Canadian Journal of Law and Technology

Volume 19
Number 2 *Technology-facilitated Gender-based Violence*
Article 9

1-2022

Bringing Section 8 Home: An Argument for Recognizing a Reasonable Expectation of Privacy in Metadata Collected from Smart Home Devices

Ana Qarri
McGill University, Faculty of Law

Bringing Section 8 Home: An Argument for Recognizing a Reasonable Expectation of Privacy in Metadata Collected from Smart Home Devices

Ana Qarri[*]

Abstract

Internet of Things devices (also known as smart home devices) are a fast-growing trend in consumer home electronics. The information collected from these devices could prove very useful to law enforcement investigations. These individual pieces of metadata — the collection of which might appear harmless on its face — can be highly revealing when combined with other metadata or information otherwise available to law enforcement. This article builds an argument in favour of recognizing a reasonable expectation of privacy in metadata collected from smart home devices under section 8 of the Canadian Charter of Rights and Freedoms. This article presents a two-step argument in favour of recognizing the collection of smart home metadata as a "search" under section 8. First, it builds on case law on house perimeter searches to argue that — in the case of smart home devices — the collection implicates both territorial and informational privacy interests. Second, the article argues that metadata, on their own, are pieces of information that attract a reasonable expectation of privacy. R. v. Spencer[1] *was not the final word on the question of inferences. Several section 8 cases decided by the Supreme Court of Canada, and the R. v. Orlandis-Habsburgo*[2] *decision, point to the willingness of courts to engage with the complex topic of data processing. They also point to the need to return to the values that underlie section 8 of the Charter with the goal of clarifying its approach to predictions and probabilities as information outcomes that deserve constitutional protection.*

INTRODUCTION

The home has traditionally attracted high levels of protection from state interference. *Entick v. Carrington,*[3] decided in 1765, is the first dispute in the common law that implicated privacy interests in the home. Three Messengers to the King forcefully entered the home of John Entick, a political dissident, to seize his writings. Entick's action against the Messengers defined the reach of executive power in the common law tradition, but the judgment also recognized that trespass into Entick's home was an infringement of liberty.[4] The status of

---

[*] Ana Qarri is a JD/BCL (2021) candidate at the McGill University Faculty of Law.

1 *R. v. Spencer*, 2014 SCC 43, 2014 CarswellSask 342, 2014 CarswellSask 343 (S.C.C.).

2 *R. v. Orlandis-Habsburgo*, 2017 ONCA 649, 2017 CarswellOnt 12187 (Ont. C.A.).

3 *Entick v. Carrington*, [1765] EWHC K.B. J98.

4 See *ibid.* There is not, as expected, an explicit mention of privacy in the decision. The

the home as a place free from government interference remains a foundational principle of constitutional privacy.[5] The home — a place where individuals engage in intimate and personal activities — attracts a heightened expectation of privacy.[6] The Supreme Court has established a presumption of a subjective expectation of privacy in the home.[7]

Police powers to enter and search the home and its perimeter are heavily curtailed.[8] However, advancements in surveillance technologies allow police to "see" inside a home without entering. The home has become more visible to the outside world as its residents increasingly interact with devices connected to the internet. In the early days of the internet, the mainstay was a desktop computer that connected the home's residents with a global information system. Today, consumers can purchase "Internet of Things" (IoT)[9] devices for their home. The introduction of IoT devices in the consumer market poses new challenges for domestic privacy.[10]

---

challenged conduct is the royal messengers' entry into Entick's home and seizure of writings. Lord Camden writes that if this type of executive order is "held to be legal, the liberty of this country is at an end."

5 Tipper McEwan, "Pulling the Ivy out of the Windows: Presumptions of Privacy in the Home and *R v. Gomboc*" (2010) 19 Dal J Leg Stud 83 at 89; Lorne Neudorf, "Home Invasion by Regulation: Truckers and Reasonable Expectations of Privacy under Section 8 of the Charter" (2012) 45:2 UBC L Rev 551 at 568.

6 Richard Jochelson & David Ireland, *Privacy in Peril:* Hunter v Southam *and the Drift from Reasonable Search Protections* (Vancouver: UBC Press, 2019) at 47.

7 See *R. v. Patrick*, 2009 SCC 17, 2009 CarswellAlta 481, 2009 CarswellAlta 482 (S.C.C.) at para. 19 [*Patrick*]. See also *R. v. Tessling*, 2004 SCC 67, 2004 CarswellOnt 4351, 2004 CarswellOnt 4352 (S.C.C.) [*Tessling*] at para. 38 (". . .it may be presumed unless the contrary is shown in a particular case that information about what happens *inside* the home is regarded by the occupants as private. Such an expectation is rooted in the ancient law of trespass and finds its modern justification in the intimacies of personal and family life").

