FREEDOM CONVOY FEVER: Social Media and the Reasonable Expectation of Privacy in the Artificially Intelligent Surveillance State

MARK SOO *

ABSTRACT

The 2022 "Freedom Convoy" in Ottawa attracted widespread attention across traditional and social media outlets as the demonstration evolved into a long-drawn-out standoff between protestors and state officials. In the ensuing aftermath, the outpour of images and videos that flooded social media during the protest were subsequently used by law enforcement to arrest and charge individuals involved. This inspired an examination of the constitutional status of these "seizures."

Using the Freedom Convoy as a backdrop, this paper examines the reasonable expectation of privacy in information shared on social media, beginning with a discussion of the influence that artificial intelligence and machine learning have on modern policing. A broad discussion of whether a reasonable expectation

* BA (Simon Fraser University), JD (University of Manitoba), student at law, Platform Litigation. The author expresses his gratitude to John W Burchill for his insightful wisdom on shaping the preliminary direction of this paper. Additionally, the author acknowledges and thanks the anonymous peer reviewers and editors at the Manitoba Law Journal for their feedback and support on previous drafts of this article. Any errors or omissions are the author's.

of privacy exists in this area of the law then follows, and the difficulty of overcoming the doctrine of abandonment in establishing a privacy interest is noted. The issue of abandonment is then re-evaluated in light of recent jurisprudence from the Supreme Court of Canada, as well as the Mosaic Theory of the Fourth Amendment from United States v. Maynard. A conclusion is then presented, and suggestions are made concerning future research efforts.

INTRODUCTION

In February of 2022, dissatisfied citizens from across Canada drove to the City of Ottawa in semi-trucks to protest the Government of Canada's mandatory vaccination requirement for cross-border truckers.[1] This large-scale movement was dubbed the "Freedom Convoy." It took Ottawa by storm, paralyzing the City almost overnight, turning parks into encampments and public roadways into parking lots.[2] Residents living near the demonstrations complained of the diesel fumes that polluted the air and the around-the-clock honking that reached noise levels between 90-110 decibels.[3] City services, such as local libraries, vaccination clinics and public transit were also impacted by the hundreds of vehicles that occupied the streets.[4]

Pictures, videos and livestreams of the chaotic atmosphere surfaced all over social media as protesters and residents alike took to Facebook, X (formerly known as Twitter), Instagram and TikTok to depict the general state of lawlessness that was unfolding.[5]

---

1 Canada, Public Order Emergency Commission, *Report of the Public Inquiry into the 2022*

Public Order Emergency (Ottawa: Public Order Emergency Commission, 2023) (Chair:

Hon Paul S. Rouleau) vol 1: Overview, at 38, online: <https://publicorderemergencycommission.ca/files/documents/Final-Report/Vol-1-Report-of-the-Public-Inquiry-into-the-2022-Public-Order-Emergency.pdf> [**perma.cc/2FAE-N7PN**][Rouleau Report].

2 *Ibid* at 14.

3 *Ibid* at 52.

4 *Ibid* at 53-54

5 *Ibid* vol 3, at 165.

On February 14, 2022, the Government of Canada sought to bring the protest to an end by invoking the *Emergencies Act* and declaring a Public Order Emergency.[6] An inquiry was commissioned in its wake by the Governor in Council on April 25, 2022.[7] The inquiry was led by the Honourable Paul S. Rouleau, who investigated the circumstances that led to the invocation of the *Emergencies Act* as well as the following issues, to the extent they affected the declaration of the Public Order Emergency:

- the evolution, goals, leadership, and organization of the convoy movement and border protests, as well as the participants;
- the impact of domestic and foreign funding, including crowdsourcing platforms;
- the impact, role, and sources of misinformation and disinformation, including the use of social media;
- the economic and other impacts of the blockades; and
- the efforts of police and other responders prior to and after the declaration.[8]

The findings of this investigation were published in the *Report of the Public Inquiry into the 2022 Public Order Emergency*.

The report describes the multi-faceted origins of the Freedom Convoy as a culmination of political cynicism and rampant misinformation across social media, among other contributing factors.[9] Importantly, the report goes on to state that social media platforms were the principal means by which the Freedom Convoy was orchestrated. The organizers were able to coordinate their efforts through social media at a rate and scale that was previously unattainable.[10]

When the Freedom Convoy finally came to an end, the police arrested 273 individuals and laid 422 charges from February 18th to the 20th.[11] Some of those individuals have taken their matter to trial, where the evidence being presented against them has been collected from social media websites.[12] Although the matters are

---

6 *Ibid*, vol 1, at 18.

7 *Ibid* at 15.

8 *Ibid* at 15-16.

9 *Ibid* at 27-33.

10 *Ibid* at 29.

11 *Ibid* at 128-129.

12 Laura Osman and Stephanie Taylor "Trial by social media: Court struggles

still making their way through the legal system, no challenges appear to have been raised in relation to a reasonable expectation of privacy in the evidence gathered through social media platforms This has raised several interesting legal questions with respect to the constitutional status of "seizing" evidence from social media without prior judicial authorization. In particular, a key question is whether their actions amount to "searches" within the meaning of section 8 of the *Charter*.[13]

This question arises at a time when the Canadian public is maintaining a greater digital presence online than previously imagined, the result of which has led to new opportunities for law enforcement officials to conduct what are termed "open source investigations." These investigations focus on targeting publicly accessible information on websites such as Facebook, Instagram, and X.

As an example, the Royal Canadian Mounted Police ("RCMP") have begun using software provided by third-party contractors to harness the power of artificial intelligence ("AI") and machine learning in order further their investigations. These companies use AI and machine learning to comb through the internet and harvest publicly available data in troves through a process referred to as "data mining."[14]

This practice has given pause to question the constitutional validity of such "searches." However, before a section 8 *Charter* challenge can be raised to question this practice, one must first

---

under weight of 'Freedom Convoy' evidence," *Toronto Star* (16 September 2023), <online: www.thestar.com> [https://perma.cc/JRG8-VESX].

13 *Canadian Charter of Rights and Freedoms*, s 8, Part 1 of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

14 Royal Canadian Mounted Police, "Babel X platform: Overview and privacy impact assessment initiation" (15 October 2022), online: <www.rcmp-grc.gc.ca> [https://perma.cc/7BXZ-SFJZ]; Babel Street (1 December 2023), online: <www.babelstreet.com> [https://perma.cc/68S7-FU5X]; Tom Simonite," Schools Are Mining Students' Social Media Posts for Signs of Trouble," (28 August 2018), online: <www.wired.com> [https://perma.cc/SH5B-5GNG]; and Andrew Guthrie Ferguson, "The Police Are Using Computer Algorithms to Tell If You're a Threat," (3 October 2017), online: <www.time.com> [https://time.com/4966125/police-departments-algorithms-chicago/].

establish a reasonable expectation of privacy exists in the subject matter being searched.[15]

This paper examines the reasonable expectation of privacy in information posted on social media, beginning with a discussion of the role of machine learning in modern policing in Part I. Part II considers whether a reasonable expectation of privacy exists in this area of the law and notes the difficulty of overcoming the doctrine of abandonment with respect to establishing a privacy interest. In Part III, the Mosaic Theory of the Fourth Amendment ("Mosaic Theory") from *United States v Maynard* is introduced.[16] Broadly speaking, the theory asserts that an individual's constitutional rights may be violated when the investigative steps taken by law enforcement are analyzed cumulatively rather than individually. The impact of the Mosaic Theory on the reasonable expectation of analysis is then assessed before moving onto Part IV, where the issue of abandonment is re-evaluated in light of this theory and recent Supreme court of Canada ("SCC") jurisprudence. Finally, Part V provides the final conclusion of the paper, while Part VI offers suggestions concerning future research efforts along this subject.

At the outset, the issue of abandonment appears to be fatal to establishing a reasonable expectation of privacy. However, by the end of this paper it will become clear that a reasonable expectation of privacy should exist in the information that one publicly shares on social media platforms, albeit a reduced one.

