IP addresses associated with hostile foreign actors outside of Canada with no *nexus* to Canada, no reasonable expectation of privacy exists. These foreign nationals do not have section 8 rights and cannot assert privacy interests in those IP addresses. These IP address holders do not come within the scope of "everyone" under section 8 (*Canadian Security Intelligence Service Act (CA) (Re)*, 2022 FC 1444 at para 170 [*Outside Canada*]). The AGC submits that the Service's collection of these IP addresses can occur pursuant to section 12 without a warrant as non-intrusive collection activity.

[75] With respect to the [...] IP addresses of Canadian victims of cyber attacks by the foreign actors, the AGC submits that these IP addresses also do not engage a reasonable expectation of privacy. Although Canadian victims are section 8 rights holders, the totality of the circumstances supports the view that these victims would either not subjectively expect that their IP addresses would be kept from the Service where this information is being collected for the non-adversarial purpose, or, alternatively, that any subjective expectation of privacy would not be objectively reasonable given that the Service is collecting the IP addresses to alert victims and/or to investigate the threat-related activity.

[76] The IP addresses collected from foreign and domestic agencies arise from interagency information sharing. The AGC submits that where the foreign or domestic agency [...] lawfully collects information, including IP addresses, in carrying out its own duties or national

security mandate, the passive receipt of this information by CSIS does not interfere with a reasonable expectation of privacy.

[77] The AGC submits more generally that for (any) IP addresses collected independently by domestic or foreign agencies, which are then disclosed to the Service as part of interagency information sharing (i.e., passive receipt), the Service's receipt and use of those IP addresses, even if they involve a section 8 rights holder, *does not engage section 8 of the Charter*. The AGC submits that the Service can collect and use this information without a warrant pursuant to section 12 as non-intrusive collection activity. The AGC explains that where there is no reasonable expectation of privacy at the point of collection or sharing, the information does not later acquire a reasonable expectation of privacy when Canadian authorities receive or use the information.

[78] The AGC also points to the post-*Bykovets* decisions, where lower courts found that where a section 8 rights holder's IP address is collected by a foreign agency and then shared with Canadian law enforcement authorities, section 8 is not engaged; there is no search.

B. *The section 12 alternative argument should be addressed*

[79] Although the *amicus* agrees with the AGC's primary position, as does the Court, and the Supplemental Application has been granted on the basis that the users of the [...] IP addresses do not have a reasonable expectation of privacy, the AGC submits that their alternative argument relying on section 12 should be addressed for several reasons, including:

- CSIS's non-warranted collection of IP addresses has and will arise in other

supplemental applications and in other contexts;

- As a matter of "judicial economy and efficiency" the Court should adjudicate the issue with the benefit of this record; and,
- The Court's guidance on CSIS's ability to collect IP addresses without a warrant will resolve the legal uncertainty post-*Bykovets*.

(1) Section 12 provides the authority for minimally intrusive collection activity for the [...] IP addresses at issue and for other IP addresses (passive receipt and direct requests)

[80] The AGC submits that if the Service's collection of the [...] IP addresses does attract a reasonable expectation of privacy and amounts to a search in light of *Bykovets*, the Service can collect these IP addresses without a warrant pursuant to section 12, based on the reasonable grounds to suspect standard as a minimally intrusive collection activity. The AGC notes that this Court has held that section 12 of *CSIS Act* provides CSIS with reasonable lawful authority to conduct searches of a minimally intrusive nature (*X (Re)*, 2017 FC 1047 [*IMSI*]).

[81] The AGC adds that if the Service wants to collect an IP address by way of a **request** to a third-party provider, as in *Bykovets*, the Service could also rely on section 12 as a minimally intrusive form of search. The AGC acknowledges that this does not arise on the facts of the Supplemental Application, but submits that their submission should be addressed.

(a) *The reasonable grounds to suspect standard is intended for searches that are minimally intrusive of privacy interests*

[82] The AGC argues that it is implicit in the *Bykovets* majority reasons that any reasonable expectation of privacy that attaches to an IP address is not a heightened privacy interest, given

that the court found that the police could obtain this information on the reasonable grounds to suspect standard, relying on a *Criminal Code*, RSC 1985, c C-46 [*Criminal Code*] production order (as opposed to the reasonable grounds to believe standard). The AGC notes that section 487.015 of the *Criminal Code* provides for a production order for transmission data if there are reasonable grounds to suspect that an offence has been or will be committed and the IP address is linked to the commission of the crime.

[83] The AGC notes that the lesser threshold of reasonable grounds to suspect is intended for searches that are minimally intrusive of privacy interests (*Mahjoub v Canada (Citizenship and Immigration)*, 2017 FCA 157 at para 177 [*Mahjoub FCA*]; *IMSI* at paras 218-219).

[84] The AGC also points to *R v Kang- Brown*, 2008 SCC 18 at paras 234-242 [*Kang-Brown*], where the SCC found that a search by sniffer dogs was a minimally intrusive search and did not require that the police obtain a warrant. The SCC noted that the search did not interfere with bodily integrity, was not unduly inconvenient, was narrowly targeted and highly accurate and that the only personal information sought was the presence or absence of contraband; i.e., the search was minimally intrusive. The AGC notes that the same criteria were considered in *IMSI*, *Outside Canada*, and *Canadian Security Intelligence Service Act (Re)*, 2020 FC 697 [*Preferred Networks*].

(b) *Section 12 authorizes minimally intrusive searches*

[85] The AGC points to *Outside Canada* where the Chief Justice noted that section 12 authorizes CSIS to pursue activities that are minimally intrusive of section 8 privacy interests (at para 176).

[86] The AGC also points to *IMSI*, where the Chief Justice noted that in the national security context, the public would likely accept some reduction in their privacy rights to enable CSIS to investigate activities suspected to constitute threats to the security of Canada (at para 171).

[87] The AGC notes that in *IMSI*, the Chief Justice relied on the considerations that distinguish a minimally intrusive search from an intrusive search, i.e., the search is highly accurate and narrowly targeted; personal or third-party information incidentally captured is not used and is destroyed; and, the technology is highly reliable (at paras 209, 226, 246, 249, 252-253).

[88] The AGC submits that if the [...] IP addresses at issue—or other IP addresses collected pursuant to a supplemental application—interfere at all with a reasonable expectation of privacy, these are at most, minimally intrusive of privacy interests. The method of collection is highly accurate and narrowly targeted, it does not incidentally capture third-party information, and the information collected is highly reliable.

[89] The AGC also submits that the same rationale supports CSIS's reliance on section 12 to request IP addresses.

[90] The AGC agrees that CSIS cannot task foreign agencies to collect, without a warrant, information that CSIS would require a warrant to collect directly. The affiant confirmed that this was not done with respect to the [...] IP addresses and is not done.

[91] The AGC acknowledges that section 12 only permits CSIS to engage in minimally intrusive activities. Anything more than minimally intrusive of a section 8 right would require a warrant. The AGC noted that where CSIS obtains an IP address, it would seek a section 21 warrant to obtain other information from a CSP.

(c) *Criminal Code production orders provide an analogy; IP addresses that interfere with a REP can be collected by police by way of a production order for transmission data, on reasonable grounds to suspect*

[92] The AGC submits that the threshold in section 12 "activities that may on reasonable grounds be suspected of constituting threats to the security of Canada" is analogous to the threshold for a production order for transmission data pursuant to section 487.015 in the *Criminal Code* of "reasonable grounds to suspect".