8 Neudorf, *supra* note 5 at 568, citing *R. v. Feeney*, 1997 CarswellBC 1015, 1997 CarswellBC 1016, 146 D.L.R. (4th) 609, [1997] 2 S.C.R. 13 (S.C.C.), reconsideration / rehearing granted 1997 CarswellBC 3179, 1997 CarswellBC 3180 (S.C.C.) ("Section 8 generally prohibits warrantless police searches of dwelling homes, with the exception of cases in which the police are in 'hot pursuit' of a suspect who slips into a residence").

9 The term "Internet of Things" (IoT) includes all devices that can communicate with other objects and the internet: Patricia Moloney Figliola, "The Internet of Things: Frequently Asked Questions" (13 October 2015), online (pdf): *Congressional Research Service* <crsreports.congress.gov/product/pdf/R/R44227/11>. See also Broadband Internet Technical Advisory Group, "Internet of Things (IoT) Security and Privacy Recommendations" (November 2016) at i, online (pdf): *BITAG* <bitag.org/report-internet-of-things-security-privacy-recommendations.php> and Sarah Villeneuve & Stephanie Fielding, "Data Never Sleeps: Data Collection Practices in Domestic Spaces" (12 November 2019), online (blog): *Brookfield Institute* <brookfieldinstitute.ca/data-never-sleeps-data-collections-practices-in-domestic-spaces/>.

10 See Section IA (IoT Infrastructure is Vulnerable to Surveillance Tools), *infra*.

Section 8[11] jurisprudence has not grappled directly with the constitutionality of the collection of metadata from IoT devices inside the home by law enforcement. This article does not address the manner of collection — it does not consider how third-party disclosure or control shapes this analysis. Instead, its focus is on a home-dweller's privacy interest in the metadata of their domestic IoT devices.

I argue that law enforcement collection of metadata from domestic IoT devices — whether through the cooperation of third parties or independently — attracts a reasonable expectation of privacy. Two arguments support this conclusion. First, section 8 jurisprudence on perimeter searches suggests that concerns about police proximity to house property lines are best understood as a concern for protecting residents from observations that invade the informational privacy interest engaged by their home activities. Therefore, when law enforcement use surveillance tools to collect data from home IoT devices, the subjective expectation of privacy related to the home is activated even if they do so from a considerable physical distance. It is the intimate nature of domestic activities, not the physical point of data collection, that matters for the purposes of a section 8 analysis. Second, the Supreme Court's focus on *strong* and *clear* inferences in *R. v. Spencer*[12] must be reassessed with an eye to the purposive reading of section 8: courts must become more comfortable engaging with predictions and probabilities used by law enforcement as informational outcomes that attract constitutional protection under the *Charter*. Doing so is crucial for the protection of privacy within the homes of individuals. The information collected by law enforcement, like heat maps or electricity usage, may not reveal much when taken alone. However, this data collection, when combined with other information or if inputted into predictive analytics models, has the potential to reveal much more than is first obvious.

(a) IoT Infrastructure is Vulnerable to Surveillance Tools

IoT devices are physical devices connected to the internet or another network.[13] Some popular examples include smart sensors, cameras, and thermostats.[14] However, devices like smart ovens, fridges, toasters, and even utensils have gained popularity in the Canadian market.[15] A 2019 consumer trends study found that a third of Canadians own at least one IoT device.[16]

---

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

[12] *Supra* note 1.

[13] See *supra* note 9.

[14] *Ibid.*

[15] See Villeneuve & Fielding, *supra* note 9.

[16] "Canadians on Smart Home Tech: Skeptical at First, Hooked Afterwards" (23 October 2019), online: *Newswire* < newswire.ca/news-releases/canadians-on-smart-home-tech-hesitant-at-first-hooked-afterwards-875438829.html > .

Smart devices record, create, and transmit data through the internet to other devices and to the servers or applications of the companies that manufacture them.[17] Smart devices that adapt and react to the home environment (i.e., learn from the events of use) collect time-sensitive data. Time-sensitive data collection gives away to large-scale data analytics, which aim to improve the overall functioning of the devices.[18] The breadth of data recorded by IoT devices gives rise to useful applications, such as tracking epidemics or overseeing large infrastructure.[19] At the same time, IoT devices allow data aggregation to a level "only written about in science fiction novels."[20] IoT infrastructure, still in the early stages of global implementation, remains vulnerable to security breaches and interferences from actors outside a user's home.[21]

This article focuses on IoT devices that do not collect obviously personal information. For example, the discussion here is not directly applicable to wearable technology or smart speakers. Instead, the more innocuous uses of smart home devices — fridges, locks, ovens, thermostats, smart electrical meters — are the context with which I am concerned. These devices create metadata as a by-product of their use.[22] The metadata created can be detailed and highly revealing, although they may appear meaningless when taken individually.[23] Data on how often law enforcement bodies request access to metadata from smart devices is not available, as far as my research indicates. However, metadata from smart home devices has been used to convict individuals in some cases. Police have sought data from IoT devices like Echo, FitBit, and Nest to resolve investigations.[24] The next section situates this type of police conduct in the Canadian constitutional context.