I. MACHINE LEARNING AND MODERN POLICING EFFORTS

The term "machine learning" itself is a catch-all phrase used to encompass a special subset of algorithms that "learn" from the results that it generates.[17] Although machine learning is a complex area of computer science and a subdiscipline of its own, at a basic level, it operates based on an algorithm. An algorithm is trained

---

15 *R v Marakah*, 2017 SCC 59 at paras 51, 83 [*Marakah*].

16 *United States v Maynard*, 615 F.3d 544 (D.C. Cir. 2010) at 549 [*Maynard*]; *United States v Jones*, 132 S. Ct. 945 (2012) [*Jones* SCOTUS]; and *Carpenter v United States*, 128 S.Ct. 2206 (2018) [*Carpenter*].

17 Harry Surden, "Machine Learning and Law" (2014) 89:87 Wash L Rev at 87-89 [Surden].

using a dataset to develop rules that govern the patterns and inferences the algorithm identifies in processing data. These rules then adapt and reconfigure the algorithm in light of new analyzed data.[18]

Machine learning is used for the automated detection of patterns and recurrences in data.[19] It harnesses the power of algorithms and statistical inference methods to identify patterns in data that allow for predictions to be made about future behaviour.[20]

For example a common display of machine learning at work is an email's spam filter.[21] It is programmed to analyze the subject line and keywords contained within an email, as well as monitor the user's behaviour to ascertain which messages are routinely and summarily deleted or marked as "spam."[22] Based on the user's actions, the algorithm begins to mould itself and take shape, revising its rules in anticipation of subsequent emails.

However, machine learning has advanced beyond simply flagging emails as spam and is now used for surveillance purposes, with many private enterprises offering monitor-for-hire services.[23] For example, in the wake of the US Capitol Riots, the Federal Bureau of Investigation ("FBI") turned to private contractors who could offer software monitoring services for social media activity.[24]

---

18 Amy B. Cyphert, "Tinker-ing with Machine Learning: The Legality and Consequences of Online Surveillance of Students" (2020) 20:2 Nev LJ at 462 [Cyphert]; see also Vera Eidelman, "The First Amendment Case for Public Access to Secret Algorithms Used in Criminal Trials" (2018) 34:4 Ga L Rev and Michael L. Rich, "Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment" (2016) 164:4 U Pa L Rev 871 at 883-886 for a more detailed explanation of machine learning.

19 Hugo M. Verhelst, Alexander W. Stannat & Giulio Mecacci, "Machine Learning Against Terrorism: How Big Data Collection and Analysis Influences the Privacy-Security Dilemma" (2020) Science and Engineering Ethic at 2977.

20 Steven M. Bellovin et al, "When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning" (2014) 8:555 New York U J of L & Liberty at 589 [Bellovin et al].

21 Surden, *supra* note 17 at 90.

22 *Ibid*.

23 *Marakah*, *supra* note 15.

24 Aaron Schaffer, "The FBI is spending millions on social media tracking software" (5 April 2022), online: <www.washingtonpost.com> [https://perma.cc/9EKC-GSHG] [Schaffer].

Prior to this, intelligence agencies in the US began to share data among intergovernmental agencies as early as 2011 through "Fusion Centers."

Fusion Centers gather data from several different sources, which included "public- and private-sector databases of traffic tickets, property records, identity-theft reports, drivers' license listings, immigration records, tax information, public-health data, criminal justice sources, car rentals, credit reports, postal and shipping services, utility bills, gaming, insurance claims, data-broker dossiers, and the like."[25] Data is also gathered from information shared online through social media platforms, as well as videos recorded through cameras installed by law enforcement, transportation authorities and private security corporations.[26] This information is collected in an effort to prevent the next terrorist attack.[27] As such, the underlying belief is that there is never enough information in a post 9/11 world.[28] These Fusion Centers continue to remain in operation to this day.[29]

Beyond counterterrorism, machine learning has also been adapted for public school systems, where algorithms are used to monitor the social media feeds of students.[30] Public schools are now retaining private contractors to flag any suspicious posts that an algorithm considers to be a risk of potential violence, hoping to avert the next active shooter incident. These algorithms are also trained to detect any indicators of self-harm or bullying.[31]

In Canada, data mining and the use of machine learning are no longer on the horizon; they are on society's doorstep. The RCMP has publicly disclosed its use of Babel X, a software program supplied by a third-party company that uses artificial intelligence to assist with open source investigations that analyze data from social

---

25 Danielle K. Citron & Frank Pasquale "Network Accountability for the Domestic Intelligence Apparatus" (2011) 62:1441 Hastings LJ at 1451.

26 *Ibid*.

27 *Ibid*.

28 *Ibid*.

29 United States Department of Homeland Security, "Fusion Centers" (17 October 2022), online: <www.dhs.gov> [https://perma.cc/5YME-LHTG].

30 See generally Amy B. Cyphert, "Tinker-ing with Machine Learning: The Legality and Consequences of Online Surveillance of Students" (2020) 20:2 Nev LJ 457.

31 *Ibid* at 469-70.

media platforms.[32] Babel X also has ties to the FBI, who began using their services following the US Capitol Riots, which the Washington Post claimed was foreshadowed on social media.[33] In the aftermath of the Capitol Riots, the FBI sought a program that could obtain intelligence from the social media activity of users on the following platforms: X, Facebook, Instagram, YouTube, LinkedIn, Deep/Dark Web, VK and Telegram as well as 8Kun, Discord, Gab, Parler, Reddit, Snapchat, TikTok and Weibo.[34]

Babel X and similar companies leverage the power of AI in order to scour the internet to identify information shared on websites such as Facebook, Instagram, LinkedIn, X, and other open-source platforms, such as blogs, forums and et cetera.[35] Once an individual has been flagged by the software, law enforcement agencies can proceed to scrape all of the available data from their social media profiles.[36] The liberal government of Canada has contemplated expanding this Orwellian trend at the recommendation of the Rouleau Report by dedicating a specific agency to monitor the use of social media by Canadian society. In particular, recommendation 28 of the report states:

> The federal government, while mindful of concerns related to privacy and government intrusiveness, should examine the question of whether a department or agency of government should have the authority and responsibility to monitor and report on information contained in social media for appropriate purposes and with appropriate safeguards.[37]

This recommendation was made in light of the "intelligence gap" identified in monitoring social media platforms.[38] It stated the Freedom Convoy was foreshadowed in part across social media platforms, where it was being openly discussed and organized before its arrival in Ottawa.[39] However, the report indicates no

---

32 Royal Canadian Mounted Police, "Babel X platform: Overview and privacy impact assessment initiation" (15 October 2022), online: <www.rcmp-grc.gc.ca> [https://perma.cc/7BXZ-SFJZ] [Babel X].

33 Schaffer, *supra* note 24.

34 *Ibid*.

35 Babel X, *supra* note 32.

36 *Ibid*.

37 *Rouleau Report*, *supra* note 1, vol 3 Analysis (Part 2) and Recommendations at 309.

38 *Ibid* at 308-309.