[93] The AGC emphasizes that *Bykovets* addressed only whether the police required a warrant to request the IP address from a third party. The court found that the police could have obtained the accused's IP address—despite finding that the IP address attracts a reasonable expectation of privacy and requires prior judicial authorization—by way of a *Criminal Code* production order for transmission data for a specified communication under section 487.015.

[94] The AGC submits that although *Bykovets* characterizes the IP address as the "first digital breadcrumb" that when combined with other information can tell you more about the user, even on the facts of *Bykovets*, the SCC indicated that the reasonable grounds to suspect threshold would provide the lawful authority for the police to acquire that information. If the police can obtain a production order pursuant to section 487.015 of the *Criminal Code* for an IP address on reasonable grounds to suspect, this signals a minimally intrusive search.

[95] The AGC argues that para 85 of *Bykovets* is a clear indication to the police that if they wanted to acquire Mr. Bykovets' IP addresses from the third-party payment processor, they should have sought a production order for transmission data on the reasonable grounds to suspect threshold, which is intended for searches that are minimally intrusive. Only searches that are more than minimally intrusive require prior judicial authorization according to the reasonable grounds to believe threshold.

[96] The AGC submits that passages in *Bykovets* relied on by the *amicus* to argue that the privacy interest in the IP address is heightened and that prior judicial authorization according to the reasonable grounds to believe standard would be required are *obiter*. The AGC submits that isolated passages that do not support what was decided in *Bykovets* do not establish legal principles.

[97] The AGC submits that the *amicus*' reliance on paras 60-70 of *Bykovets* cannot be isolated from para 85 and should not be interpreted as establishing that the collection of IP addresses of section 8 rights holders is more than minimally intrusive and, therefore, requires prior judicial authorization according to the reasonable grounds to believe standard; this cannot be reconciled with para 85, which accepts that a warrant could be sought on the reasonable grounds to suspect standard.

[98] The AGC notes that in *R v Otto*, 2019 ONSC 2473 at paras 56, 76-77 [*Otto*], the *Criminal Code* data transmission provisions, which require reasonable grounds to suspect, were found to comply with section 8. In *Otto*, the court concluded that the transmission data obtained is a minimal intrusion on privacy and that the reasonable suspicion standard provides sufficient

constitutional protection. The court also clarified that the transmission data obtained pursuant to the warrant cannot be used to obtain the contents of the communication, as that would attract a high degree of privacy and call for the reasonable grounds to believe standard. The AGC disputes the *amicus*' submission that *Bykovets* casts doubt on the finding in *Otto.*

[99] The AGC argues that if the police can obtain a *Criminal Code* production order on the reasonable grounds to suspect standard and obtain transmission data (a minimally intrusive search), then CSIS should be able to collect this same type of information pursuant to section 12 as minimally intrusive collection in the national security context. The AGC notes that in the law enforcement context, the police will require a warrant, but need only meet the standard of reasonable suspicion, which is the standard for warrantless collection pursuant to section 12 (where all other criteria are also met). CSIS should be able to collect this same type of information pursuant to section 12 on the same standard in the national security context; no higher standard should be imposed in the national security context (*Mahjoub FCA* at paras 265-267).

C. *The post-acquisition use of IP addresses*

[100] The AGC notes that *Bykovets* does not address the issue of post-collection use (also referred to as enrichment) or exploitation of an IP address.

[101] The AGC notes that the CSIS affiant explained that CSIS uses tools to enrich the IP address collection (whether warranted or non warranted). These are open-source and publicly available tools, which generally provide geolocation information and the CSP. The AGC submits that enrichment via publicly available open-source tools is non-intrusive collection. The CSIS

affiant clarified that in the cyber context, CSIS does not collect personal information associated with an IP address, unless it is publicly available. Otherwise, a warrant is sought.

[102] The AGC notes that in *Leger*, the court accepted that the police use such tools and did not find that the RCMP's use of the IP address—which relied on open-source information and used the information to obtain a production order and search warrant—engaged section 8.

[103] The AGC submits that where IP addresses of section 8 rights holders have been collected independently by foreign agencies and then provided to CSIS as part of interagency information sharing, or otherwise lawfully collected, section 8 is not engaged when CSIS receives or when CSIS uses that information. Given that section 8 is not engaged by the receipt of information by CSIS, then it is also not engaged by the subsequent use by CSIS of that information. The information does not acquire a reasonable expectation of privacy after the point of collection. The AGC submits that CSIS can conduct open-source inquiries using these IP addresses to determine their general geographic location and CSP.

[104] The AGC further submits that if CSIS has any lawful collection of IP addresses, whether non-warranted or warranted, it does—and is lawfully entitled to— "run this information through its own holdings".

D. *Balancing test; reliance on the approach described in En Banc*

[105] The AGC further alternatively submits that if any of the [...] IP addresses were collected in breach of section 8 and the Court also finds that section 12 is not sufficient authority, the Court retains the discretion to permit the Service to collect the IP addresses by applying the

three-part balancing test crafted in the *En Banc* decision. The AGC notes that the further alternative argument is a "fall back" position.

[106] The AGC submits that the same factors, as adapted to the context, would guide the Court in exercising this discretion, including the seriousness of the unlawful activity; fairness (e.g., the impact on an individual's legal rights or interests and whether the unlawful activity undermines the credibility or reliability of the information); and, societal interests, including the nature and severity of the threat to the security of Canada.

[107] The AGC submits that any unlawfulness associated with CSIS's collection of the [...] IP addresses is minor given that CSIS received the information passively and there was no pattern of illegal conduct. All of the IP addresses at issue were collected prior to the SCC's decision in *Bykovets*, and at that time, IP addresses were not viewed as information subject to the protection under section 8.

[108] With respect to fairness, any unlawfulness associated with the collection of the [...] IP addresses does not undermine the credibility or reliability of that information. In addition, there is a societal interest in CSIS's capacity to investigate threats to the security of Canada and in the circumstances of the Supplemental Application there was evidence of an immediate threat to the security of Canada posed by the cyber espionage and sabotage activities. The AGC submits that the immediacy and severity of that threat are extenuating circumstances supporting the admissibility of the IP addresses notwithstanding any illegality in the collection.

VI. The *amicus*' position

A. *The Supplemental Application can be granted; there is no reasonable expectation of privacy*

[109] The *amicus* agrees that the Supplemental Application can be granted on the basis that the [...] IP addresses at issue do not engage any reasonable expectation of privacy. The *amicus* notes, however, that other circumstances may raise different considerations.

[110] The *amicus* agrees that a foreign entity with no *nexus* to Canada does not have section 8 rights. The *amicus* submits that the AGC (and CSIS) must establish the lack of *nexus* to permit a warrantless collection of IP addresses. In this Supplemental Application the AGC's affiant did so, explaining that [...] IP addresses collected were used by foreign hostile actors with no *nexus* to Canada and no section 8 rights, and the other [...] IP addresses were victims of cyber attacks.

[111] The *amicus* submits that where it is not certain whether a section 8 rights holder is involved, to ensure against unreasonable searches, CSIS should rely on other legal authority to acquire the IP address—i.e., interagency intelligence sharing, possibly section 12 collection, or a section 21 warrant.

[112] With respect to Canadian victims, the *amicus* submits that it should be assumed that a reasonable expectation of privacy exists in their IP address. However, foreign or domestic interagency intelligence sharing may provide the legal authority for CSIS to acquire a Canadian victim's IP address, and did so with respect to the IP addresses at issue.

