Office of the
Saskatchewan Information
and Privacy Commissioner

Policing Technology and the Citizen's Reasonable Expectation of Privacy

Grace Hession David
Saskatchewan Information and Privacy Commissioner
503-1801 Hamilton Street
Regina, Saskatchewan
June 3, 2026

Canadian Association for Civilian Oversight of Law Enforcement

Introduction

Privacy interests have always influenced the outcome of many trials in the Canadian criminal justice system. In this digital age, legal issues involving privacy now intersect with police investigations in a way that could not have been conceived of five years ago. An individual will usually request the protection afforded by sections 8 and 7 of the *Charter*[1] upon an allegation of a violation of privacy. For many years the Supreme Court of Canada has considered privacy issues in the context of police investigations. Several cases that are making their way up the appellate chain involve challenges to the police use of newer technology including the use of artificial intelligence. This paper hopes to explore the reasonable expectation of privacy analysis as it applies to the more recent police investigations. In some of the earlier cases, the courts were inclined to admit impugned evidence even though the ruling found *Charter* rights had been violated. In more recent cases, the courts have been reluctant to admit the evidence through the *Grant* analysis.[2] This paper will concentrate on how the courts define a reasonable expectation of privacy in the context of informational privacy.[3] If we can understand how courts have developed this concept, it will be easier to predict how the newer technologies will fare in the ultimate analysis when the challenge is inevitably brought.

R v Spencer[4] - Reasonable Expectation of Privacy in Subscriber Information from an IP Address

In 2011 the Saskatoon police service online child abuse investigation identified the IP (Internet Protocol) address of a computer engaged in an internet file-sharing program on an online child pornography site. The police made a "law enforcement request" to the Internet Service Provider (ISP), Shaw, for the subscriber information including the name, address and telephone

---

[1] *Canadian Charter of Rights and Freedoms,* Part I of the *Constitution Act, 1982,* enacted by the *Canada Act 1982 (UK),* c. 11, (April 17, 1982).

[2] *R v Grant,* 2009 SCC 32, [2009] 2 SCR 353.

[3] *R v Spencer,* 2014 SCC 43, [2014] 2 SCR 212 at paragraph [35] ("*Spencer"*). The Supreme Court of Canada has defined three broad types of privacy interests: (1) Territorial; (2) Personal; and (3) Informational.

[4] *Ibid*.

number of the client using the IP address. [5] The ISP provided the information and the police obtained a search warrant. The home was searched, a laptop obtained and the owner of the laptop arrested. Spencer was charged with possession of child pornography contrary to section 163.1(4) of the *Criminal Code* and making child pornography available contrary to section 163.1(3). The trial judge found there was no merit to Spencer's section 8 argument because the police request to the ISP was not a "search". Spencer was convicted of the possession count but acquitted of making pornography available because the trial judge found there was no evidence of an identifiable act to prove the *actus reus* on the facts. The Saskatchewan Court of Appeal upheld the conviction on the possession count but found the lower court erred in failing to consider the doctrine of willful blindness on the making child pornography available.

A unanimous court panel at the Supreme Court of Canada found that a police request for the subscriber information without prior judicial authorization constituted an unreasonable search. As such the accused's section 8 *Charter* rights were violated. However, the court admitted the evidence pursuant to the *Grant* analysis. This was largely because the state conduct did not constitute a willful or flagrant violation of the law in 2014.

In coming to this conclusion, the Supreme Court of Canada formulated a test to assist in the analysis of a reasonable expectation of privacy. The four pillars of the test recommended an analysis of: (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 is objectively reasonable.[6] Spencer's subjective expectation of privacy was given because it was inferred from his use of the internet to transmit sensitive information. Similarly, Spencer's direct interest in in the subject matter of the search was obvious from the use of his own computer in his own place of residence. This case turned on two issues. First the trial judge erred in finding that there was no search. The subject matter of the search was found to involve *core biographical*

[5] The request was made according to the wording of the service contract between the subscriber and Shaw. The contract stipulated that the request could be made by the police pursuant to section 7(3)(c.1) of the *Personal Information Protection and Electronic Documents Act,* SC 200 c. 5 (*PIPEDA)* upon a showing of "lawful authority".

[6] *Supra,* footnote 3 at paragraph [18].

data revealing intimate and private information about Spencer, not as the Crown submitted and the trial judge agreed – simply generic information that did not touch at the core of biographical information.[7] The second issue was the determining factor: whether the subjective expectation of privacy was reasonable. This concept was decided based on the contractual and statutory framework that formed the basis of the relationship between Spencer and the ISP. Even though Spencer was not a party to the contract between the ISP and his sister, Spencer accepted the internet through his sister's subscription. That contract referred to *PIPEDA* and the various means within *PIPEDA* that allowed disclosure of information.