39 *Ibid*.

government department or agency believed it had the requisite authority or even capability to effectively monitor and analyze such data.[40] This is despite the passing of Bill C-59, *An Act Respecting National Security Matters*, which authorizes the Communications Security Establishment Canada ("CSE"), the national cryptologic agency of Canada, to collect publicly available information. In particular, Bill C-59 specifically states:

> The general prohibition against CSE directing its activities at Canadians or persons in Canada would not prevent it from acquiring and using "publicly available information", including information about Canadians (paragraph 24(1)(a)). Such information includes what has been published or broadcast, and what is available to the public upon request or by purchase or subscription (section 2). Considering the information about individuals that can be aggregated, and the things that can be learned from such aggregations using modern technologies and then offered for sale by data-brokers, CSE's acquisition and use of such information, for example, has the potential to affect privacy interests protected by section 8 of the *Charter*.
>
> The following considerations support the consistency of the authority to acquire and use publicly available information. The acquisition and use of information already in the public realm would generally not intrude upon protected privacy interests. Where it would, the level of privacy expectation that could be affected would generally be low by virtue of the fact of prior public exposure. In any event, publicly available information could only be acquired and used for compelling purposes in support of CSE's mandate. Any such information acquired would be subject to appropriate measures to protect privacy (section 25).[41]

The recent attention of social media and its involvement in documenting and foreshadowing large scale events, such as the Freedom Convoy protests and U.S. Capital Riots, suggests law enforcement's use of artificial intelligence in conducting open source investigations will only continue to grow. In the future, search warrants and production orders may be sought based on intelligence acquired through open-source investigations of a user's social media presence, leading courts to consider whether a reasonable expectation of privacy exists in such information. The next section of this paper intends to address the current state of

---

40 *Ibid*.

41 Bill C-59, *An Act Respecting National Security Matters*, 1st Sess, 42nd Parl, 2019 (assented to 21 June 2019).

the law with respect to the reasonable expectation of privacy in information shared online.

II. REASONABLE EXPECTATION OF PRIVACY OVERVIEW

The SCC has outlined on many occasions that a claimant must first demonstrate a reasonable expectation of privacy exists in order to raise a section 8 *Charter* violation.[42] Whether a reasonable expectation of privacy exists depends on the "totality of circumstances," as articulated in *R. v. Edwards*.[43]

The totality of circumstances analysis is guided by the following four avenues of inquiry:

> (1) an examination of the subject matter of the alleged search;
> (2) a determination as to whether the claimant had a direct interest in the subject matter;
> (3) an inquiry into whether the claimant had a subjective expectation of privacy in the subject matter; and
> (4) an assessment as to whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances.[44]

A. An Examination of the Subject Matter of the Alleged Search

The court must take a broad and functional approach in considering the nature of the privacy interests at stake and what information might the state activity tend to reveal in determining the subject matter of the search.[45] This longstanding approach was taken by the Court in *R. v. Spencer* and re-iterated recently in *R. v. Bykovets*, which states a strong claim to privacy exists in relation to the "biographical core of personal information which individuals in a free and democratic society would wish to maintain and

---

42 *Marakah*, *supra* note 15 at paras 51 and 83.

43 *R v Cole*, 2012 SCC 53 at para 39 [*Cole*].

44 *Ibid* at para 40; *R v Edwards*, 1996 CanLII 255 (SCC) [*Edwards*]; *R v Tessling*, 2004 SCC 67 at paras 31-32 [*Tessling*]; *R v Gomboc*, 2010 SCC 55 at paras 18 and 78 [*Gomboc*]; and *R v Patrick*, 2009 SCC 17 at para 27 [*Patrick*].

45 *R v Spencer*, 2014 SCC 43 at paras 25, 26 and 31 [*Spencer*]; *R v Bykovets*, 2024 SCC 6 at para 51 [*Bykovets*].

control from dissemination to the state."[46] The Court elaborated, holding that the analysis is to focus on the privacy of the area or thing being searched, as well as the impact it has on the individual.[47] Further guidance was provided in *Bykovets* when the Court stated the operative component of section 8 cannot be analyzed in relation to only one use of the evidence. Instead, the Court made it abundantly clear that the purpose of section 8 demands an inquiry into "what information the subject matter of the search tends to reveal".[48] The guiding principle at this stage of the analysis is "what were the police really after?"[49]

In determining the subject matter, the SCC in *R. v. Marakah* cautioned the need to carefully define the subject matter when electronic data is involved, a point that was subsequently re-iterated in *Bykovets*.[50] In *Bykovets*, the Court stated this principle is especially pronounced in the context of electronic information, given the capability of computers to store large quantities of data, some of which may even be generated automatically without the user's awareness.[51]

The subject matter of the search can also be classified under three categories: personal privacy, territorial/spatial privacy and informational privacy. This analysis in this paper will be confined to informational privacy, as it bears the most relevance.

Informational privacy has been defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[52] Informational privacy can be further subdivided into three different concepts: (1) privacy as secrecy, (2) privacy as control and (3) privacy as anonymity.[53]

The first concept, privacy as secrecy, is the notion that certain information will be held in confidence or remain a secret, such as

---

46 *Spencer*, *supra* note 45 at para 27.

47 *Ibid* at para 36; *Patrick*, *supra* note 44 at para 32.

48 *Bykovets*, *supra* note 45 at para 34.

49 *Ibid* at para 53.

50 *Marakah*, *supra* note 15 at para 14; *Bykovets*, *supra* note 45 at para 54.

51 *Bykovets*, *supra* note 45 at para 54.

52 *Tessling*, *supra* note 44 at para 23.

53 *Spencer*, *supra* note 45 at para 38.

that between a doctor and patient.[54] In relation to information that is posted on their Internet, individuals are deliberately making information about themselves available in a digital public forum, thereby undermining anonymity.

Next, privacy as control relates to the wider notion that all information about a person is fundamentally their own and as such, they should maintain sovereignty over whether it can be shared.[55] Here, the notion is that individuals who share information about themselves online should be in control of their audience. Finally, privacy as anonymity is the idea that individuals should be free to act in public spaces without being monitored and identified.[56]

With respect to the discussion at hand, an individual who posts their information online cannot expect to maintain their anonymity when they use a public profile to do so. For example, a Freedom Convoy protester who posts a picture of themselves onto Instagram is doing so with the intention of being seen and/or heard by others. This can be likened to the doctrine of abandonment, as will be demonstrated below.

For the purposes of this paper, the subject matter of the search is the publicly shared information that law enforcement officials have access to through social media platforms, such as Facebook, Instagram and X. There are of course several other social networking websites, but the scope of this paper will primarily refer to these three for practical purposes.

B. A Determination as to Whether the Claimant had a Direct Interest in the Subject Matter

In *Edwards*, the SCC stated that an individual's privacy rights must be contravened in order to have standing.[57] Although individuals may deliberately post information online about themselves with the goal of drawing the attention of others, it would be fair to say that even protesters would expect to maintain at least a minimal privacy interest in that information.

---

54 *Ibid* at para 39.

55 *Ibid* at para 40.

56 *Ibid* at paras 42-43.

57 *Edwards*, *supra* note 44 at paras 43 and 45-47.

For example, in *R. v. Patrick*, the SCC found that the accused had a direct privacy interest in the garbage that he was disposing of, as well as the information that it contained, even though it was considered household waste.[58] The Court reasoned that residential trash reveals an "enormous" amount of information and detail about one's lifestyle and behaviour.[59] Included in trash is DNA, personal and private records, such as letters, overdue bills and tax returns, as well as prescription medication bottles, syringes and sexual paraphernalia.[60] This can reveal a substantial amount of information about what the SCC referred to as a resident's "hidden vices."[61] Similarly, in *Marakah*, where the Court dealt with the reasonable expectation of privacy in text messages, the Court found Mr. Marakah had a direct interest in the private text messages he sent to his co-accused, even though he relinquished some control over them once he sent them.[62]

Naturally, one would similarly expect a continuing privacy interest in the information they choose to share about themselves online. Like the garbage that is being removed for disposal and collection, a protester who posts information to social media is likewise parting with the ability to control and regulate access over their information. Yet it would be reasonable to assume that they would wish to keep certain information private and confidential like the contents of a trash bag, especially when it could be used to their detriment. Accordingly, one would expect an individual in these circumstances to have a direct privacy interest in their social media activity.

C. An Inquiry into Whether the Claimant had a Subjective Expectation of Privacy in the Subject Matter

Ordinarily, a claimant would testify to their subjective belief in maintaining a privacy interest. However, the Court in *R. v. Tessling* held a subjective belief in the privacy interest may be presumed by

---

58 *Patrick*, *supra* note 44 at para 31.

59 *Ibid* at para 30.

60 *Ibid* at paras 29-30.