B. *CSIS can collect IP addresses from foreign and domestic intelligence agencies pursuant to interagency sharing without a warrant*

[113] The *amicus* agrees that the passive receipt of intelligence from foreign agencies via interagency cooperation does not generally engage the *Charter*.

[114] The *amicus* also agrees that the [...] IP addresses provided [...] to CSIS constitute a lawful warrantless collection. The evidence shows that these IP addresses were associated with infrastructure compromised by foreign actors.

[115] The *amicus* further agrees, more generally, that CSIS may receive IP addresses [...] and can assume [...] has lawfully collected the IP addresses as part of its mandate.

[116] The *amicus* submits, however, that as with IP addresses provided by foreign agencies, the further exploitation by CSIS of this information (e.g., via public search engines or otherwise) in the context of an investigation of a person (i.e., a target) in Canada may give rise to a reasonable expectation of privacy.

C. *The impact of Bykovets*

[117] The *amicus* and AGC agree about the key finding on the facts in *Bykovets*, but disagree about the scope of its application, including whether the SCC views the request for an IP address as a minimal intrusion on a reasonable expectation of privacy, and about the threshold for the authorization to obtain the IP address.

[118] The *amicus* notes that the majority in *Bykovets* links the privacy interest inherent in an IP address to it being the "first digital breadcrumb" that leads to other information and may ultimately reveal highly personal information about the user. The *amicus* submits that the privacy interest exists in that first breadcrumb.

D. *Section 12 is not sufficient authority to seek an IP address*

[119] The *amicus* submits that the Court should focus only on the [...] IP addresses at issue and should not address the AGC's alternative arguments.

[120] However, if the Court does so, the *amicus* does not agree that section 12 permits CSIS to request an IP address.

(1) Collection of an IP address is not always a minimally intrusive search

[121] The *amicus* disputes the AGC's argument that *Bykovets* supports the position that seeking an IP address is a minimally intrusive search, that reasonable grounds to suspect that the information is about activities constituting threats to the security of Canada is sufficient, and that section 12 provides authority to CSIS for warrantless collection.

[122] The *amicus* submits that *Bykovets* does not support the conclusion that the collection of a target's IP address is always minimally intrusive and would fall within section 12.

[123] The *amicus* submits that holders of IP addresses do not have a lesser degree of privacy protection in the national security context than targets of criminal investigations.

[124] The *amicus* emphasizes that post-*Bykovets*, the IP address, once viewed as only a string of numbers, must now be viewed from the perspective of what it has the potential to reveal. Therefore, once the collection of the IP address moves beyond minimally intrusive (and narrowly targeted and highly accurate) a warrant is required.

[125] The *amicus* acknowledges that the IP address on its own remains just a string of numbers and does not include any private information; however, a warrant may be required when the "digital breadcrumbs" of the IP address have the potential to reveal intimate details close to the biographical core of the target's privacy interests.

[126] The *amicus* agrees that in the cyber warrant context, the prospect of a focused investigation into any particular person (i.e., a "target"), much less a section 8 rights holder, is remote. However, in circumstances, for example, where the target of a CSIS investigation has a *nexus* to Canada and has section 8 rights, the target would have a reasonable expectation of privacy in their IP address (per *Bykovets*). The *amicus* submits that the collection of the target's IP address would be more than minimally intrusive.

[127] The *amicus* also posits a scenario where CSIS requests a third-party payment processor for an IP address associated with online purchases that suggest a national security threat. If the IP address is obtained, CSIS could then use other investigative techniques to develop an account of the target's online existence, all without a warrant. The *amicus* submits that in such a scenario, the intrusion is more than minimal; section 12 is not enough and a warrant is required.

[128] The *amicus* submits that a direct request by CSIS for an IP address should require prior judicial authorization; such a search cannot be assumed to be minimally intrusive.

(2) A *Criminal Code* production order is not analogous

[129] The *amicus* submits that *Bykovets* does not establish that reasonable grounds to suspect is the threshold to obtain an IP address. Although the majority in *Bykovets* noted, at para 85, that obtaining judicial pre-authorization would be relatively easy and that a telewarrant for a production order for transmission data could be sought on the reasonable suspicion standard, the *amicus* submits that this is cited only as an example and is only applicable to the facts in *Bykovets.*

[130] The *amicus* reiterates that where CSIS requests an IP address of a Canadian target of investigation from an ISP or third party, that target has a reasonable expectation of privacy. The *amicus* submits that the example of a production order cited in *Bykovets* does not resolve whether the threshold to seek an IP address is reasonable grounds to believe or reasonable grounds to suspect nor does it resolve the level of suspicion necessary to overcome a reasonable grounds to suspect threshold.

[131] The *amicus* submits that the SCC's rationale in *Bykovets* for finding that the reasonable expectation of privacy must be protected stems from the intensely personal information that can be disclosed by first obtaining an IP address. The *amicus* argues that this cannot be reconciled with the AGC's argument that it is not more than minimally intrusive for the state to seek an IP address. The *amicus* submits that paras 60-70 and other passages highlighting the privacy interest in an IP address cannot be downplayed; the SCC means what it says.

[132] The *amicus* submits that the circumstances in *Bykovets* did not require the SCC to determine the type of judicial authorization that may or may not be sufficient to overcome a reasonable expectation of privacy interest in an IP address because no judicial authorization had been sought at all. The *amicus* therefore regards the reference at para 85 to the ease of obtaining a production order, relied on by the AGC, as *obiter* and not part of the SCC's decision on the facts. The *amicus* agrees, however, that this is "worthy of careful consideration".

E. *The post – acquisition use of IP addresses*

[133] The *amicus* submits that the use of open-source technology to enrich IP addresses is only permissible where an IP address does not have a reasonable expectation of privacy or where an IP address with a reasonable expectation of privacy is lawfully obtained in the first place. The [...] IP addresses at issue in the Supplemental Application did not enjoy a reasonable expectation of privacy and were lawfully collected. The subsequent enrichment of the [...] IP addresses does not engage a reasonable expectation of privacy as none existed in the first place.

[134] The *amicus* explains that in his submissions in CSIS-24-22 before Justice Gleeson, he took the position that the exploitation of the device at issue required a warrant. The *amicus* notes the distinction between a device and a bare IP address.

[135] The *amicus* notes that in the CSIS-24-22 matter, he accepted that passive receipt of intelligence through interagency cooperation does not engage the *Charter*. However, the *amicus* argued that the exploitation by CSIS of that information in the context of a domestic investigation of a person in Canada may engage section 8 if there is a residual expectation of privacy in the material "depending on the context".

[136] In the Supplemental Application, the *amicus* states, "an IP address is obviously very different from an electronic device…, it does not itself contain anything private. Therefore, the acquisition/exploitation dichotomy articulated by *amicus* in [the matter in CSIS-24-22] does not apply in this context."

[137] The *amicus* acknowledges that an IP address remains a "string of numbers" (unlike a device that could be further exploited) but again notes that, while the numbers do not contain private information, the numbers have the potential to be correlated with other internet activity and lead to other information, hence the finding that an IP address has a reasonable expectation of privacy. The *amicus* points to para 65 of *Bykovets*, which conveys that the availability of open-source tools and other databases factored into the courts' finding that there is a reasonable expectation of privacy in the first digital breadcrumb—i.e., the IP address.