The Supreme Court found that section 7(3)(c.1) of *PIPEDA* did not create police search and seizure powers. In order to obtain disclosure of information from the ISP, the police would have to fit within the contractual terms of the subscription that referenced section 7(3)(c.1) of *PIPEDA*. In other words, the police had to demonstrate "lawful authority" when making the request of the ISP. This involved one of two possible options in law: either the police would have to prove exigent circumstances or reference another law to authorize the search. The police interpreted the lawful authority for the request as the fruits of their investigation up to that point - the transmission of child pornography to Spencer's laptop. This was the mistake. The nature of "lawful authority" was misunderstood by the investigating authorities. The Court made it clear that the lawful authority of the police request had nothing to do with reasonable grounds or the fact that it was a police investigation. In fact, the legality or illegality of the alleged behaviour on the part of the accused and the fact that the police were already investigating, *heightened* Spencer's privacy interest such that his expectation of privacy was reasonable:

> [36] The nature of the privacy interest does not depend on whether, in the particular case, privacy shelters legal or illegal activity. The analysis turns on the privacy of the area or the thing being searched and the impact of the search on its target, not the legal or illegal nature of the items sought. To paraphrase Binnie J. in *Patrick*[8], the issue is not whether Mr. Spencer had a legitimate privacy interest in concealing his use of the Internet for the purpose of accessing child pornography,

[7] *Ibid,* at paragraphs [31] and [32].

[8] *R v Patrick*, 2009 SCC 17, [2009] 1 SCR 579.

> but whether people generally have a privacy interest in subscriber information with respect to computers which they use in their home for private purposes.
> …
>
> [67] …Similarly in this case, the police request that the ISP disclose the subscriber information was in effect a request to link Mr. Spencer with precise online activity that had been the subject of monitoring by the police and thus engaged a more significant privacy interest than a simple question posed by the police in the course of an investigation.

The provisions of *PIPEDA* as they were cited in the contract between the ISP and the user were found to be crucial in the final analysis of the reasonableness of Spencer's subjective expectation of privacy. The Supreme Court of Canada read *PIPEDA* to prohibit an ISP's disclosure of information unless the requirements of the law enforcement provisions were met. Section 7(3)(c) of *PIPEDA* provides that personal information may be disclosed to authorities without consent where the authorities have provided a subpoena or a warrant to obtain the information. The Court interpreted this to mean that the requirements of section 7(3)(c.1) involved disclosure without consent only when another form of lawful authority exists outside of judicial authorization. Since there was neither in this case, the search of the Spencer house was based on improperly obtained subscriber information and therefore unlawful.

R v Bykovets[9]- Reasonable Expectation of Privacy in an IP Address

In *Spencer* the police investigation revealed a suspect IP address and the Supreme Court of Canada found that the police improperly used the provisions of *PIPEDA* to obtain the subscriber information attached to the IP address. Ten years later, the Supreme Court of Canada addressed the issue of whether there was a reasonable expectation of privacy in the IP address itself. *Bykovets* has clarified the scope of a reasonable expectation of privacy and it is notable that there was no *Grant* argument.

[9] *R v Bykovets*, 2024 SCC 6 (March 1, 2024). ("*Bykovets"*)

The Calgary Police Service investigated an online scammer who was actively engaged in fraud. The offender was using an unauthorized credit card to purchase gift cards. He then went online to a liquor store and purchased liquor with the stolen gift cards. Police contacted the third-party company that managed the store's online sales - Moneris. The police simply asked Moneris to give them the IP address of the individual who used the stolen gift cards in the identified transactions. Police then obtained a production order and presented it to Moneris to obtain the subscriber information attached to the IP address following the guidance in *Spencer*. Having obtained this information, the police obtained a search warrant to search his house.

At trial, Bykovets alleged that the police effected an unreasonable warrantless search when the IP address was simply handed over by the third party provider Moneris without any prior judicial authorization. Bykovets argued he had a reasonable expectation of privacy in his personal IP address. The trial judge ruled that Bykovets did not have a reasonable expectation of privacy in an IP address and convicted him of 14 fraudulent offences related to the online liquor sales. The Alberta Court of Appeal dismissed the conviction appeal. The Crown argued that there could be no expectation of privacy in an IP which is nothing more than a long blockchain of meaningless numbers that provided no biographical core information.