61 *Ibid* at para 30.

62 *Marakah*, *supra* note 15 at para 21.

the court.[63] Further, with respect to informational privacy, the SCC in *R. v. Jones* and *Spencer* have recognized that "all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit", as originally stated in *R. v. Dyment*.[64] This should allow a court to proceed on the basis an individual maintains a subjective expectation of privacy over the information they choose to disclose.

D. An Assessment as to Whether this Subjective Expectation of Privacy was Objectively Reasonable, Having Regard to the Totality of the Circumstances

Whether an individual's subjective expectation of privacy was objectively reasonable involves analyzing a number of different factors. To guide the analysis, the Court in *Bykovets* stated "The question, in all cases, is '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'", citing *Hunter v. Southam*.[65]

While the SCC has chosen not to create an exhaustive list, the Court has stated that the number of factors to be assessed will vary according to the circumstances of each case and be viewed holistically.[66] Such an approach offers the flexibility needed to meet the changing ways in which people communicate.[67] The scope of this paper will likewise endorse that approach and limit the discussion to factors that bear a direct relevance on the reasonable expectation of privacy in information shared on social media.

1. Place where the alleged "search" occurred

The place of the search is relevant to whether one could reasonably hold an expectation of privacy. As one would naturally

---

63 *Tessling*, *supra* note 44 at para 38.

64 *Spencer*, *supra* note 45 at para 40; *R v Jones*, 2017 SCC 60 at para 39 [*Jones* SCC].

65 *Bykovets*, *supra* note 45 at para 44.

66 *Marakah*, *supra* note 15 at para 84; see also *Spencer*, *supra* note 45 at para 17; *Cole*, *supra* note 43 at para 45; *Tessling*, *supra* note 44 at para 32; *Edwards*, *supra* note 44 at para 45.

67 *Marakah*, *supra* note 15 at para 86.

expect, private dwellings attract a heightened reasonable expectation of privacy.[68] Similarly, a conversation held behind the closed doors of one's bedroom is a conversation that one would expect to remain private.[69] However, a conversation that takes place in a crowded room should not attract the same level of constitutional protection.[70] While the Court made these comments in the context of territorial privacy, which does not readily lend itself to electronic conversations, information that is publicly posted on social media websites should attract an expectation of privacy.[71]

In *Marakah*, the SCC classified electronic conversations as existing in a digital sphere where text messaging can create *de facto* private chat rooms between individuals.[72] These "chat rooms" therefore constituted the place searched. The Court accordingly found a reasonable expectation of privacy in text message conversations.[73] It reasoned that a high expectation of privacy would exist in one's own phone, as they have complete control over it. Likewise, the phone of a friend whom the individual is conversing with would carry a lesser expectation of privacy due to the lack of control.[74]

Importantly, the Court went on to find no reasonable expectation of privacy exists if the text message is shared with the public.[75] This was a point that Justice Moldaver agreed with in his concurring opinion, stating "a person may have a reasonable expectation of personal privacy in his or her intimate thoughts about friends, hobbies and romantic interests when they are recorded in a diary, but not when these same thoughts are shared publicly on social media or reality television."[76]

---

68 *R v Kokesch*, 1990 CanLII 55 at 16-18; *R v Feeney*, 1997 CanLII 342 at 43-45; *R v Plant* 1993 CanLII 70 at 291 [*Plant*].

69 *Marakah*, *supra* note 15 at para 26.

70 *Ibid.*

71 *Ibid* at para 27.

72 *Ibid* at para 28.

73 *Ibid.*

74 *Ibid* at para 29.

75 *Ibid.*

76 *Ibid* at para 116.

Under this branch of the analysis, the public accessibility nature of the information undermines finding a privacy interest in the information shared online. However, the Court in *Tessling* stated although the place of the search is important to the objective reasonableness analysis, it is also not determinative, citing Chief Justice Lamer in *Wong*.[77] For example, in that decision, Mr. Tessling's home was scanned using forward-looking infrared ("FLIR") technology, which the Court stated was not the deciding factor. The place of the search must be considered in light of the surrounding context, having regard to the nature and quality of the information that can be gathered through the investigative technique.[78] Accordingly, information a user deliberately shares publicly online should not be determinative of whether constitutional protection ensues. Instead, further analysis should be considered in light of the entire circumstances, even though this factor militates against finding an expectation of privacy.

2. Whether the subject matter was in public view

The SCC has said on numerous occasions that there can be no reasonable expectation of privacy in something that is deliberately exposed to the public. Nor can there be a reasonable expectation of privacy in something that is abandoned in a public place.[79]

The situation at hand can be likened to that of Mr. Patrick, who placed his garbage outside for collection. In *Patrick*, the trash bags were in plain view to anyone passing by in the alleyway to loot in much the same way that can anyone visit Facebook or other social media website to obtain information from a person's profile.[80] In fact, the purpose of posting information on social media is presumably to make it known to others. For instance, the Freedom Convoy protestors who flooded the internet with photos, videos and live streams of the protests did so in an effort to express their disapproval of the government's vaccination requirement and

---

77 *Tessling, supra* note 44 at para 44.

78 *Ibid* at para 45.

79 *Ibid* at para 40; *R v Boersma*, 1994 CanLII 99 (SCC); *R v Stillman*, 1997 CanLII 384 (SCC) at paras 62 and 226 [*Stillman*]; *Baron v Canada*, 1993 CanLII 154 (SCC) at 453 [*Baron*]; *R v Dyment*, 1988 CanLII 10 (SCC) at 435 [*Dyment*]; *R v Monney*, 1999 CanLII 678 (SCC) at para 45; *Patrick*, *supra* note 44 at paras 27, 40, and 53; and *Gomboc*, *supra* note 44 at para 119.

80 *Patrick*, *supra* note 44 at para 63.

garner support. This factor accordingly weighs against finding a privacy interest in the information shared over social networking platforms.

3. Control over / ability to regulate access to the subject matter of the search

Control, ownership, possession and historical use have all been relevant to the analysis of whether an expectation of privacy was reasonable.[81] However, control is not determinative of a reasonable expectation of privacy, nor is the lack of control fatal to establishing a privacy interest.[82]

With respect to information shared on social media, the individual undoubtedly loses control over the ability to regulate access, use and possession once they make their post publicly available. However, in *Marakah* the Court found people deliberately choose what and how much information they wish to share with others in the context of text messaging.[83] The Court also found that the individual sharing their information via text messaging may expect the contents of their messages to remain safe from state scrutiny, even if they lose exclusive control over it.[84]

In setting out its reasons, the SCC rejected the Crown's argument that Mr. Marakah lost control over the electronic conversation due to the possibility that it could be reproduced and shared with third parties.[85] The Court held that the risk of disclosure to third parties does not alter the analysis.[86] Specifically, the Court stated that accepting the risk that the recipient could disclose the details of the conversation is not the same as accepting the risk that the state will intercept the details of the conversation without disclosure.[87]

---

81 *Marakah*, *supra* note 15 at para 38; see also *Cole*, *supra* note 43 at para 51; *Edwards*, *supra* note 44 at para 45.

82 *Marakah*, *supra* note 15 at para 38.

83 *Ibid* at para 39.

84 *Ibid* at para 41; see also *Jones* SCC, *supra* note 64 at para 45; and *Cole*, *supra* note 43 at para 54.

85 *Ibid* at para 40.

86 *Ibid*.

87 *Ibid*.