[138] The *amicus* also acknowledges, in his written submissions, that it would not make sense for police to require a warrant to exploit the IP addresses already lawfully acquired. In accordance with *Bykovets*, the "knock-on privacy implications of the state acquiring the IP address are already accounted for in the privacy analysis of the acquisition itself."

[139] The Court understands the *amicus*' position to be that if there is no reasonable expectation of privacy in the IP address or the IP address is passively received and/or otherwise lawfully obtained, the IP address can then be enriched via public open-source tools as long as that enrichment does not yield personal information. The *amicus* notes that CSIS would require a warrant to conduct any intrusive methods against a target with section 8 rights after acquiring that target's IP address.

VII. The CSIS Act; Relevant provisions

[140] Section 12 states:

> 12 (1) The Service shall collect, by investigation or otherwise, to the extent that is strictly necessary, and analyze and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.
>
> (2) For greater certainty, the Service may perform its duties and functions under subsection (1) within or outside Canada.
>
> [emphasis added].

[141] Subsection 21(1) states:

> 21 (1) If the Director or any employee designated by the Director for the purpose believes, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate, within or outside Canada, a threat to the security of Canada or to perform its duties and functions under section 16, the Director or employee, may, after having obtained the Minister's approval, make an application in accordance with subsection (2) to a judge for a warrant under this section.

[142] Other subsections set out the requirements for the application and of what the judge must be satisfied. Subsection 21(2) sets out the matters that must be addressed in the application for the warrant, including the facts relied on to justify the reasonable grounds to believe, any other investigative procedures that have been tried and were not successful or that would not be feasible, or, where applicable, that without a warrant it is likely that important information with respect to the threat to the security of Canada or the performance of CSIS's duties and functions under section 16 would not be obtained. Subsection 21(3) sets out what the judge must be

satisfied of in order to grant the warrant (which may include terms and conditions "advisable in the public interest" (paragraph 21(4)(f)).

VIII. *Criminal Code* production orders – sections 487.014, 487.0141, 487.015, and 492.2

[143] The police are governed by the provisions in the *Criminal Code*, which provide for warrants to obtain information, documents or things. In the investigation of online or cyber crime, the police have several specific options to seek judicial authority, depending on the circumstances. Some examples are described below.

[144] Section 487.013 provides that a justice or judge, on an *ex parte* basis, may order a person to preserve computer data in their possession where there are reasonable grounds to suspect that an offence has or will be committed and the data will assist in the investigation of the offence.

[145] Section 487.014 provides that a justice or judge, on an *ex parte* basis, may order a person to produce a document containing data that is in their possession where there are reasonable grounds to believe that an offence has or will be committed and the document or data will provide evidence respecting the commission of the offence.

[146] Section 487.015 provides that for the purpose of identifying a device or a person involved in the transmission of a communication, a justice or judge, on an *ex parte* basis, may order a person to prepare and produce a document containing transmission data related to that purpose, where the justice or judge is satisfied that: there are reasonable grounds to suspect that an offence has or will be committed; the identification of a device or person involved in the transmission of a communication will assist in the investigation of the offence; and transmission data that is in

the possession or control of one or more persons whose identity is unknown when the application is made will enable that identification. (As noted, in *Bykovets*, the SCC pointed to section 487.015, the production order for transmission data, as an option for the police to seek judicial authority to request an IP address.)

[147] Section 487.016 provides that a justice or judge may order, on an *ex parte* basis, a person to prepare and produce a document containing transmission data that is in their possession or control, where satisfied that there are reasonable grounds to suspect that an offence has or will be committed and the transmission data will assist in the investigation of the offence.

[148] Section 487.017 provides for a production order for tracking data, also on the reasonable grounds to suspect standard.

[149] Section 492.2 provides that a justice or judge who is satisfied that there are reasonable grounds to suspect that an offence has or will be committed and that transmission data will assist in the investigation may issue a warrant authorizing a peace officer or public officer (police) to obtain the transmission data by means of a transmission data recorder.

[150] With the exception of a warrant for the production of a document containing data, reasonable grounds to suspect that an offence has or will be committed is the threshold for the police to meet to obtain various warrants, including a warrant to identify a device.

IX. Analysis

[151] The AGC submits that the key issue is whether CSIS's collection of the [...] IP addresses was authorized by section 12 as non-intrusive or minimally intrusive or whether the collection of this information is more than minimally intrusive and if so, that warranted authority pursuant to section 21 was required for this to be lawful and compliant with section 8 of the *Charter*. As found, the [...] IP addresses were lawfully collected as non-intrusive collection because there was no reasonable expectation of privacy in those particular addresses; there was no search.

[152] The SCC decided *Bykovets* on the facts before it; the police requested an IP address from a third party without a warrant and that IP address was then used to obtain other warrants which led to charges against Mr. Bykovets. The SCC found that an IP address enjoys a reasonable expectation of privacy which must be protected against an unreasonable search and therefore, prior judicial authorization is required. Although the context in *Bykovets* differs from the Supplemental Application—including that there was no request by CSIS for the IP addresses and the CSIS mandate is to investigate threats to national security—the SCC's emphasis on the privacy interest in an IP address, given the potential to unearth more information, requires this Court to carefully consider the scope of section 12.

[153] The AGC characterizes some passages in *Bykovets* as *obiter* while the *amicus* characterizes other passages as *obiter*. In the Court's view, none of the passages can be ignored, even where difficult to reconcile. The SCC's guidance can be adapted to the CSIS context, which requires CSIS to investigate threats to the security of Canada, described as a critical and essential

role in "Canada's national security apparatus" (*IMSI* at para 203). The primary issue that arises on this Supplemental Application can be determined without any inconsistency with the principles in *Bykovets* because there was no reasonable expectation of privacy in the [...] IP addresses.

[154] Whether CSIS can collect IP addresses in other contexts requires consideration of the principles in *Bykovets* along with the existing jurisprudence from this Court and the Federal Court of Appeal that has considered the parameters of section 12 and the privacy implications of CSIS's reliance on new technology.

[155] In *Bykovets,* the SCC voiced strong concerns about the potential of an IP address to lead to the revelation of a biographical core of information. However, in the investigation of threats to national security, particularly in the cyber context, CSIS is not seeking the IP address to gather information about the lifestyle of the user, but rather for the purpose of thwarting a threat to national security. The IP address on its own as collected by CSIS does not reveal any personal information.

[156] The CSIS affiant explained that obtaining any personal information about the user of the IP address, apart from any personal information that would be publicly available, would require a warrant.

A. *The [...] IP addresses at issue in the Supplemental Application were lawfully collected*

[157] The Court agrees with the AGC and *amicus* and finds that the passive receipt and collection of the [...] IP addresses at issue does not engage section 8; there was no reasonable expectation of privacy and no search.

[158] The [...] IP addresses of hostile foreign actors with no *nexus* to Canada do not engage section 8 of the Charter. These foreign nationals do not come within the scope of "everyone" under section 8.

[159] As noted by the Chief Justice in *Outside Canada* at para 6, "foreign nationals with no recognized nexus to Canada do not benefit from the protections afforded by section 8." The Chief Justice explained at para 170, that foreign nationals without one of the three recognized grounds of nexus to Canada (Canadian citizenship, physical presence in Canada, or being subject to criminal proceedings in Canada) do not come within the scope of the term "everyone" in section 8.

[160] The [...] IP addresses of the Canadian victims of the cyber attacks—although they otherwise enjoy section 8 rights—did not have a reasonable expectation of privacy taking into account the totality of the circumstances.