The analysis at the Supreme Court focussed on two issues that the lower courts had misinterpreted: the subject matter of the search and the reasonableness of the subjective expectation of privacy. A broad and functional approach was taken in defining the subject matter of the search. The police were not interested in a "collection of numbers". The request for the IP address was based on *the information that the IP address could reveal* - information about a specific internet user including their online activity, and their identity.[10] This is the biographical core information that underlines a true section 8 search.

[10] *Ibid,* at paragraph [41].

The reasonableness of Bykovets' expectation of privacy involved a consideration of three issues: Bykovets' degree of control over the subject matter, the place of the search and the private nature of the search. The fact that Bykovets had no choice but to reveal his biographical core information to conduct his affairs on the internet was not determinative of the issue. On this point, the Canadian courts will differ with American courts because a reasonable expectation of privacy is negated in the United States if information is possessed or known by third parties.[11] The fact that the place of the search was the "internet" was also not determinative with respect to the reasonableness of the expectation of privacy. The Supreme Court recognized that online spaces are qualitatively different from physical spaces. The real determining factor of the reasonableness issue was the private nature of the subject matter at the centre of the search. In this case, the Supreme Court threw the doors open wide to protect an individual's online privacy. Prior judicial authorization beyond that in *Spencer* was required because of the vast amounts of personal information attached to an individual's IP address:

> [67] …We would not want the social media profiles we linger on to become the knowledge of the state. Nor would we want the intimately private version of ourselves revealed by the collection of key terms we have recently entered into a search engine to spill over into the offline world. Those who use the Internet should be entitled to expect that the state does not access this information without a proper constitutional basis.
>
> …
>
> [69] Thus, to say that a *Spencer* warrant protects against the privacy concerns raised by IP addresses is simply not supported by modern technological realities. IP addresses play a crucial role in the inherent structure of the Internet. They are the means by which Internet-connected devices both send and receive data. As such, they are the key to unlocking an Internet user's online activity – the first "digital breadcrumbs" on the user's cybernetic trail…Those 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.
>
> [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.

[11] *Ibid,* at paragraph [47].

Noting that the community wants privacy but also insists on protection, the Supreme Court found that the balance had to weigh in favour of the expectation of privacy over the need for protection. This finding was steered by the fact that private third parties have now become predominate in the digital world. They have begun to work with the police and they have it within their ability to assimilate an ever growing mass of information that can rapidly expand the scope of police surveillance powers.[12] Prior judicial authorization was seen by the Supreme Court as serving to narrow the state's online reach and prevent it from acquiring the details of a citizen's online life that may or may not be relevant to an investigation. There is a reasonable expectation of privacy in an IP address, and this is protected by section 8 of the *Charter.*

Clearview AI Inc. v British Columbia (Information and Privacy Commissioner)[13]- Reasonable Expectation of Privacy in Mined Facial Images

Bykovets is the last pronouncement of the Supreme Court of Canada on the reasonable expectation of privacy. Interestingly, the decision in *Spencer* came from a unanimous court. *Bykovets* was a close 5:4 call with the minority siding with the community's need for protection when they ruled that there is no reasonable expectation of privacy in the IP address. Presently, there are two cases in the corridor on their way to the top court. The first is *Facebook Inc. v Privacy Commissioner of Canada.*[14] *Facebook* was argued at the Supreme Court on March 19th of this year. This case is only semi-related to our consideration of policing and privacy matters, but we mention it because it deals with privacy concepts that may affect the employment of new artificial policing technology. The main argument in the *Facebook* case was whether Facebook Inc. had given its subscribers proper notice of the fact that it collects, uses and discloses subscriber personal information to third party applications for a fee. The concept of "meaningful consent" is central to this case and resort was had throughout the oral argument to the contractual terms that

---

[12] *Ibid,* at paragraphs [78] and [79]

[13] *Clearview AI Inc. v British Columbia (Information and Privacy Commissioner),* 2026 BCCA 67 (application for leave to appeal filed April 20, 2026 – file number: SCC 42312). ("*Clearview"*)

[14] *Canada (Privacy Commissioner) v Facebook Inc.,* 2024 FCA 140.

must be consented to by subscribers as a prerequisite to page creation on the Facebook site. The concept of "meaningful consent" is a privacy fundamental but has little to do with policing where evidence is gathered without consent. This case is still important because of the concept of transparency upon which meaningful consent is based.