For greater clarity, the Court held that even when the technological reality robs an individual of the ability to exclusively control their personal information, they may still reasonably expect that information to remain out of the state's hands.[88] In *Jones* SCC, the companion case to *Marakah*, the Court arrived at a similar conclusion, when it dealt with the reasonable expectation of privacy of text messages stored on a telecommunication provider's network.[89] In that decision, the Court found that Mr. Jones retained a privacy interest in the text message records stored by his service provider, despite losing control upon sending them.[90] The Court reasoned that the only way one could retain control is to completely abstain from using the telecommunication provider's services.[91] However, that was held not to be a meaningful choice that can be reconciled with the purposive approach to section 8 of the *Charter*.[92] As the Court described it, "Canadians are not required to become digital recluses in order to maintain some semblance of privacy in their lives."[93]

Similarly, individuals who share information publicly on social media should not be forced to withdraw from participating in the digital public square in order to maintain a privacy interest in their information. As the Court stated, such a demand would be inconsistent with the purposive approach to section 8 of the *Charter*. Although these individuals accept the risk that the information they share online could be copied and reproduced elsewhere or retained by the website host, they cannot be said to accept the greater risk that the state will intercept the data to their detriment. Simply forfeiting control and access of the subject matter does not mean they agree to relinquish any and all expectations of privacy in what they choose to share online.

Support for this notion can be found in an early article on data mining and privacy, in which Professor Wayne Renke (now the Honourable Justice Renke) discussed the possibility of state agents accessing publicly available information that was only intended for

---

88 *Ibid* at para 41.

89 *Jones* SCC, *supra* note 64 at para 45.

90 *Ibid*.

91 *Ibid*.

92 *Ibid*.

93 *Ibid*.

use by members of the public.[94] In particular, he stated that there is a big difference between a member of the public accessing the information as opposed to an agent of the state.[95] While the act of retrieving the information may be the same, Professor Renke argued the former was distinguished on the basis that it does not entail any potential risk of jeopardy whereas the latter does.[96]

4. Whether the subject matter had been abandoned

The Supreme Court of Canada has long held that abandonment is fatal to a reasonable expectation of privacy since *Dyment* and *R. v. Stillman*.[97] In *Stillman*, the Court specifically held section 8 is not engaged when an individual discards property.[98] Since then, the Court has continued to uphold that position in *Patrick*, where it found Mr. Patrick no longer harboured any objectively reasonable privacy interest when he placed his garbage bags at the property line for collection.[99]

More recently, that position was reiterated by Justice Moldaver in *Marakah*, albeit in a concurring opinion. In that decision, he stated "when an individual assumes the risk of public access, they are equally assuming the risk of state access. That is why the risk of publicity has featured prominently in so many of this Court's decisions applying the reasonable expectation of privacy test."[100] Although this comment was made in response to the Chief Justice's reasons for decision, it nevertheless relates to the doctrine of abandonment.

However, abandonment is determined by the facts of each case. The question is whether the individual asserting a section 8 *Charter* breach has behaved in a manner that an objectively reasonable and independent observer could conclude a reasonable

---

94 Wayne N Renke, "Who Controls the Past Now Controls the Future-Counterterrorism, Data Mining and Privacy" (2006) 43:3 Alta L Rev at 802.

95 *Ibid*.

96 *Ibid*.

97 *Dyment*, *supra* note 79 at 435; see also generally *R v Boersma*, 1994 CanLII 99 (SCC); *Stillman*, *supra* note 79 at paras 62 and 226; *Baron*, *supra* note 79 at 453; and *R v Monney*, 1999 CanLII 678 (SCC) at para 45.

98 *Stillman*, *supra* note 79 at paras 62, 223 and 274.

99 *Patrick*, *supra* note 44 at para 63.

100 *Marakah*, *supra* note 15 at para 162.

expectation of privacy continued to exist in the totality of the circumstances.[101]

In *Patrick*, the SCC found abandonment of residential garbage is a function of both location and intention.[102] The Court held there is no doubt that Mr. Patrick intended to abandon the physical objects contained in the garbage.[103] However, the question was whether he retained a reasonable continuing privacy interest in the information that the garbage disclosed.[104] The Court found the idea of extending section 8 *Charter* protection to his garbage, to the point where it disintegrates into indecipherable material to be "too extravagant to contemplate."[105] It reasoned that doing so would effectively extend constitutional protection to the municipal disposal system, which is far beyond the confines of a private dwelling house.[106]

The question then became where the Court should draw the line to denote when constitutional protection ends.[107] That line was ultimately determined by Mr. Patrick's actions, rather than the conduct of the garbagemen, police or anyone else who may have been involved in the collection of his trash.[108]

However, in the current situation, a user who shares information on social media is effectively abandoning it in the public sphere. By publicly sharing it on the internet, they are deliberately attempting to reach a wider audience beyond those who would ordinarily be privy to it. Thus, an analogy can be drawn with *Patrick*, where the idea of taking garbage out for disposal and collection can be equated to posting information on the web.

While personal information shared on social media is in no way literal trash, finding a continuing privacy interest after something has been made publicly available would be, as the SCC said, "too extravagant to contemplate." For example, a Freedom Convoy protester who deliberately exposes information to the

---

101 *Ibid* at para 25.

102 *Ibid* at paras 54, 55 and 62.

103 *Ibid* at para 54.

104 *Ibid*.

105 *Ibid*.

106 *Ibid*.

107 *Ibid*.

108 *Ibid*.

public extinguishes any continuing privacy interest they may have had. The SCC has a long line of authorities which support the notion that abandonment is fatal to establishing a reasonable expectation of privacy.[109] Moreover, in addressing the expectation of privacy in text messages in *Marakah*, the SCC stated "this case does not concern, for example, messages posted on social media, conversations occurring in crowded Internet chat rooms, or comments posted on online message boards."[110]

Accordingly, an individual forfeits any continuing privacy interest in their information once they share it online. It no longer becomes objectively reasonable to harbour a continuing privacy interest in the data, as it has been "digitally abandoned." Law enforcement officials can then collect the data in the same manner that Mr. Patrick's garbage was retrieved.[111]

No reasonable expectation of privacy should exist as a result of this factor alone. However, when the doctrine of abandonment is re-analyzed in light of the Mosaic Theory of the Fourth Amendment and recent SCC jurisprudence, it will become clear that abandonment should not be fatal to a privacy interest. At the very least, a reduced expectation of privacy should be found.

5. Invasiveness of the technique or technology

The intrusiveness of an investigating technique is also a factor in the privacy interest analysis.[112] However, discussion of this factor has revolved around physical searches where the person's bodily integrity was at stake. For example, pat-downs, strip searches, cavity searches and bodily samples swabs all involve invasive searches of varying degrees.[113]

With respect to digital communication, continuous monitoring of incoming and outgoing text messages was held by the SCC to be subject to high standards that require prior judicial

---

109 See cases referenced at *supra note* 97.

110 *Marakah, supra* note 15 at para 55.

111 *Patrick, supra* note 44 at paras 55 and 63.

112 *Tessling, supra* note 44 at para 50; See also *R v Wong*, 1990 CanLII 56 (SCC) at 44 [*Wong*]; Thomson Newspapers Ltd v Canada (Director of Investigation and Research, Restrictive Trade Practices Commission), 1990 CanLII 135 (SCC) at 496 and 594; and *Plant*, *supra* note 68 at 295.

113 See generally *R v Golden*, 2001 SCC 83; *R v Saeed*, 2016 SCC 24; *Stillman, supra* note 79.

authorization.[114] For example, in *R. v. Duarte*, the interception of private communication by the state was found to be a serious intrusion into the privacy rights of those affected.[115]

In the context of technologically aided searches, the Court in *Tessling* dealt with the constitutional validity of aerial searches conducted using FLIR technology that allowed the police to detect heat signatures emanating from the external surfaces of a home.[116] In that decision, the Court drew on Justice La Forest's comment in *Wong* regarding technology, where he stated "we must always be alert to the fact that modern methods of electronic surveillance have the potential, if uncontrolled, to annihilate privacy."[117] However, the Court qualified that statement by stating the technology must be assessed with respect to its current capabilities.[118]

In the present case however, accessing information that is shared publicly on a social media network is hardly invasive. Retrieving such information is akin to the collection of disposed residential trash, which the Court in *Patrick* has already determined carries no privacy interest.[119] Further, society's interest in maintaining privacy must be balanced with the legitimate goals of law enforcement, a point that was expressed by the Court in *Hunter v. Southam*.[120]

However, the issue here is not the invasive nature of the technique, it is the commercial scale at which the data is being harvested. Artificial intelligence offers several advantages in its ability to identify and analyze relevant data about a potential target that cannot be rivaled by human endeavours. This has the potential, as Justice La Forest put it, "to annihilate privacy" when the artificially intelligent software is fed information directly from a suspected individual's social media profiles, which can be

---

114 *R v TELUS Communications Co.*, 2013 SCC 16 at paras 1, 5 and 32.