[161] The Supplemental Application was therefore granted on the basis that the [...] IP addresses at issue did not engage any reasonable expectation of privacy; CSIS lawfully collected the IP addresses without a warrant pursuant to section 12 as a non-intrusive collection activity.

B. *The [...] IP addresses could have been collected pursuant to section 12 as minimally intrusive collection*

[162] In *Bykovets*, the SCC found that the "IP address may betray an intensely private array of information touching on the intimate details of the lifestyle and personal choices of an individual user" (at para 70 [emphasis added]). However, in the cyber warrant context the IP address does not; CSIS is not seeking anything more than the IP address for the purpose of thwarting a cyber attack. The IP address in this context does not betray personal details of lifestyle. As the affiant attested, CSIS would seek a warrant to obtain any personal information, as that is more than minimally intrusive.

[163] Moreover, where the IP address is being collected only to thwart a cyber attack, in such circumstances, any expectation of privacy would not be reasonable.

[164] The [...] IP addresses at issue, if any reasonable expectation of privacy had been found to exist, could have been collected in accordance with section 12 as a minimally intrusive search. The collection of the IP address was also narrowly targeted, accurate (to the extent possible given that IP addresses change quickly) and no other information was incidentally captured (and if so, would not be retained) (*IMSI* at para 236).

[165] In future supplemental applications, IP addresses passively received via interagency sharing of hostile foreign actors and/or victims of cyber attacks could be collected as either non-intrusive (if no reasonable expectation of privacy is apparent) or as a minimally intrusive collection. [...]

C. *Passive receipt of IP addresses*

[166] As noted, CSIS passively received the majority of the [...] IP addresses from foreign and domestic agencies. CSIS also passively receives IP addresses in other contexts. The *amicus* notes that such passive receipt, given that the foreign and domestic agencies have lawfully collected the IP addresses and then shared them, does not engage the *Charter*.

[167] The Court has considered how *Bykovets* has been interpreted and applied by superior and provincial courts. This jurisprudence, as noted above, supports the view that the passive receipt by law enforcement agencies of IP addresses from foreign agencies and non-state actors does not engage section 8 rights.

[168] The Court agrees that on the basis of the analogous jurisprudence in the criminal context, when CSIS passively receives IP addresses from foreign or domestic agencies without any request or "state action" on the part of CSIS, there is no search.

[169] In analogous circumstances to the present circumstances, or in other contexts where there is passive receipt of IP addresses by CSIS, reliance on section 12 is sufficient to collect IP addresses; this is minimally intrusive (if not non-intrusive).

D. *Section 12 permits minimally intrusive searches where all criteria of section 12 are met*

(1) Section 12 provides the authority for minimally intrusive searches – which includes a request for an IP address

[170] The jurisprudence of this Court and the Federal Court of Appeal has addressed the scope of section 12. While *Bykovets* clarifies the reasonable expectation of privacy in an IP address and establishes that prior judicial authorization is required for the police to request an IP address in investigating a crime, the jurisprudence of this Court has addressed the different context of national security and can live alongside the guidance of *Bykovets.* This jurisprudence establishes that section 12 does not authorize more than minimally intrusive searches (i.e., those that would capture information related to the biographical core of the individual). Moreover, section 12 has other checks and balances.

[171] In *Outside Canada*, the Chief Justice stated at paras 176 and 178:

> [176] This Court has consistently held that, without a warrant, section 12 only authorizes CSIS to engage in activities that are minimally intrusive. However, that jurisprudence involved subjects of investigation who benefitted from the rights afforded by section 8 of the *Charter*.
>
> […]
>
> [178] I recognize that "prior authorization, usually in the form of a valid warrant, has been a consistent prerequisite for a valid search and seizure both at common law and under most statutes": *Hunter*, above, at 160. However, section 12 overrides the common law by providing specific authority to CSIS to collect, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada.

[172] *Bykovets* clearly calls for prior judicial authorization for the police to request an IP address for a criminal investigation, but section 12 does not require prior judicial authorization for CSIS to collect "to the extent that it is strictly necessary" intelligence respecting activities that are reasonably suspected of constituting threats to the security of Canada.

[173] In *Mahjoub (Re)*, 2013 FC 1096 at para 33, Justice Blanchard noted that while section 12 appears to be broad in scope, it is constrained by the warrant requirements of sections 21-24. Justice Blanchard clarified that section 12 does not authorize intrusive searches or seizures of private information.

[174] Justice Blanchard found, at para 35, that section 12 requires CSIS to have an objective, particularized basis for the use of minimally intrusive investigative techniques, and strikes the balance "between the public interest in investigating threats to the security of Canada and the individual target's privacy rights."

[175] The Federal Court of Appeal considered three related appeals, including Justice Blanchard's decision, noted above, and stated at para 176 of *Mahjoub FCA*:

> Section 12 …empowers the collection of information and intelligence on activities that may on reasonable grounds be suspected of constituting threats to the security of Canada. Contrary to Mr. Mahjoub's submission, that power is not untrammelled: investigations may be undertaken only if there are "reasonable grounds to suspect" that activities constitute "threats to the security of Canada" and then only "to the extent that is strictly necessary". I agree with the Federal Court that section 12 is neither vague nor overbroad. Section 12 is limited by section 2, which defines in detail what constitutes a "threat to the security of Canada" in a manner that conforms to the standards set by the

> Supreme Court of Canada [in jurisprudence governing overbreadth and vagueness].

[176] In *Mahjoub FCA*, at para 177, the Federal Court of Appeal also agreed with Justice Blanchard's finding that section 12 and the warrant provisions were constitutional and that the reasonable grounds to suspect standard in section 12 complied with section 8 of the *Charter* given the minimally intrusive nature of the searches permitted pursuant to section 12.

[177] In *IMSI*, the Chief Justice considered CSIS's reliance on section 12 and found that section 12's requirement for reasonable grounds to suspect "is a "robust" standard that is well known in Canadian law…", noting that the scope of section 12 is further narrowed by the requirement that the information collected is "strictly necessary" (at para 213).

[178] At para 218, the Chief Justice clarified:

> …CSIS has no mandate under section 12 to investigate persons whose activities do not give rise to reasonable grounds to suspect that they constitute threats to the security of Canada. The investigative powers provided to it under section 12 are confined to those whose activities meet this robust threshold…

[179] The issue before the court in *IMSI* was the use by CSIS of cell site simulators [CSS] to capture identifying characteristics of mobile devices of a subject of investigation, in particular the international mobile subscriber identity [IMSI] and international mobile equipment identity [IMEI]. The Chief Justice found that section 12 provides CSIS with reasonable lawful authority to collect IMSI and IMEI information as subsets of transmission data as a minimally intrusive search.