The next significant privacy case that is on its way to the top court is *Clearview*. Clearview AI Inc., is a private US-based technology company that sells facial recognition software. Its search engine detects and scans human faces and associated metadata (web page title, source link, and content description) from publicly accessible websites, such as YouTube, Instagram, and Facebook. Clearview's software analyzes each face using detailed measurements to produce a *numerical biometric identifier* (or "vector"). All facial images are stored indefinitely on Clearview's servers. In 2017, Clearview's database contained facial data for some three billion individuals the world over. By 2023 the Clearview database had grown to over 30 billion facial images.[15] Clearview primarily markets its services to law enforcement and government agencies in the United States. At the material time, it had several Canadian police services as clients. When a Clearview client uploaded a facial image of a person of interest, Clearview's algorithm retrieved facial images in the Clearview database that had a matching vector. A search on the Clearview application also provided link(s) to the website(s) from which the image was originally sourced. The Information and Privacy Commissioner of British Columbia found that the facial images that Clearview used constituted "personal information" within the meaning of the British Columbia *Personal Information Protection Act,* SBC 2003, c.63 [*PIPA*]. In early 2020 the information and privacy officers of BC, Alberta, Québec and Canada commenced a joint investigation into whether Clearview was violating privacy laws in those jurisdictions. In February of 2021 a joint report was issued by the privacy officers. The joint report concluded that Clearview was breaching the privacy laws of all four jurisdictions. The joint report recommended that Clearview stop offering its facial recognition services to clients in Canada; stop collecting, using and disclosing facial data of individuals in Canada; and delete any stored data of individuals in Canada on its server. Clearview chose to leave the Canadian market in July of 2021. Clearview's response was that it was no longer present in the Canadian market. The other two recommendations were deemed by Clearview to be unjustified and impossible to meet. In December of 2021 the British Columbia

[15] *Supra,* footnote 11 at paragraph [33].

Information and Privacy Commissioner issued a ruling that found Clearview had contravened the personal information sections of *PIPA*. Clearview was ordered to follow the same orders as the joint report but with reference to BC and/or to seek consent from the individuals from whom they had used, collected or disclosed a facial image. Clearview applied to judicially review the Commissioner's decision and the application was dismissed. The chambers judge made several consequential findings against Clearview on judicial review: (1) *PIPA* applied to Clearview as a matter of constitutional law in spite of the fact that it was a corporation resident in another sovereign nation; (2) Even though the personal information was "publicly available", Clearview still had to obtain consent from the individuals from whom they obtained the facial images; and (3) Clearview did not have a reasonable purpose such that consent was statutorily implied.

In February of 2026, Clearview brought the same three issues to the British Columbia Court of Appeal and that court upheld all of the chambers judge's findings. Clearview argued that there was no evidence with respect to the physical location of Clearview's servers or any of the platforms from which Clearview mined its data such that there could be a finding of sufficient connection between it and the citizens of British Columbia. The Court of Appeal dismissed this argument finding that in this digital age, physical location has little to do with the sufficient connection test. The Court of Appeal reasoned that if it were to hold that the provincial privacy laws were inapplicable to Clearview, the ability of the provincial jurisdictions across Canada to protect personal information of its residents would be significantly impeded. Clearview argued that to subject it to the vagaries of provincial privacy law would subject it to wholesale commercial liability. The appellate court noted that securities law is applied in cross-border cases of securities fraud. The regulation of privacy matters should be no different. The commercial aspect of the Clearview's relationship with police agencies was perhaps a deciding factor overall:

> [61] Second, as I have explained, this case is not about the "incidental touching" of a person's publicly available data. It is about a systematic acquisition of facial data regardless of jurisdiction that enables an enterprise to commercially exploit that information by disclosing it to law enforcement and other entities who are interested in connecting with an individual. …

Clearview argued that consent to mine the facial images of the residents of British Columbia should not be required because section 6(1)(d) of *PIPA* negates the need for consent if the data is publicly available. The court dismissed this argument as well because material that is publicly available is defined in the statute as "magazines, books or newspapers". Even though all three of these resources are now available digitally – they are still created and their content controlled by their authors. This is different than social media platforms that are created and controlled by the users of the site and upon whom the final say of the content is totally dependent. The fact that the public may submit comments on the content of the creator does not detract from the fact that the primary creator has the final say in the creation and display of the content. Thus, the material that is posted by the author of a social media site is not "publicly available" in British Columbia.