115 *R v Duarte*, 1990 CanLII 150 (SCC); see *Wong, supra* note 112 at 47-49; and *R v Tse*, 2012 SCC 16 at para 17)

116 See generally *Tessling, supra* note 44.

117 *Ibid* at para 54.

118 *Ibid* at para 55.

119 See generally *Patrick*, *supra* note 44.

120 *Hunter et al v Southam Inc*, [1984] 2 SCR 145.

aggregated to make inferences that would not otherwise be discernable to the human mind.[121]

In *Bykovets*, the Court acknowledged this possibility when it found even mundane information could reveal far more about an individual when the data is aggregated with other sources of intelligence.[122] Accordingly, the problem does not lie with the invasive nature of machine learning and data mining, rather its ability to do so with great efficiency and draw unforeseen inferences in the data. This factor should accordingly weigh in favour of finding an expectation of privacy.

6. Nature of the information

The nature of the information being sought, and any reasonable expectations of privacy were discussed in *Tessling*, where the Court referred to Justice Sopinka's dictum in *R. v. Plant*. In *Plant*, Justice Sopinka found documents of a personal and confidential nature that tend to reveal details about an individual's biographical core should attract constitutional protection, stating:

> [I]n order for constitutional protection to be extended, the information seized must be of a "personal and confidential" nature. In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[123]

Likewise, information shared to social media that could potentially reveal intimate details of one's life should attract constitutional protection, even if publicly available. For example, one may share photographs of their family, or information about where they reside, what profession they carry on, what political party they support, whether they are a person of faith or a member of a minority class. The personal and intimate nature of such information goes to the biographical core of information that Justice Sopinka envisioned in *Plant*. This weighs in favour of finding a privacy interest.

---

121 *Wong*, *supra* note 112 at 43.

122 *Bykovets*, *supra* note 45 at para 65.

123 *Tessling*, *supra* note 44 at para 60, emphasis added.

E. CONCLUSION OF PART I

There is no dispute that a user has a direct interest in the data they choose to share with others over social media. Nor is there any doubt that a subjective expectation of privacy could be presumed in this hypothetical scenario.

However, the subjective expectation of privacy must be objectively reasonable in light of the factors discussed above in order for a court to find a privacy interest exists.[124] In this scenario, control and access, the degree of intrusion of the technique used and the nature of the information all militate in favour of finding a reasonable expectation of privacy in the totality of circumstances.

By contrast, the place of the search, the public accessibility of the matter, and most importantly, the abandonment of the information weigh against a reasonable expectation of privacy. As the SCC has repeatedly indicated, no reasonable expectation of privacy exists in something that is intentionally exposed to the public or abandoned in a public place.[125]

In the totality of circumstances, no reasonable expectation of privacy should be found with respect to data that is intentionally shared online with the public due to the doctrine of abandonment. However, a different conclusion should be reached in light of the Mosaic Theory of the Fourth Amendment and the Supreme Court of Canada's recent decision in *Bykovets*.

III. THE MOSAIC THEORY OF THE FOURTH AMENDMENT

In *United States v Maynard*, the D.C. Circuit Court of Appeal Court introduced what scholars have termed the "Mosaic Theory of the Fourth Amendment."[126] The theory offers claimants a new approach to finding a violation of the Fourth Amendment of the U.S. Constitution, which protects against unreasonable search and seizure in similar fashion to section 8 of the *Charter*.[127]

---

124 *Marakah*, *supra* note 15 at paras 10-12.

125 *Supra* note 97.

126 See generally Orin S Kerr, "The Mosaic Theory of the Fourth Amendment" (2012) 111:311 Mich L Rev [Kerr].

127 US Const amend IV.

Historically, to find an infringement of the Fourth Amendment, the Court would need to find a violation in the sequential investigative steps taken by law enforcement.[128] If no individual step in the sequence constituted a search, then there was no infringement of the Fourth Amendment.[129] For example, in *United States v. Katz*, the Supreme Court of the United States ("SCOTUS") outlined one of the possible ways a Fourth Amendment violation could be established. Justice Harlan, in his concurring opinion outlined the following two-step test that has now been widely adopted:

> (1) was there a subjective expectation of privacy? and
> (2) was the subjective expectation one that society is prepared to recognize as reasonable?[130]

However, the US Court of Appeals for the District of Columbia Circuit ("DC Circuit") introduced an additional approach to establishing a Fourth Amendment violation in *Maynard*. This new approach was premised the Mosaic Theory, which conceptualizes the investigative actions of law enforcement as a collective sequence of actions for the purposes of determining whether an infringement has occurred.[131] The advantage to the Mosaic Theory is that it allows the court to find a Fourth Amendment violation in situations that would not otherwise have amounted to a breach if the investigative steps of lawful enforcement were all constitutionally compliant in isolation.[132]

The theory is based on the notion that aggregated data, even if innocuous, reveals far more about an individual when viewed collectively like a mosaic than it would if the data gathered were examined individually.[133] According to Mosaic Theory, each step of the investigation constitutes a "tile" in the mosaic.[134] When a sufficient number of "tiles" are gathered over time and aggregated together, the mosaic reveals a "big picture" of who the individual

---

128 Kerr, *supra* note 126 at 312.

129 *Ibid*.

130 See generally *Katz v United States*, 389 US 347 (1967) at 361.

131 Kerr, *supra* note 126 at 313 (see also *Maynard*, *supra* note 16; *Jones* SCOTUS, *supra* note 16 at 562).

132 *Ibid*.

133 Bellovin et al, *supra* note 20 at 556.

134 *Ibid* at 562.

is and what their lifestyle and behavioural habits are.[135] With this big picture, the theory claims that far wider reaching inferences can be made about the individual than what can be gleaned or understood from individual observations made independently of one another.[136] Stated simply, Mosaic Theory considers the whole greater than the sum of its parts.[137]

To illustrate this idea, consider the facts in *Maynard*. Mr. Maynard was the manager of a nightclub owned by his co-accused, Mr. Jones. .[138] The two were investigated by a joint federal and local narcotics task force for suspected crack and cocaine trafficking.[139] The investigation relied on several investigative techniques, such as wiretaps, informants, surveillance, and cameras directed at the front door of the nightclub.[140] However, the Fourth Amendment violation relating to the Mosaic Theory emerged from the global position system ("GPS") tracking device that was installed on a vehicle operated by Mr. Jones.[141]

Although a search warrant was obtained to install the device, the warrant was not executed within the authorized time.[142] The warrant permitted the agents to install the tracking device within 10 days of the warrant's issuance, however installation was not carried out until the 11th day.[143] While the device was operating, it recorded the location of Mr. Jones's vehicle over the course of 28 days, generating 2,000 pages of location data. Collectively, this data helped indicate where Mr. Jones met his co-conspirators, as well as identify the location of his "stash house" where the drugs and cash proceeds were held.[144]

When the legality of the tracking device was challenged, the DC Circuit Court found a Fourth Amendment infringement based on the idea that the aggregated data revealed more about the

---

135 *Ibid* at 556.

136 *Ibid* at 562.

137 *Ibid*.

138 *Maynard*, *supra* note 16 at 549.

139 *Ibid*.

140 *Ibid*; *Jones* SCOTUS, *supra* note 16 at 948.

141 *Jones* SCOTUS, *supra* note 16 at 948.

142 *Ibid*.

143 *Ibid*.