---

17 Patrick McFadin, "Internet of Things: Where Does the Data Go?" (2018), online: *Wired* ; Office of the Privacy Commissioner of Canada, "The Internet of Things: An Introduction to Privacy Issues with a Focus on the Retail and Home Environments" (February 2016), online (pdf): *Office of the Privacy Commissioner of Canada* < priv.gc.ca/media/1808/iot_201602_e.pdf > [OPC, *Privacy Issues*].

18 McFadin, *supra* note 17.

19 Marie-Helen Maras & Adam Scott Wandt, "Enabling Mass Surveillance: Data Aggregation in the Age of Big Data and the Internet of Things" (2019) 4:2 J Cyber Policy 160.

20 *Ibid.*

21 Lily Hay Newman, "Critical Flaws in Millions of IoT Devices May Never Get Fixed" (8 December 2020), online: *Wired* < https://www.wired.com/story/amnesia33-iot-vulnerabilitiesmay-never-get-fixed/ > .

22 Nader R Hasan, "Searching the Digital Divide" in Gerald Chan and Nader R Hasan, eds, *Digital Privacy: Criminal, Civil and Regulatory Litigation* (Toronto: LexisNexis, 2018) at 11 [Nader, Digital Divide].

23 OPC, *Privacy Issues*, *supra* note 17.

24 Zack Whittaker, "Smart Home Tech Makers Don't Want to Say if Feds Come for Your Data" (19 October 2018), online: *TechCrunch* < techcrunch.com/2018/10/19/smart-home-devices-hoard-data-government-demands/ > .

PART I: COLLECTION OF METADATA FROM SMART HOME DEVICES AMOUNTS TO A SECTION 8 "SEARCH"

IoT metadata contains a wealth of information that may be relevant to police investigations. The examples shared above — data collected by wearable device — attract high informational sensitivity. However, we can imagine hypotheticals of police looking for signs of human presence in a dwelling, or strange patterns of appliance and electricity use that may lead to a reasonable ground to believe individuals are carrying out illegal activities. These may be data points that are helpful when connected with other information that the police have or can observe legitimately, without the need to acquire prior judicial authorization through a warrant.[25] I argue that collection of these types of metadata engage an individual's reasonable expectation of privacy under section 8 of the *Canadian Charter of Rights and Freedoms*.[26]

To determine whether state conduct amounts to a violation of section 8 rights, courts first consider whether there has been a search or seizure. If so, the court must determine whether the search or seizure was unreasonable.[27] Generally, this means that even if state conduct amounts to a search within the meaning of section 8, a search conducted through lawful means (such as a warrant or production order) is "reasonable." The practical implication of recognizing this form of metadata collection as a search is that police will be required to acquire prior judicial authorization. This mechanism creates a safety valve between an individual's privacy interest and law enforcement.

My argument focuses exclusively on whether metadata collection from smart home devices comprises a search under section 8. In order for police conduct to amount to a search under section 8, the individual must hold a reasonable expectation of privacy in the contents of the search.[28]

The Supreme Court of Canada has taken a normative approach to the reasonable expectation of privacy analysis.[29] To determine whether the police conduct attracts a reasonable expectation of privacy, a contextual inquiry into the "totality of circumstances of a particular case" is undertaken.[30] Four lines of inquiry guide this analysis[31]:

---

[25] Such a warrant may be issued under the authority of section 487 of the *Criminal Code,* RSC 1985, c C-46.

[26] *Charter*, *supra* note 11.

[27] Department of Justice, "Section 8 — Search and Seizure" (last modified 8 June 2020), online: *Charterpedia* <justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art8.html> [Charterpedia, section 8].

[28] *Ibid*. See also Kent Roach & Robert J Sharpe, *The Charter of Rights and Freedoms*, 6th ed (Toronto: Irwin Law, 2017) at 311 — 317.

[29] Steven Penney, "The Digitization of Section 8 of the Charter: Reform or Revolution?" (2014) 67:16 SCLR 505 at 519.

[30] *Ibid.*

[31] *Spencer*, *supra* note 1 at para 18.

i. The nature of the subject matter of the search;
ii. The individual's direct interest in the contents of the search;
iii. Whether the subject had a subjective expectation of privacy;
iv. Whether the subjective expectation of privacy was objectively reasonable.

This inquiry aims to assess whether the subject has an objective (reasonable) expectation of privacy. While the Court has, in the most recent section 8 jurisprudence, followed this order of analysis, the goal remains to assess the "totality of the circumstances."[32] It is in the last line of inquiry — assessing whether the subjective expectation of privacy was objectively reasonable — that careful regard is given to the "totality of the circumstances."[33]

In cases related to smart home devices, the analysis of factors ii and iii will be straightforward. The resident of a home from which police collects IoT metadata will have a direct interest in the contents of that data — the information is not about a third party and is directly related to the residents.[34] The Court has also held that a subjective expectation of privacy can be presumed with regards to activities taking place in the home.[35] Smart home devices are evidently used inside the home. By their very design, smart home devices collect information about activities taking place inside the home. Notwithstanding an unusual contractual and regulatory matrix, residents will have a subjective expectation of privacy in the data collected and created by the device.