[180] The Chief Justice's decision was succinctly captured by Justice O'Reilly in *Preferred Networks* at paras 105, 107, and 109-110:

> [105] This Court, in a decision authored by Chief Justice Paul Crampton, has addressed the use of CSS in the context of s 12 of the Act, that is, for purposes of investigating threats to national security (Re X (CSS), 2017 FC 1047). The Chief Justice concluded that the use of CSS amounted to a search because users of mobile devices had a reasonable expectation of privacy in respect of the information CSS technology could capture. However, he found that use of CSS without a warrant was lawful so long as the Service took measures to minimize the intrusion on privacy by refraining from intercepting communications or information stored on the device, destroying any information collected incidentally from third parties, and desisting from using the information for purposes of geo-location. <u>While the information available through CSS could assist the Service to create a thin personal profile of the user, thereby engaging s 8 of the Charter, the Chief Justice found that the warrantless searches were not unreasonable given that they were narrowly targeted, highly accurate, and minimally intrusive.</u>
>
> […]
>
> [107] The Chief Justice began by making clear that warrantless searches are presumptively unreasonable and contrary to the protection in s 8 of the Charter against unreasonable searches and seizures. Nevertheless, a search could be found to be reasonable if it was authorized by law, the law was reasonable, and the search was executed reasonably. He found that, under s 12, the Service had an obligation to collect, analyze, and retain information and intelligence about activities posing a threat to national security (para 196). The Act also sets out the circumstances when the Service should obtain a warrant (s 21). However, the Act does not require the Service to obtain a warrant whenever it seeks to gather information relating to national security even when a person's reasonable expectation of privacy is at stake. He found that there is a range of minimally intrusive activities the Service can carry out within its national security mandate without having to obtain a warrant (para 198), again, so long as the law authorizes those activities, the law is reasonable, and the means of carrying out the search are reasonable.
>
> […]

> [109] The Chief Justice found that s 12 was a reasonable law, considering its nature and purpose, the degree of intrusiveness it authorizes, the mechanism of intrusion, the availability of judicial supervision, and other checks and balances. The first of these criteria, the nature and purpose of the applicable statutory provision, differs significantly as between ss 12 and 16, as discussed above.
>
> [110] The Chief Justice considered the nature and purpose of s 12 to be the assignment of responsibility to the Service, where strictly necessary, to collect, analyze, and retain information and intelligence in respect of activities it reasonably suspects constitute a "threat to national security", a statutorily defined term (s 2). He described this role as "critical, central and arguably essential". He rejected arguments of the amici before him that the reasonable suspicion standard was unconstitutionally low, noting that that standard had been approved by the Supreme Court of Canada in cases where privacy interests were limited, important public interests were at stake, or the search method involved was highly accurate (paras 206-207). Each of those circumstances, he concluded, was present in respect of searches using CSS for s 12 purposes – minimal intrusion, pressing national security concerns, and high precision.
>
> [Emphasis added].

[181] Similarly, the collection of an IP address with a reasonable expectation of privacy would be a minimally intrusive search because the IP address, without more, reveals no personal information. While an IP address could be used to create a "thin profile of the user" if "enriched" through a public search engine, the collection of the IP address via section 12—if all the criteria of section 12 are met, in particular that it is for the investigation of a threat to national security and is strictly necessary—is a reasonable search. The request for the IP address would fall within the "range of minimally intrusive activities the Service can carry out within its national security mandate".

[182] In *IMSI*, the Chief Justice found that the use of CSS constituted a search because the individual had a "reasonable expectation of privacy in respect of the information that CSIS was in a position to begin to gather about him, or about which it was able to make informed inferences, upon gaining access to the IMSI and IMEI numbers of his mobile devices" and "[t]o the extent that this enabled CSIS to begin to gain an understanding of, or to make reasoned inferences about, certain aspects of [his] core biographic personal information, it engaged his rights under s. 8 of the Charter" (at para 6).

[183] The same rationale underlies the SCC's finding in *Bykovets* that an IP address has a reasonable expectation of privacy. However, in the CSIS context the IP address alone would not generally enable CSIS to make inferences about core biographical information. Nonetheless, *Bykovets* establishes that the users of IP addresses (all IP addresses) have a reasonable expectation of privacy in the IP address, which engages their section 8 rights. The issue is whether a search for an IP address is reasonable.

[184] In *IMSI*, the Chief Justice found that, although the collection of IMSI and IMEI engaged section 8, the warrantless collection of that information (i.e., the search) was not unreasonable because it was narrowly targeted, highly accurate and minimally intrusive (at para 7).

[185] The Chief Justice noted, at para 112, that "[i]n assessing whether an individual had a reasonable expectation of privacy in relation to the subject matter of an alleged search, the totality of the circumstances to be assessed include various factors directly related to the individual's expectation of privacy, both subjectively and objectively viewed." The Chief Justice

noted the factors established in the jurisprudence, which are the same factors noted by the SCC in *Bykovets.*

[186] The Chief Justice also found, at para 198, that section 12 "provides CSIS with all the authority it requires to investigate activities that may on reasonable grounds be suspected of constituting threats to the security of Canada, without a warrant, unless a warrant is required at common law."

[187] The Chief Justice addressed the difference between the requirement for police to obtain a warrant and the ability for CSIS to rely on section 12, noting at para 200:

> [200] The Amici further suggest that requiring a warrant before seeking to obtain IMSI and IMEI identifiers through the use of CSS technology would be consistent with the implicit requirement that the police must obtain a general warrant under section 487.01 of the Criminal Code, or a transmission data recorder warrant under section 492.2, before they may use a CSS to obtain and attribute IMSI and IMEI numbers to a suspect. However, the fact that Parliament may have determined that police require a warrant to use a CSS to attribute IMSI and IMEI numbers to an individual would not provide a sufficient basis for inferring that CSIS is also required to obtain a warrant in such circumstances. Among other things, police do not have available to them the powers conferred by section 12 of the Act.

[188] This is analogous to the current circumstances where the *Criminal Code* warrant provisions govern the police where they request an IP address and section 12 governs CSIS where CSIS requests or collects an IP address.

[189] In *IMSI,* the Chief Justice responded to the *amici* regarding Parliament's intent in enacting section 12, noting at para 201:

> [201] The *Amici* also maintain that it is for Parliament to decide whether to allow CSIS to use a CSS to intercept and attribute the IMSI and IMEI numbers of a mobile device to a subject of investigation, based on "reasonable grounds to suspect." I agree, and I find that Parliament implicitly did so when it passed section 12 of the Act. Therefore, CSIS's use of a CSS for that particular purpose is "authorized by law," as contemplated by the jurisprudence cited at paragraph 133 above.

[190] Similarly, section 12 authorizes CSIS to request or otherwise collect IP addresses on the reasonable grounds to suspect standard, where all the criteria of section 12 are met. If Parliament wants to limit CSIS's authority it can do so, but would also need to balance the need to ensure that CSIS has the tools needed to investigate and, ideally, to thwart threats to national security.

[191] In *IMSI*, the Chief Justice concluded that section 12 is a reasonable law, explained his conclusion at paras 202-235 and summarized the rationale at para 236, noting the purpose of section 12, the degree of intrusiveness authorized by section 12, the judicial supervision of section 21 that applies once CSIS seeks authority to engage in more than minimally intrusive activities, and the review role of the Security Intelligence Review Committee [SIRC] (now the National Security Intelligence Review Agency [NSIRA]). The same rationale applies to CSIS in relying on section 12 to collect IP addresses without a warrant.

(2) Is the search for an IP address always minimally intrusive?

[192] The *amicus* submits that the search for an IP address is not <u>always</u> minimally intrusive.

[193] The *amicus* acknowledges that the IP address on its own is just a string of numbers and does not include any private information. However, the *amicus* argues that a warrant <u>may</u> be required when the "digital breadcrumbs" of the IP address have the potential to reveal intimate

details close to the biographical core of the target's privacy interests. While this potential exists, not all IP addresses will lead to this revelation. To the extent that the affiant addressed this issue on the Supplemental Application, the evidence is that CSIS does not obtain biographical core type information derived from an IP address except with a warrant. CSIS would apply for a section 21 warrant to seek any other information regarding an IP address (on the higher threshold of reasonable grounds to believe that the information is required to enable CSIS to investigate a threat to the security of Canada and where all the other requirements of section 21 are satisfied). The affiant confirmed that CSIS does so.