144 *Ibid* at 948-49.

individuals than would otherwise be possible.[145] However, when the matter reached the SCOTUS under the name of *United States v Jones*, the matter was decided without resorting to the Mosaic Theory.[146] Justice Scalia, writing for the majority, held that the late installation of the GPS device constituted an illegal search due to the trespass of the vehicle.[147]

Although the matter was decided on different grounds, Justices Alito and Sotomayor wrote concurring opinions which expressed support for the Mosaic Theory. In Justice Alito's opinion, which was joined by Justices Ginsberg, Breyer and Kagan, he ultimately found the extended GPS surveillance of the car constituted a search under the *Katz* approach.[148] However, his concurring opinion nevertheless supported the Mosaic Theory. Consider the following excerpt:

> [T]he use of longer-term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.[149]

Similarly, Justice Sotomayor's concurring opinion examined "whether people reasonably expect that their movements will be recorded and aggregated in such a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[150] She then also went on to comment on the implications of even short-term GPS monitoring, stating:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. See, e.g., *People v. Weaver*, 12 N. Y. 3d 433, 441–442, 909 N. E. 2d 1195, 1199 (2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-

---

145 *Maynard*, *supra* note 16 at 561-62.

146 *Jones* SCOTUS, *supra* note 16 at 951-54.

147 *Ibid*.

148 *Ibid* at 957-64.

149 *Ibid* at 964.

150 *Ibid* at 956.

> the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on"). The Government can store such records and efficiently mine them for information years into the future.[151]

Since *Jones*, the Mosaic Theory re-surfaced in *United States* v *Carpenter*, where SCOTUS grappled with the issue of cell-site data.[152] The Court ultimately found a Fourth Amendment violation, when it said the following, citing Justice Sotomayor's opinion in *Jones* SCOTUS:

> Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the timestamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations."[153]

As discussed, the GPS tracking device in *Maynard/Jones* SCOTUS allowed the police to make inferences that would not be otherwise possible if the police simply relied on one investigative technique. However, when the device was able to constantly monitor the vehicle's location over several weeks, the data revealed far more than simply Mr. Jones's whereabouts when it was combined with the rest of the evidence gathered by the police. Collectively, the data revealed the depth and location of his drug trafficking network, as well as who his associates were.[154]

Although the Mosaic Theory originates out of the United States, the SCC's recent decision in *Bykovets* lends credence to the idea that the whole is greater than the sum of its parts.[155] In *Bykovets*, the Court considered whether a reasonable expectation of privacy exists in one's Internet Protocol address ("IP address").[156] An IP address is a unique number that is attached to a user's specific online activity. It is essential to surfing the web and is controlled by the user's Internet Service Provider ("ISP").[157] IP addresses also connect internet activity to a specific location. As a result, the Court found IP addresses capable of revealing deeply

---

151 *Ibid*.

152 See generally *Carpenter*, *supra* note 16.

153 *Ibid* at 2218.

154 *Jones* SCOTUS, *supra* note 16 at 948-49.

155 *Bykovets*, *supra* note 45 at paras 65 and 74.

156 *Ibid* (see generally).

157 *Ibid* at para 4.

personal and private information, including the identity of the user, when it said the following in relation to the heightened danger of combining a user's IP address with other intelligence gathered by law enforcement:

> Correlated with other online information associated with that IP address, such as that volunteered by private companies or otherwise collected by the state, an IP address can reveal a range of highly personal online activity. And when associated with the profiles created and maintained by private third parties, the privacy risks associated with IP addresses rise exponentially. The information collected, aggregated and analyzed by these third parties lets them catalogue our most intimate biographical information.[158]

The Court elaborated on this point, recognizing that aggregating data creates "synergies" that can be analyzed to reveal new facts about a person, which includes facts that were previously unknown to the individual when they shared the information.[159] For example, it stated even "information that may at first blush appear mundane and outside of the biographical core may be profoundly revealing when situated in context with other data points".[160]

Although these findings were made in the context of IP addresses, they nevertheless support the Mosaic Theory. Once data is collected from multiple sources and grouped together for analysis, new inferences and connections can be made about the individual. Similarly, in *R. v. Ramelson*, a child luring case dealing with issues of entrapment through an internet advertisement, the SCC recognized that "Information once revealed to the state in pieces can now be "compiled, dissected and analyzed to lend new insights into who we are as individuals or populations".[161]

In *Jones* SCOTUS/*Maynard*, GPS, a fairly ubiquitous piece of technology, was used to uncover the extent of Mr. Jones's drug trafficking operation. However, if the RCMP were to carry out a similar drug investigation using artificial intelligence software, it would be more than capable of processing a subject's movements. In addition to simply tracking the target's location, the software could crawl across the individual's social media presence to collect data about their "likes", comments and re-posted media, and what

---

158 *Ibid* at para 9.

159 *Ibid* at paras 65 and 74.

160 *Ibid* at para 74.

161 *R v Ramelson*, 2022 SCC 44 at para 48.

they choose to upload or share themselves. The data can then be fed to an algorithm to reveal hidden patterns and trends that investigators were previously ignorant of. These inferences could then provide the foundational basis for a search warrant or production order to be obtained.

If members of Canadian society were privy to the technology that law enforcement possesses and its capabilities, it would be reasonable to assume they would not willingly share information with the public, knowing it could bring them into subsequent jeopardy. This is especially true if they became aware of the software's capability to compile and analyze even innocuous data. As a result, this should fundamentally alter the reasonable expectation of privacy analysis and whether "digital abandonment" is truly fatal to establishing a privacy interest.

IV. ABANDONMENT REVISITED

The SCC has stated no reasonable expectation of privacy can exist in something that is deliberately exposed to the public or abandoned in a public place, especially with respect to messages posted on social media.[162] However, these rulings were made based on the technology that existed at the time. Since then, AI software has advanced and is now capable of providing law enforcement officials with a deeper understanding of a target's lifestyle choices and behavioural patterns. The law simply no longer reflects the true capabilities law enforcement's contemporary investigative tools.

Although the posting of information online can be conceptualized as a form of "digital abandonment", the Court in *Marakah* held there are different levels of risk associated with text messaging that the user is prepared to accept. In the context of text messages, the Court found that an individual who sends text messages is assuming the risk that those messages may be shared with others without their consent.[163] However, the Court also went on to state that accepting such a risk did not mean the user also agreed to the greater peril of permitting state scrutinization of the

---

162 *Marakah*, *supra* note 15 at para 55.

163 *Ibid* at para 40.

data.[164] As the Court described it, agreeing to the state's use of the information against them represents a risk of an entirely different order and magnitude that they did not agree with:

> To accept the risk that a co-conversationalist could disclose an electronic conversation is not to accept the risk of a different order that the state will intrude upon an electronic conversation absent such disclosure. "[T]he regulation of electronic surveillance protects us from a risk of a different order, i.e., not the risk that someone will repeat our words but the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words": *Duarte*, at p. 44. Therefore, the risk that a recipient could disclose an electronic conversation does not negate a reasonable expectation of privacy in an electronic conversation.[165]

The degree of risk that an individual is willing to accept when they send text messages bears even more relevance in the context of social media use. In light of the wider permissible inferences that can be made with the use of artificial intelligence, one would argue that the aggregated information represents a risk of an entirely different magnitude and fundamentally alters the risk equation.

As a result, social media users would likely not agree with the state's use of such information against them. For example, if Freedom Convoy protestors understood the information they shared online could be accumulated and analyzed to reveal personal and intimate details about their lives, then it is highly unlikely they would have continued to use social media to facilitate the movement and attract support.

Consider for example an individual who posts location-tagged photographs or videos that depict their whereabouts. Tracking this information over time would be tantamount to following the individual's movements with the aid of a GPS device. Such information could be used to suggest personal affiliations with stigmatized activities and/or demographics in an area they visited. Alternatively, it could implicate their involvement in a crime that took place nearby. In the context of the Freedom Convoy, protesters wanted to express their political dissatisfaction with the current state of the government through social media rather than subject themselves to the Orwellian eyes of the state who may be seeking to place them at the scene of a crime.