My arguments focus on two aspects of the "search" inquiry: the nature of the subject matter of the search and whether the subjective expectation of privacy was objectively reasonable. I outline the relevant aspect of each factor below.

(a) The Subject Matter of the Alleged Search

The Court has taken a "broad and functional approach" to this line of inquiry.[36] First, the Court has recognized that identifying the subject matter of the search requires looking beyond a narrow consideration of the physical space or the physical acts involved. Instead, the subject matter of the search is identified with an eye to the "privacy interests potentially compromised."[37] *Spencer* built on this rejection of a narrow analysis of the subject matter of the alleged search. Justice Cromwell (writing for the majority) noted that the inquiry to define the subject matter looks not only at the "precise information sought," but also at the "nature of the information it tends to reveal."[38] The inquiry into the privacy interest compromised depends on elements such as the privacy of the

---

32 *R. v. Mills*, 2019 SCC 22, 2019 CarswellNfld 161, 2019 CarswellNfld 162 (S.C.C.) at para. 13 [*Mills*].

33 *Ibid.*

34 Charterpedia, Section 8, *supra* note 27.

35 *Patrick*, *supra* note 7 at para 37.

36 *Spencer*, *supra* note 1 at para 26.

37 *Ibid.* at para 31.

38 *Ibid.* at para 26.

place or thing searched and "the impact of the search on the target."[39] The subject matter analysis, as defined to date, requires understanding i) the privacy interests at stake and ii) what information tends to be revealed by the information sought or collected.

(i) Whether the subject's subjective expectation of privacy is objectively reasonable

This last step in the "search" inquiry is a normative question and not a descriptive one.[40] The question is in what contexts "Canadians *ought* to expect privacy," or, in other words, in what contexts Canadians ought to expect security against unreasonable search.[41] To determine whether someone ought to expect privacy in a given situation, this part of the inquiry considers a non-exhaustive list of factors.[42] The most salient factors are identified depending on the facts of the case. In cases related to police collection or capture of information about the house that is also under the control of third parties, three factors are usually considered[43]:

1. Place of the search;
2. Whether the search reveals details about the lifestyle of the person or details that are intimate;
3. Whether the information was already in the hands of third parties; if so, whether it is subject to an obligation of confidentiality

For the purposes of this article, two factors are significant: place of search, and the ability to reveal details about lifestyle. The article proceeds by discussing first the privacy interests at stake, with an emphasis on the role of the home as a locus of heightened privacy. The role of inferences in defining the subject matter and the reasonable expectation of privacy is then considered in Part III.

PART II: TERRITORIAL AND INFORMATIONAL PRIVACY ARE OVERLAPPING INTERESTS IN HOME-RELATED SEARCHES

Section 8 protects at least three privacy interests: personal privacy, territorial privacy and informational privacy.[44] These categories serve as an analytical tool to determine the nature of the subject matter of the search and to aid the contextual analysis of the objective reasonability inquiry. These categories of privacy interest can overlap.

---

[39] *Patrick*, *supra* note 7 at para 32; *Spencer, supra* note 1 at para 36.

[40] *Mills*, *supra* note 32 at para 20.

[41] *Ibid.*

[42] Nader, Digital Divide, *supra* note 22.

[43] See generally *R. v. Gomboc*, 2010 SCC 55, 2010 CarswellAlta 2269, 2010 CarswellAlta 2270 (S.C.C.) [*Gomboc*]; *R. v. Orlandis-Habsburgo*, 2017 ONCA 649, 2017 CarswellOnt 12187 (Ont. C.A.) [*Orlandis-Habsburgo*].

[44] *Gomboc*, *supra* note 43 at para 19.

On a purposive view, section 8 protects "people, not places"[45]; however, the well-established principle of one's dwelling as a place that attracts heightened expectations of privacy acknowledges the reality that many activities pursued inside the home engage both territorial and informational privacy interests. The Court has consistently recognized the overriding constitutional importance of the privacy interests connected to activities engaged in within the home.[46] In *Tessling*, Binnie J. explained that state power to see inside our dwelling must be more limited relative to other locations because "the home is where our most intimate and personal activities are most likely to take place."[47]

The collection of metadata from smart home devices engages both territorial and informational privacy interests. This is true even if the police do not need to enter the home to collect metadata, but do so remotely, whether in physical proximity to one's home or by surveying from afar. It is important to recognize both interests independently *and* where they overlap.