[194] In *IMSI* at para 219, the Chief Justice captured the scope of section 12 as follows:

> [219] For the narrowly circumscribed scope of remaining activities that fall within the purview of section 12, CSIS may collect, analyse and retain information that ranges from non-intrusive to highly intrusive. However, once it moves beyond minimally invasive collection activities, it will require a warrant. In brief, by including the provisions of section 21 pertaining to warrants in the Act, Parliament implicitly contemplated that CSIS would not conduct collection activities under section 12 that are more than minimally intrusive, without first obtaining judicial pre-authorization under section 21. It can be inferred from this framework that, in the absence of a warrant, section 12 only provides CSIS with the ability to engage in non-intrusive or minimally intrusive activities.

[195] It is not disputed that warrantless searches pursuant to section 12 are restricted to minimally intrusive searches. If CSIS requests an IP address in a context that already provides some information about a target of an investigation, who has a reasonable expectation of privacy in their IP address, the IP address may permit more than a "thin personal profile" to emerge. In such contexts the collection of the IP address would be more than minimally intrusive and would require a warrant.

[196] The *amicus* further submits that no lesser degree of privacy exists in an IP address collected in the national security context than in the context of a criminal investigation. However, whether the reasonable expectation of privacy—regardless of the degree of privacy—is the same in the national security context as in the criminal context depends on the circumstances.

[197] Even though IP addresses have a reasonable expectation of privacy, some users' expectation may not be reasonable. The starting point is to determine if there is a reasonable expectation of privacy in the totality of circumstances. In *Bykovets,* the SCC noted that the expectation is reasonable where the public interest in being left alone outweighs the government's interest in intruding on the individual's privacy to advance their goals. In the investigation of threats to national security, the government's interest in requesting and collecting the IP address may outweigh that of the individual, depending on the nature of the threat and the other circumstances.

[198] In *IMSI* at para 166, relied on by the *amicus*, the Chief Justice addressed the AGC's argument that the lower possibility of being prosecuted based on personal information gathered by CSIS than on information gathered by the police does not on its own support finding a lower expectation of privacy. The Chief Justice found that several factors—including the potential consequences—inform the reasonable expectation of privacy.

[199] In his analysis of why section 12 provided the authority for minimally intrusive searches, the Chief Justice noted, among other things, the essential role played by CSIS in national security (at para 203). The Chief Justice added at para 206:

> The Court [SCC] has subsequently reiterated that the "balancing of interests can justify searches on a lower standard where privacy interests are reduced, or where state objectives of public importance are predominant" (*Chehil*, above, at para 23). In brief, the standard required to withstand scrutiny under section 8 "may vary depending on the context" (*Rogers*, above, at para 35).
>
> [emphasis added].

[200] With respect to the reasonableness of a search, in relying on section 12, the Chief Justice stated in *IMSI* at para 211:

> I consider that the national security objectives permeating section 12 will generally be sufficient to tip the balance in favour of the state interest, when searches conducted by CSIS are minimally intrusive (*Jarvis*, above, at para 71; *Mahjoub FCA*, above). As the Supreme Court has recognized, "[o]ne of the most fundamental responsibilities of a government is to ensure the security of its citizens."
>
> (see *Charkaoui v Canada (Citizenship and Immigration)*, 2007 SCC 9 at para 1).

[201] As noted above, in *IMSI*, the Chief Justice reiterated the importance of CSIS's role in investigating threats to national security as "critical, central and arguably essential" (at para 203).

[202] The *amicus* acknowledges that the nature of the investigation—e.g., CSIS's investigation of a threat to national security—is a relevant factor as is other information CSIS may have when seeking an IP address.

[203] Although the *amicus* cautioned about reliance on established jurisprudence regarding section 12 in light of *Bykovets*, the Court finds that the jurisprudence of the Federal Court and Federal Court of Appeal remains binding and guiding. This jurisprudence, in considering intrusions on a reasonable expectation of privacy and the scope of section 12, has addressed

many of the same issues considered in *Bykovets* regarding what constitutes a reasonable expectation of privacy, the need to consider the totality of the circumstances and the need for balance, albeit in the national security context. *Bykovets* confirms that there is a reasonable expectation of privacy in an IP address, just as, for example, in *IMSI* the Court accepted that there was a reasonable expectation of privacy in IMSI and IMEI numbers, yet concluded that section 12 could be relied on for a minimally intrusive collection, where narrowly targeted and accurate and acknowledging all the other checks and balances on reliance on section 12.

(3) Production orders in the *Criminal Code* vs section 12 of the *CSIS Act*

[204] As noted, the *amicus* cautions that *Bykovets* should not be interpreted to support the conclusion that section 12 provides the authority to seek an IP address. The *amicus* submits that although the majority in *Bykovets* suggests that obtaining judicial pre-authorization—for example a *Criminal Code* production order for transmission data by telewarrant—would be relatively easy, this should not be relied on to more generally conclude that the SCC regarded the request for an IP address as a minimally intrusive search.

[205] The *amicus* agreed in response to questions from the Court that *Bykovets* supports the view that a *Criminal Code* production order for transmission data pursuant to section 487.015 would have avoided the outcome in *Bykovets*, but does not agree that this would generally be the approach or that it is a minimally intrusive search.

[206] In this Court's view, there would be no other reason for the SCC to provide the specific example of the section 487.015 production order for transmission data by telewarrant, if not to signal that this is what the police could have done to obtain Mr. Bykovets' IP address—and

should do to obtain IP addresses in similar circumstances in the future. Section 487.015 provides for a production order for the purpose of identifying a device involved in the transmission of data (which captures an IP address). The other likely options in the *Criminal Code* are tailored to obtaining specific information and, with the exception of a production order for a document containing data (i.e., content), are all based on the reasonable grounds to suspect standard.

[207] Of the analogous *Criminal Code* provisions, only the production order for a document containing data (whether general or for specific dates) requires reasonable grounds to believe that an offence has or will be committed and the document or data will provide evidence respecting the commission of the offence. An IP address on its own does not contain data.

[208] The *amicus*' view is that the section 487.015 *Criminal Code* telewarrant example should not be relied on because in *Bykovets* the SCC was not called upon to determine the type of prior judicial authorization that should have been sought, as the police had not sought any authorization at all. However, if the police had sought judicial authorization, this matter would not have reached the Court. The SCC responded to the *Charter* challenge that arose on the facts and addressed what would have avoided that violation—as it routinely does in other circumstances where *Charter* violations are found. In this Court's view, the SCC signalled that a warrant should have been sought and if there were "enough" grounds to support the reasonable suspicion that an offence had or would be committed, the *Criminal Code* production order for transmission data would have provided the authority to the police to request the IP address from the third-party payment processing company. The concepts of reasonable grounds, whether to suspect or to believe, are not new concepts to the police, CSIS or the courts. What is "enough" to meet the threshold is a case-by-case determination in the particular circumstances.

[209] Despite the broad statements in *Bykovets* regarding the privacy interests at stake in that case, which suggest that the privacy in an IP address is significant (because of what it may reveal, and because it is the first digital breadcrumb), the SCC would not have suggested that a section 487.015 production order for transmission data would have been the better way to proceed if the reasonable grounds to suspect threshold was not sufficient to guard against an unreasonable search.