Conceptually Clearview showed its misunderstanding of the Canadian privacy regime as respected by the Canadian courts. Clearview erred significantly when it framed the privacy statutory regime in British Columbia as a "dual rights" regime that balances the rights of individuals to protect their personal information with the rights of organizations to collect and use personal information. Fundamental to the Court of Appeal's dismissal of the appeal was the finding that provincial privacy laws across Canada exist to provide individuals with some measure of control over the use of their personal information. An individual's right to control the use of their personal information is intimately connected to their autonomy, dignity and privacy. This right has been recognized as a quasi-constitutional right by the Supreme Court of Canada.[16] These are cherished values that lie at the heart of Canadian democracy. Clearview's submission that this was a case of competing rights was misguided. The Court of Appeal framed this case as a fundamental right that had to be balanced with a corporate need.[17]

---

[16] *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401,* 2013 SCC 62, [2013] 2 SCR 733 at paragraph [19] . See also *Canada (Information Commissioner) v Canada (Minister of National Defence),* 2011 SCC 25, [2011] 2 SCR 306 at paragraphs [40] and [79].

[17] *Supra,* footnote 11 at paragraphs [79] to [82].

Finally, Clearview argued that its purpose in collecting, using and disclosing personal information was connected to a purpose that a reasonable person would consider appropriate because it was central to law enforcement. *PIPA* allows for the collection, use and disclosure of personal information in circumstances that a court would define as "reasonable". Clearview was not persuasive on this ground simply because of the commercial relationship that tied Clearview with law enforcement. The underlying commercial relationship refuted Clearview's argument that its sole purpose was a dedication to law enforcement.[18]

Canadian Civil Liberties Association v Canada (Attorney General)[19]- Constitutional Challenge to Provisions of *PIPEDA*

Accused people are not the only parties that seek relief through privacy arguments. The above case followed on the heels of *Spencer* with an application to the Ontario Superior Court for a ruling that certain provisions of *PIPEDA* be declared unconstitutional on the grounds they violate section 8 and section 7 of the *Charter*. In particular the sections of *PIPEDA* that the Canadian Civil Liberties hoped to have declared a null and void included section 7(3)(c.1) which figured prominently in *Spencer,* and sections 9(2.1), (2.2.), (2.3) and (2.4). Section 7(3)(c.1) of *PIPEDA* allows a private TSP to disclose basic subscriber information to a Canadian government authority (the police for instance), if there is *"lawful authority"* as defined by *Spencer*, and as long as the police can show that the information requested is for the purpose of enforcing any law in Canada or carrying out an investigation pursuant to that law.

Sections 9 (2.1), (2.2), (2.3) and (2.4) are known as the "veto provisions" of *PIPEDA* in that they negate the requirement of notice when the police request disclosure from a TSP. If an individual applies to the TSP for an access to information with respect to any police requests, the

---

[18] *Ibid,* at paragraph [98].

[19] *Canadian Civil Liberties Association v Canada (Attorney General),* 2026 ONSC 783.

TSP must notify the police of the access request and the TSP cannot disclose to the requester the fact they have notified the police. Further, if the TSP conveys subscriber information to the police, the TSP is prohibited from disclosing the fact of disclosure to the individual if it can reasonably be expected to be injurious to (1) national security or the defence of Canada; (2) the detection, prevention or deterrence of money laundering or the financing of terrorist activities; or (3) the enforcement or investigation of any law in Canada.[20]

The chambers judge noted that TSPs across Canada have inconsistent definitions of subscriber information. Some limit "subscriber information" to names and addresses while others ascribe highly sensitive information such as date of birth, government-issued identification numbers, email addresses and even credit card data. The chambers judge was bound by the finding in *Spencer* and a more recent Ontario Court of Appeal decision that ruled *PIPEDA* does not prescribe search and seizure powers. Thus, the impugned provisions of *PIPEDA* do not engage the traditional section 8 privacy protection. [21] As a result, the chambers judge found that the *PIPEDA* provisions are permissive and in no way determinative of a section 8 claim. She found that the terms of *PIPEDA* are one of many factors that inform a court's determination of whether a reasonable expectation of privacy exists and if so, the nature and extent of that expectation.[22] The chambers judge dismissed the application to declare the impugned provisions of *PIPEDA* unconstitutional. She was concerned by the lack of prior judicial authorization, and the overall

---

[20] The provisions in *PIPEDA* are overwritten by the proposed provisions of the framework in Bill C-22 which passed its first reading in the House of Commons on March 26, 2026. The progress of that bill is currently stalled at second reading because of debate involving digital privacy considerations and the potential for an expansion of governmental surveillance powers. Bill C-22, "An Act Respecting Lawful Access" purports to allow authorities to demand subscriber information from TSPs subject to a production order form of judicial authorization. The authorities only need to allege a "reasonable grounds *to suspect*" in order to legalize the demand which is a significant departure from the reasonable grounds *to believe* now required by a section 487.014 *Criminal Code* production order.