Access to the metadata of smart home devices is an intrusion into the home despite the absence of physical entry by law enforcement. As I argue in subsection A (below), protecting the perimeter of dwellings — which has been recognized to engage the territorial privacy dimension of section 8 — is also tied to the informational privacy interest of the individual. Although the Supreme Court has asserted that perimeter searches engage territorial privacy, I argue that the concern at the core of these cases is also the protection of informational privacy interests. In subsection B, I expand the boundary of inquiry by considering cases to date that have found a reasonable expectation of privacy in information collected about the home from outside the home. These cases have attracted a reasonable expectation of privacy because they engage both informational and territorial interests — both the information collected and the nature of the *place* indirectly surveyed (the home) are integral to the analysis. These elements of section 8 jurisprudence point to the significant and overlapping interests at stake, which are of both a territorial and informational nature. As such, the collection of metadata from IoT devices would attract both of these privacy interests. Most significantly, the established line of cases that limit police powers in relation to perimeter searches are conceptually applicable to the collection of metadata from IoT devices and should guarantee the same level of protection moving forward.

(a) Limits on Perimeter Searches are a Proxy for Limiting Police Observations of Activities Inside the Home

The distinction between police conduct that is and is not a violation of a target's territorial privacy continues to evolve.[48] Police have "implied licence" to

---

[45] *Tessling*, *supra* note 7 at para 22.

[46] *R. v. Plant*, 1993 CarswellAlta 94, 1993 CarswellAlta 566, [1993] 8 W.W.R. 287, [1993] 3 S.C.R. 281 (S.C.C.) at para. 48 [*Plant*]; *Tessling, supra* note 7 at paras 13, 22.

[47] *Tessling*, *supra* note 7 at para 22.

do things such as approach the door of a home and knock to communicate with the occupant or check in on a complaint.[49] Other legitimate avenues are also available to police, such as observing the home from the public areas around it, noting who is entering and leaving the home, and asking neighbours for information related to activities taking place inside.[50]

There are also clear examples of what police conduct constitutes a search of the home. In *Plant*, the Supreme Court ruled that the police's search of a house's perimeter violated section 8.[51] In that case, the police walked around to the back of the house and tampered with a vent to see what was inside. In *R. v. Kokesch*, the police carried out a perimeter search without a warrant or probable grounds.[52] While doing so, "they heard electrical humming from the basement, noticed plywood nailed to the wall of the residence covering a louvered metal vent and, from the side of the plywood, detected an odour of marijuana as well as heat coming from the area."[53] The Supreme Court found that the process in which these observations were gathered violated the target's section 8 rights.

To date, the line between what conduct related to the home violates section 8 and what does not, has been determined with an eye to the physical conduct of the police. This means that the primary focus of these inquiries has been the territorial privacy interest at stake. Police have a sufficiently clear directive not to enter a target's home without a warrant or other lawful grounds. Their ability to conduct perimeter searches (i.e., their ability to be physically close to the home) is similarly limited.

Novel investigative techniques, like intercepting digital signals, do not require entry into the home to gather information about the activities inside the home. Through different technologies, police can make observations about the home without entering its premises or getting close to its perimeter. For example, whether the house temperature has been adjusted, or whether an IoT-connected toothbrush is communicating with the servers of its parent company, can result in reliable inferences about activity (or lack thereof) inside the home.

The protection of the home through the lens of territorial privacy interests has the purpose of protecting an individual's privacy interest in the intimate details that can be uncovered when the state intrudes upon the home. These cases focus on the physical closeness of police to home in order to establish a territorial privacy interest. However, even territorial privacy interests in these cases are meant to protect information about people's intimate lives, such as inferences

---

48 See e.g. Neudorf, *supra* note 5; see also Kent Roach & Robert J Sharpe, *supra* note 28 at 311 — 317.

49 *R. v. MacDonald*, 2014 SCC 3, 2014 CarswellNS 16, 2014 CarswellNS 17 (S.C.C.) at para. 26; Jochelson & Ireland, *supra* note **6** at 47.

50 *Gomboc*, *supra* note 43 at para 47.

51 *Supra* note 46.

52 *R. v. Kokesch*, 1990 CarswellBC 255, 1990 CarswellBC 763, [1990] 3 S.C.R. 3 (S.C.C.).

53 *Ibid.*

that police can make from peering through windows, looking inside vents, or smelling what is going on inside the home.

These perimeter search cases are not about identifying the physical space that police can occupy in relation to the home, and they are not about property lines. Instead, they are about the physical proximity that allows police to make clear observations and collect information that strongly reveals what is happening inside the home. In other words, the closer police get to the interior of the home, the closer they get to infringing upon detailed and intimate information about someone's life.

(b) Collection of Information about the Home from Outside the Home is Protected by Section 8

Section 8 protects territorial privacy in the home and guarantees a presumption of a subjective expectation of privacy about what goes on inside our homes.[54] If police access metadata from smart home devices without entering the home, they are still engaging the target's territorial privacy interest. The access to data created and communicated by smart home devices attracts the same type of privacy interest as has been engaged in cases where police have used technologies to carry out external collection of specific types of observations and measurements related to events taking place inside the home.