---

164 *Ibid*.

165 *Ibid*.

The Court in *Bykovets* alluded to this point when it said "we would not want the social media profiles we linger on to become the knowledge of the state".[166] Although this was stated in the context of anonymous internet usage, the Court still recognized society's need to keep intimate versions of themselves from being outed by the collection of recently used search terms *en masse* by law enforcement.[167]

The SCC's comments in *Spencer* also bear particular relevance here. In *Spencer*, the Court found privacy as anonymity was particularly important to internet usage.[168] Drawing on a finding by Justice La Forest made in *Wise*, the Court stated "[i]n a variety of public contexts, we may expect to be casually observed, but may justifiably be outraged by intensive scrutiny. In these public acts we do not expect to be personally identified and subject to extensive surveillance, but seek to merge into the 'situational landscape.'"[169] The Court then went on to state that simply because someone leaves the privacy of their home to enter a public space does not mean that they have forfeited all their privacy rights, even though they retain a reduced amount of control over who observes them in public.[170]

Applying that concept to information shared over social media, one should expect to retain a privacy interest in the matter and as Justice La Forest stated, "merge into the 'situational landscape'".[171] This is even more true if the power of artificial intelligence can be harnessed to reveal hidden connections between the various sources of data from across the internet.

Finally, the Court in *Spencer* left the possibility open that anonymity could constitute the foundation of a privacy interest that engages section 8 of the *Charter*, referencing a quote by Appellate Justice Doherty of the Ontario Court of Appeal in *Ward*.[172] However, the Court qualified this statement by saying it

---

166 *Bykovets*, *supra* note 45 at para 67.

167 *Ibid*.

168 *Spencer*, *supra* note 45 at para 41.

169 *Ibid* at para 44.

170 *Ibid* at para 44.

171 *Ibid*.

172 *Ibid* at para 48.

would be contingent upon the totality of the circumstances.[173] In the totality of the current circumstances, the potentially permissible inferences of accumulated data should constitute the basis of a privacy interest that engages section 8 of the *Charter*. AI and the use of social media could form the basis of such a privacy interest, given that AI software could allow law enforcement officials to effectively peer into the lives of social media users through an analysis of their data, whether they were aware of it, much less consenting to it.

Indeed, in *Bykovets*, the Court found the digital landscape of privacy has evolved due to third-party websites that operate beyond the scope of the *Charter*'s protection when it said the following:

> the Internet has fundamentally altered the topography of informational privacy under the *Charter* by introducing third-party mediators between the individual and the state — mediators that are not themselves subject to the *Charter*. Private corporations respond to frequent requests by law enforcement and can volunteer all activity associated with the requested IP address. Private corporate citizens can volunteer granular profiles of an individual user's Internet activity over days, weeks, or months without ever coming under the aegis of the *Charter*. This information can strike at the heart of a user's biographical core and can ultimately be linked back to a user's identity, with or without a *Spencer* warrant. It is a deeply intrusive invasion of privacy. [174]

The Court went on to reiterate the purpose of section 8 of the Charter should focus on a searches' potential to reveal personal or biographical core information, not that it will reveal such information.[175]

Although the approach taken in *Bykovets* to resolve the issue does not mirror the Mosaic Theory, the Court's reasons ultimately echo the same underlying sentiment.[176] Both focus on how information can be gathered about an individual without a warrant and how such information can be used reveal more about them when analyzed in tandem with other sources of data.

V. FINAL CONCLUSION

---

173 *Ibid*.

174 *Bykovets*, *supra* note 45 at para 10.

175 *Ibid* at paras 7, 13, 42, 55, 56, and 57.

176 *Ibid*, see generally.

Whether the information that one shares online is sufficiently private and confidential to merit constitutional protection will ultimately come down to the facts of a particular case and whether a reasonable expectation of privacy can be established. Social media users have a direct interest in maintaining privacy over the information they choose to share with others, and that subjective expectation of privacy is objectively reasonable in the totality of circumstances.

Personal information that reveals the intimate details about one's lifestyle and behaviour should attract constitutional protection. However, the doctrine of abandonment has proven to be fatal in establishing privacy interests. When applied to the digital context, information that is posted publicly online can be conceived as digital abandonment and likened to the disposed garbage in *Patrick* that was ultimately held to retain no continuing privacy interest.[177]

On the contrary, the highest levels of court in this country and the US have concluded that even seemingly benign information, such as GPS data, is capable of revealing personal and intimate details about a person's lifestyle when amassed in sufficient quantity.[178] This is particularly alarming when AI and data mining software are brought into the discussion. At a click of a few buttons, an open-source investigation can be conducted where AI software can cull the data from millions of people's social media profiles and use it in furtherance of obtaining a search warrant or production order against them. Such a feat was previously impossible to achieve by human endeavours alone.

AI offers a depth and breadth of investigative assistance that allows law enforcement to take advantage of vulnerable information that is shared over social media platforms. This outright wholesale harvesting of data upsets the balance between seeking to uphold the legitimate objectives of law enforcement and ensuring the constitutional rights of Canadian society are respected. Individuals should not have to contemplate the risks of sharing seemingly harmless information online out of fear it could lead to subsequent jeopardy. This should constitute a basis to reconsider the issue of abandonment in favour of finding a privacy interest.

---

177 See generally *Patrick*, *supra* note 44.

178 Cyphert, *supra* note 18 at 459.

An expectation of privacy is not viewed on an all-or-nothing basis.[179] In *Tessling*, the Court provided a hierarchy of places that attract privacy interests of varying degrees. Although the Court held that section 8 of the *Charter* protects people, not places, it did go on to find that the place searched serves as "an analytical tool to evaluate the reasonableness of a person's expectation of privacy."[180]

In these circumstances, personal information shared on social media should attract a reasonable expectation of privacy, albeit a reduced one given the public accessibility of the information. This would ensure prior judicial authorization is sought.

The police routinely apply and obtain warrants for different search sites in order to respect the differing territorial privacy interests at stake.[181] As such, imposing an additional search warrant requirement for open-source investigations relating to a target's social media profiles would not result in an onerous burden to satisfy

Privacy is a doorbell that cannot be unrung once breached. Prior judicial authorization is required to ensure a measure of judicial oversight.

VI. AREAS OF FUTURE RESEARCH

Until such time that a Court determines whether a reasonable expectation of privacy exists in the information users share online, future scholars and researchers alike should consider whether a reasonable expectation of privacy exists with respect to data that a government purchases from a third-party. Isabelle Canaan discussed this possibility in an article that examined the US government's purchase of data from a mobile application known as Muslim Pro.[182] This raises an interesting issue as to whether section 8 of the *Charter* would be engaged if law enforcement agencies attempted to replicate this process in Canada.

---

179 *Tessling*, *supra* note 44 at para 22.

180 *Ibid*.

181 *Bykovets*, *supra* note 45 at para 85.

182 See generally Isabelle Canaan, "A Fourth Amendment Loophole?: An Exploration of Privacy and Protection Through the Muslim Pro Case" (2022) Colum HRLR.

Similarly, Justice Côté, writing for the dissent in *Bykovets*, briefly mentioned the constitutional uncertainty surrounding third-parties that provide unsolicited information to law enforcement officials.[183] Academics may find this scholarly endeavour worthy of pursuit.

Alternatively, future publication could focus on the common law doctrine of plain view, and whether it could defeat a reasonable expectation of privacy in information shared on social media. The Court has already stated that objects in plain view do not attract a reasonable expectation of privacy, however, much like abandonment, this requires further reconsideration in light of recent Supreme Court jurisprudence and the Mosaic Theory.[184] As such, subsequent research should examine whether the plain view doctrine could be adopted across digital dimensions for a court to find evidence in digital plain sight.

---

183 *Bykovets*, *supra* note 45 at para 135.

184 See cases referenced at *supra* note 79.