[21] *Supra,* footnote 17 at paragraphs [74] and [83]. The chambers judge also found that the section 7 argument in this case was unconvincing and simply a re-packaging of the section 8 argument at paragraph [121].

[22] *Ibid,* at paragraph [78].

lack of oversight, accountability and transparency with respect to the gathering of information within the *PIPEDA* framework.

It is significant that the chambers judge was bound by a prior Ontario Court of Appeal decision from 2017. In *R v Orlandis-Habsburgo*[23] the appellate court dismissed a conviction appeal in a grow operation where the section 8 rights of the accused people were found to have been violated but the evidence of the marijuana grow operation was properly admitted by means of the *Grant* analysis. In that case, the third party energy company noticed a significant spike in energy use consistent with an illegal grow operation. The third party volunteered this information to the police. The police commenced surveillance on the house and ultimately obtained a warrant to search the house. The claimants argued that their section 8 rights had been violated because they had a reasonable expectation of privacy in the energy readings. In finding that the reasonable expectation of privacy was valid, the Ontario Court of Appeal emphasized that a reasonable expectation of privacy analysis will draw not just from the specific constellation of relevant facts of each case but also from cherished societal aspirations and values:

> [42] The value Canadian society places on the individual's right to be left alone by the state, absent state justification for any intrusion, lies at the heart of the normative inquiry required by s.8. Personal privacy is crucial, both to individual freedom and security and to the maintenance of a dynamic and healthy democracy. If a court holds that an individual has a reasonable expectation of privacy in a certain place, thing or information, the court is declaring that community values will not accept that the state should be allowed to intrude upon individual privacy in the way that it did without first establishing compliance with the reasonableness standard in s.8 of the *Charter.* See *Ward,* at paras. 79-87; *R v Pelucco,* 2015 BCCA 370, 327 CCC (3d) 151, at para 63; and *R v Wong,* [1990] 3 SCR 36, at pp. 45-46. Professor Stewart captures the inquiry well:
>
> > Put another way, the ultimate normative question is whether, in light of the impact of an investigative technique on privacy interests, it is right that the state should be able to use that technique without any legal authorization or judicial supervision? Does our conception of the proper relationship between the investigative branches of the

[23] *R v Orlandis-Habsburgo,* 2017 ONCA 649. The constitutionality of the *PIPEDA* provisions were also challenged in this case. In paragraph [122] of this ruling, Justice Doherty noted that *Spencer* had settled the issue that the privacy statutes in Canada do not create any police search and seizure powers.

state and the individual permit this technique without specific legal authorization?

Conclusion

Police Services who wish to introduce new technologies to increase their investigative powers must be very careful to respect the societal values that our courts have held to be at the heart of the reasonable expectation of privacy analysis in Canada. First and foremost, a reasonable expectation of privacy will not be narrowed to the subject matter of a search. As in *Spencer* and *Bykovets,* the courts will look beyond the subject matter of the search and determine whether core biographical data is at stake. The analysis is broad and functional. Further, having obtained core biographical data, the next step will be to acknowledge the claimant's interest in the subject matter and whether there is a subjective expectation of privacy. In determining whether the subjective expectation is reasonable, the final decision will be based on "whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement".[24]

Bykovets outlined that in the absence of a definitive list of factors, courts will focus on the claimant's control over the subject matter, the place of the search and the private nature of the subject matter.[25] The legality or illegality of the claimant's activities are irrelevant at this phase of the analysis. The third issue is the determining factor: biographical core information is directly related to identity. With the advent of artificial intelligence that can link a great deal of information to one piece of identity information, the issue will not be so much with whether individuals have a privacy interest in the subject matter of the search, but the totality of the information that the subject matter may tend to reveal.[26] There is a great need for transparency in the law enforcement

[24] *Hunter v Southam Inc.,* [1984] 2 SCR 145 at pages 159-160.

[25] *Supra,* footnote 7 at paragraph [44].

[26] *Ibid,* at paragraph [53].

purpose of the technology, a clarification and communication to the community with respect to the various uses attached to the technology and concrete systems in place to protect the security of the data retrieved by the technology if it is ever to survive a claim that it was obtained in violation of *Charter* and privacy rights.