For example, in *R. v. Tessling,* the RCMP used a Forward Looking Infra-Red (FLIR) camera to capture images of thermal energy radiating from the accused's building.[55] The Supreme Court found that the privacy interest was primarily informational, but also implicated territorial privacy.[56] In *Tessling*, the RCMP did not enter the accused's home; however, the information the RCMP was seeking was about activities taking place in the home.[57] The Supreme Court held that the RCMP's actions implicated the accused's territorial privacy interest.

The issue at bar was whether the thermal energy radiation recordings revealed any intimate details about the target's life. The Supreme Court was clear that the use of the FLIR did not implicate the same extent of intrusion as an entry into the home by police. The Supreme Court recognized that the data collected implicated territorial privacy by looking into the home in a very specific way but held that it was mainly a matter of informational privacy. However, the recognition that it implicated territorial privacy points to conceptualizing the use of a surveillance technique that collects information about events taking place inside the home as territorial intrusion. This was the case even though the collection was technically achieved from outside the house.

In *Tessling*, the information collected by the FLIR did not already exist in a readable format. It was created by the FLIR, or rather it was "read" by it. In

---

54 *Patrick*, *supra* note 7.

55 *Tessling, supra* note 7.

56 *Ibid.* at para 24.

57 *Ibid.*

contrast, smart home metadata already exists and can give way to even more detailed observations than those in *Tessling*. Smart home devices collect detailed information that tracks events, changes, and interactions in the home. Collecting metadata from smart home devices would allow the police to "see" inside the home with much clearer vision than in *Tessling*. Perimeter search case law limits how close the police can get to observe the home. Section 8 jurisprudence recognizes the risk that this conduct causes to privacy interests. Applying this principle to smart home devices means that the police's ability to see inside the home should be equally limited even if they are not seeing in the physical sense. This kind of search goes beyond the acceptable avenues that police are currently granted to observe the home during criminal investigations.

In *R. v. Gomboc*, a digital recording ammeter (DRA) was installed on the power line connected to the house with the cooperation of the utility provider.[58] The DRA recorded hourly usage data which enabled police to make a "strong inference" that the pattern matched that of a grow-op.[59] Justice Deschamps (writing for the majority) decided that territorial privacy was not engaged because "the home itself was never *directly* the object of a search. The location where the search took place was not the home but the transformer box where the power lines entering the home could be accessed. After some confusion . . . about whether the transformer was located on Mr. Gomboc's property, it was common ground before this Court that it was not. Accordingly, no direct territorial privacy interest is engaged in this case."[60] Further, Deschamps J. noted that the search was "non-invasive and unintrusive" as it did not require entering the home.[61] Deschamps J.'s judgment in *Gomboc* assesses the severity of the intrusion by relying heavily on the physical intrusion of the police in relation to the home. The point where the data is collected (by the DRA, outside the home) is considered a key reason for why the expectation of privacy is not heightened, despite the fact that the home is involved.

In the context of smart home devices, however, *Gomboc* is easily distinguishable. Unlike the DRA, which was placed outside property lines, smart home devices are always inside the home. This means that the data is created and collected inside the home. Should police wish to access them, their conduct would involve intercepting the metadata's flow directly between the device and the network it is plugged into. Alternatively, police could access the metadata by requesting the information from a third-party manufacturer. As such, the principle from *Gomboc* that the collection is taking place outside the home does not apply. Even if there exists a hypothetical situation where it does apply, I have argued that the collection of metadata from smart home devices engages overlapping informational and territorial privacy interests. As a result,

---

[58] *Gomboc*, *supra* note 43 at para 1.

[59] *Ibid.* at paras 5 — 6.

[60] *Ibid.* at para 48.

[61] *Ibid.* at para 50.

collecting the metadata would attract the heightened protection of privacy that the home usually attracts.

The Supreme Court's decisions to date on information collected about the home with the use of advanced digital surveillance techniques that do not require entry have failed to draw a clear conceptual line that clarifies the connection between territorial and informational privacy interests. There will hopefully be occasions for courts to spell out this relationship in future cases. The distinction between the interior and exterior of a home is based on an assessment of police capabilities that precedes the kinds of surveillance, interception, and digital technologies that law enforcement uses today. Courts should be guided by the principle established in section 8 jurisprudence that searches in which the home is the object of the search attract a heightened expectation of privacy due to both the territorial nature of home privacy and the sensitive nature of the informational privacy interest engaged.