[210] With respect to the mixed messages in *Bykovets*, the *amicus* acknowledges that there is "tension" between the passages that note the significant privacy interest in an IP address and para 85, which points to a production order on the reasonable grounds to suspect standard as the requisite authority. The *amicus* views some passages as *obiter*, while the AGC views others as *obiter*.

[211] The SCC's references are, in some paragraphs, directed to the particular facts of *Bykovets* and, in others, more general; for example, regarding the privacy interests implicated in IP addresses. This Court has attempted to reconcile and apply the guidance of the SCC, albeit in the different circumstances of the Supplemental Application and the context of the *CSIS Act*, and with the guidance of the Federal Court and Federal Court of Appeal jurisprudence that has focussed on the scope of section 12 in the national security context.

[212] As noted by the AGC, CSIS's mandate pursuant to section 12 for non-warranted collection has many checks and balances, including: the statutory requirements; judicial scrutiny in the event that CSIS relies on the information collected to later seek a warrant; oversight by the Minister of Public Safety; the requirement for the Director of CSIS to report to the AGC and

Minister where an employee may have acted unlawfully; and, accountability to and review by NSIRA and the National Security and Intelligence Committee of Parliamentarians.

E. *CSIS should not be held to a higher standard than the police*

[213] In *Bykovets*, the majority characterized the reasonable grounds to suspect standard imposed on law enforcement to obtain a section 487.015 production order for transmission data by telewarrant as not onerous. I agree with the AGC that CSIS should not be held to a more onerous standard in the national security context, where all the criteria of section 12 are met.

[214] Telewarrants are not an option for CSIS. The options are section 12 for minimally intrusive searches without a warrant (where all the criteria are met), or section 21, with its additional requirements, including detailed affidavits, *ex parte in camera* hearings, cross-examination of affiants and a determination by a Designated Judge. Seeking a section 21 warrant to request an IP address which will not be used to obtain any further biographical core type information is onerous and would not permit CSIS to investigate and thwart cyber threats or other threats to national security as they arise.

[215] If the police can obtain a *Criminal Code* section 487.015 production order to identify a device on the reasonable grounds to suspect standard and obtain an IP address, then CSIS should be able to collect this same type information pursuant to section 12 on the same standard in the national security context; no higher standard should be imposed in the national security context (*Mahjoub FCA* at paras 265-267).

[216] However, CSIS will require a warrant to seek other information that reveals biographical core type information.

F. *The post – acquisition use of IP addresses*

[217] As noted, the Court agrees that the [...] IP addresses in the Supplemental Application were lawfully collected without a warrant as non-intrusive collection and alternatively, could have been collected as minimally intrusive collection. The users of the [...] IP addresses do not have a reasonable expectation of privacy and, therefore, the collection of the IP addresses does not engage section 8 (i.e., no search).

[218] A related issue is whether CSIS can use or enrich the [...] IP addresses. The AGC and *amicus* agree that the further use or enrichment of the [...] IP addresses is not a search. Their rationale is that because the collection of the [...] IP addresses did not engage section 8, the further use of these addresses would also not engage section 8. There was no reasonable expectation of privacy in the first place and it would not be acquired after the fact.

[219] The *amicus* notes that it is the capacity for the IP address to reveal other information that grounds the reasonable expectation of privacy (*Bykovets* at paras 63-65), and if the IP address is lawfully obtained, the subsequent use or enrichment of the IP address, using open-source tools limited to obtaining geolocation and the CSP should not require a warrant. The *amicus* cautions, however, that any more intrusive collection would require a warrant on the reasonable grounds to believe standard.

[220] In *Bykovets*, the SCC did not comment on the subsequent use of the IP address once lawfully obtained, but noted that other warrants would be required to obtain the content of communications—as they would in the CSIS context. In a more targeted investigation by CSIS, a warrant would be required to obtain other information based on a lawfully collected IP address that would reveal biographical core type information.

[221] Whether other IP addresses lawfully collected (warranted or non-warranted) can be enriched via publicly available open-source tools is not an issue to be determined in this Application. Although the AGC acknowledges that this enrichment occurs and submits that the enrichment of IP addresses via public open-source tools, which are also used by police (as noted in *Leger* and *Pengelly)*, does not engage section 8, this issue remains to be addressed in the context of an appropriate application with a factual record that fully explains the capacity of the open-source tools to enrich an IP address.

X. AGC's further alternative argument

[222] The AGC's "fall-back" position relying on the balancing test established in *En Banc* need not be addressed. That approach would be an "after the fact" determination of whether the collection of intelligence and/or IP addresses was lawful. If this issue arises in the future, it will be addressed at that time.

XI. Conclusion

[223] To summarize, the Court finds:

- The [...] IP addresses at issue in the Supplemental Application were lawfully

collected pursuant to section 12 as non-intrusive collection; the [...] IP addresses did not attract a reasonable expectation of privacy and did not engage section 8.

- IP addresses collected pursuant to the cyber warrant, in analogous circumstances (for example passive receipt and/or no reasonable expectation of privacy) may be lawfully collected as non-intrusive or minimally intrusive pursuant to section 12.
- IP addresses in other contexts, where the IP addresses are passively received by CSIS and where there is no "state action", may be lawfully collected pursuant to section 12.
- IP addresses may be requested by CSIS pursuant to section 12 as a minimally intrusive search where all the criteria of section 12 are met (to the extent that the information is strictly necessary and the information relates to activities that may reasonably be suspected of constituting threats to the security of Canada). The restriction is that the collection is minimally intrusive, narrowly targeted and highly accurate. As noted above, this conclusion is supported by the jurisprudence regarding section 12, which among other things, acknowledges that while a warrant is required for the police—on the reasonable suspicion standard—section 12 provides analogous non-warranted authority for CSIS in the national security context.
- Any collection of IP addresses that is more than a minimal intrusion requires judicial pre-authorization.
- For example, where CSIS requests an IP address in a context that initially provides some information about a target of an investigation, who has a

reasonable expectation of privacy in their IP address, the IP address has the potential to reveal biographical core type information; in such contexts the collection of the IP address would be more than minimally intrusive and would require a warrant.

- With respect to the use or enrichment of the [...] IP addresses at issue in the Supplemental Application, because there is no reasonable expectation of privacy in these IP addresses, the subsequent use or enrichment of the [...] IP addresses does not raise any section 8 concerns.

"Catherine M. Kane"
Judge

FEDERAL COURT

SOLICITORS OF RECORD

DOCKETS:	C-1-24
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 CYBER ESPIONAGE, CYBER SABOTAGE, and CYBER FOREIGN-INFLUENCED ACTIVITIES
PLACE OF HEARING:	OTTAWA
DATE OF HEARING:	OCTOBER 15 AND 24, 2024
CLASSIFIED REASONS:	KANE J.
DATED:	DECEMBER 16, 2025

APPEARANCES:

JEFFREY JOHNSTON ZORICA GUZINA	FOR THE ATTORNEY GENERAL OF CANADA
MATTHEW GOURLAY	*AMICUS CURIAE*

SOLICITORS OF RECORD:

Attorney General of Canada Ottawa (Ontario)	FOR THE ATTORNEY GENERAL OF CANADA
Henein Hutchison Robitaille LLP Toronto (Ontario)	*AMICUS CURIAE*