PART III: INFERENTIAL CAPABILITIES OF INFORMATION MUST BE CONSIDERED WHEN DETERMINING THE SUBJECT MATTER OF SEARCH

The strength of correlations or inferences that police can make based on the information collected or captured is at the core of the reasonable expectation of privacy analysis in *Plant*, *Tessling*, and *Gomboc*. The case law focuses on how clear the inference is or what the data can reveal about the individual's personal activities and intimate life. It is the information that is revealed, and not the information collected, that must attract a privacy interest for the individual to secure section 8 standing. Courts must acknowledge today's technological realities when determining the type of information that innocuous metadata can reveal and engage with predictions and probabilities as information that goes to the biographical core for the purposes of section 8. If courts do not take notice of these realities, large parts of individuals' personal lives will lose constitutional privacy protection.

IoT metadata, combined with the increasingly strong inferential capabilities of new technology, complicates this analysis. Any given piece of metadata could be combined with another piece of previously known information such that it gives rise to new information. For example, a recent study found that external parties could use metadata about the traffic of encrypted (unreadable) information to "infer, in real time, that a specific interaction . . . is occurring between the user and a smart [device]."[62] We can imagine this information being about any device in someone's home, including devices that may be particularly private and interact with someone's most intimate activities. In addition to connections between IoT metadata and other sets of information, police can use predictive technologies that use these data as input to output inferences and

---

[62] Alanoud Subahi & George Theodorakopoulos, "Detecting IoT User Behavior and Sensitive Information in Encrypted IoT-App Traffic" (2019) 19:21 Sensors (Basel) 4777.

probabilistic information.[63] Although they may not guarantee absolute certainty, smart home devices in combination with other tools available to law enforcement are powerful inferential instruments that can reveal intimate details about someone's life.

(a) Spencer was not the Final Word on the Reasonable Expectation of Privacy in Inferences Made from Collected Data

When defining the subject matter of the search, courts must inquire beyond the nature of the precise information sought to the nature of information a search reveals.[64] In the context of smart home devices, this means that, while information about when and how many times someone uses their air conditioner or toothbrush might not appear highly revealing of their biographical core, the information that metadata from smart home devices is likely to reveal could infringe on the individual's privacy interest.

In *Spencer*, the Supreme Court looked beyond the specific information collected. It focused on the information that the police planned to access and the privacy interests that the resulting information engaged. For example, in *Spencer*, "the subject matter of the search was not simply a name and address . . . it was the identity of an Internet subscriber which corresponded to particular Internet usage."[65] The Court recognized that Spencer's "specific online activities" were what the police were really seeking.[66]

Spencer involved a clear, one-step link between the original information (subscriber information) and the inference (history of online activity). The police were able to input the seemingly innocuous information into a database. This allowed them to unlock detailed information about Spencer's subscriber history. When deciding what information is revealed by data points such as electrical consumption records, or an IP address and name, the Supreme Court has looked for a clear link between one piece of information and the resulting piece of information. In *Spencer*, the clear link was found. In previous cases, like *Plant* and *Gomboc*, the link was not as clear: it required police to compare the information about other data sets and to make "informed *predictions*" [emphasis in original].[67]

---

[63] See e.g. Kate Robertson, Cynthia Khoo & Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (University of Toronto, 2020) at 41 — 65, online (pdf): *The Citizen Lab* <https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf>. See also Andrew Guthrie Ferguson, "Big Data and Predictive Reasonable Suspicion" (2015) 163:2 U Penn L Rev 327; Xerxes Minocher & Caelyn Randall, "Predictable Policing: New Technology, Old Bias, and Future Resistance in Big Data Surveillance" (2020) 26:5 Convergence 1108.

[64] *Spencer*, *supra* note 1 at para 26.

[65] *Ibid.* at para 32.

[66] *Ibid.* at para 49.

[67] As characterized by McLachlin C.J. (as she then was) and Fish J. in their dissent in *Gomboc, supra* note 43 at para 124 ("The significance of the DRA data derives from its

The Supreme Court's reliance on "strength" and "certainty" is not easily reconciled with the types of metadata that smart home devices often collect and communicate. Metadata can be meaningless on their own but can be very revealing when placed in context with other metadata or analyzed with other known patterns.[68] *Spencer* did not remedy the focus on the strength of inferences, since in that case the link between the IP address, name, and subscriber history was conclusive. It was less of an inference and more like a missing link that gave the police access to verifiable and certain information. The framework for assessing whether raw data that gives way to information about an individual's life can itself attract a reasonable expectation of privacy remains to be decided.

(b) Section 8 Does Not Protect only "Strong" Inferences

The cases decided before *Spencer* took different and confusing approaches to the treatment of information that can reveal other information that in turn attracts a reasonable expectation of privacy. These examples show a Supreme Court divided on how to understand information that is not itself revelatory of personal details. The information collected in these cases requires some type of processing in order to be useful to police. The process of taking data points, combining them with other points, and reaching new conclusions or educated prediction about actions, surroundings, or behaviour has not been addressed directly by the Supreme Court in these cases.[69]

For example, in *Plant*, there was disagreement about the relationship between electrical consumption data and intimate details. Sopinka J. (writing for the majority) held that there was no link between the electrical consumption information and intimate details about the residents' life. McLachlin J. (as she then was) dissented on this point, arguing that "[t]he very reason the police wanted [the electricity consumption records at issue] was to *learn about the appellant's personal lifestyle*, i.e. the fact that he was growing marihuana" [emphasis added].[70] In *Tessling*, Binnie J. (writing for the majority) held that the FLIR data provided "meaningless" information. The information was meaningless because it did not give any *certain* links between the FLIR data and the activities inside the home.[71] Instead, the FLIR data supported "a

---

utility in making informed *predictions* concerning the *probable* activities taking place within a home. Predictions of this sort, while not conclusive, nonetheless convey useful private information to the police").

68 Office of the Privacy Commissioner of Canada, "Metadata and Privacy: A Technical and Legal Overview" (October 2014), online (pdf): *Office of the Privacy Commissioner of Canada* < priv.gc.ca/media/1786/md_201410_e.pdf > .

69 A similar proposition is made in Nader R Hasan et al, *Search and Seizure* (Toronto: Edmond, 2021) at 60 ("The Internet of Things means that courts and counsel will increasingly have to consider the ways in which different data sets *in combination* with other data sets affect privacy rights").

70 *Plant*, *supra* note 46 at para 49.

71 McEwan, *supra* note 5 at 83 — 84.

number of hypotheses including as *one possibility* the existence of a marijuana grow-op" [emphasis added].[72]

In *Gomboc*, the Court was divided on how to conceptualize what information could be revealed by data on electricity consumption. Deschamps J. (writing for the majority) took a narrow view. She focused on "the degree to which the DRA data reveals private information"[73] and concluded that such data "reveals nothing about the intimate or core personal activities of the occupants. It reveals nothing but one particular piece of information: the consumption of electricity."[74] In her concurring opinion, Abella J. argued that the DRA, which measured minute-by-minute electrical consumption data points, yielded "usually reliable inferences as to the presence within the home of one particular activity."[75] McLachlin C.J. and Fish J. in their dissent argued that "the fruits of a search *need not produce conclusive determinations* about activities within a home in order to be considered informative and thus intrusive" [emphasis added].[76]

(c) Section 8 Protects People from Unreasonable State Intrusion, not from Perfect Predictive Power

The treatment of inferences in these cases indicates both confusion and division among the Supreme Court. The Supreme Court in *Spencer* did not have the opportunity to address issues of possibilities, inconclusive determination, or other points of contention from these judgments. Instead, *Spencer* sets a strong foundation for protecting information with inferential capabilities, whether on its own or in combination with other data. Its interpretation in the future must not be limited to clear-cut cases.

Others have argued that metadata collected from IoT devices should be treated similarly to the heat-based data in *Tessling* or the electricity consumption data in *Gomboc*.[77] Lee-Ann Conrod, for example, argues that this should be so, in part by characterizing smart home devices like a fridge or a lightbulb as a "dumb device" since it does not reveal "a massive amount of information" about the user on its own.[78] She argues that "any search to obtain data from a dumb device would be minimally intrusive, specific, and have pinpoint accuracy".[79]

---

[72] *Tessling*, *supra* note 7 at para 53.

[73] *Gomboc*, *supra* note 43 at para 6.

[74] *Ibid*. at para 14.

[75] *Ibid*. at para 81.

[76] *Ibid*. at para 123.

[77] Lee-Ann Conrod, "Smart Devices in Criminal Investigations: How Section 8 of the *Canadian Charter of Rights and Freedoms* Can Better Protect Privacy in the Search of Technology and Seizure of Information" (2019) 24 Appeal 115 at 128 ("I would imagine that the SCC would treat this type of technology much like they did the forward looking infrared ('FLIR') or digital recording ammeter ('DRA'). Like FLIR, the information 'may or may not be capable of giving rise to an inference about what was actually going on inside'").

[78] *Ibid*.

The manner in which the search is conducted is a factor in deciding whether the search is reasonable, in later steps of the section 8 analysis. However, the fact that this type of search would on its own be minimally intrusive compared to, for instance, a police car sitting outside of someone's house to determine whether they are home does not mean that the collection of metadata is not a search. Section 8 is technologically neutral and whether information collected from a source about an individual amounts to a search under section 8 should not rely on the type of device from which such information is collected.

Courts should read *Spencer* broadly, as an example of a strong inference that falls under the set of situations where seemingly non-personal data has the potential to reveal more intimate information. *Spencer* has already been applied in cases related to the collection of information about the home.

Orlandis-Habsburgo, a Court of Appeal for Ontario (CAO) decision, found that "subject matter of the search includes both the raw data and the inferences that can be drawn from that data about the activity in the residence."[80] Most notably, the decisions in *Orlandis-Habsburgo* and *R. v. Tran*[81] applied *Spencer* and refused to follow the precedents set by *Gomboc* and *Plant* that electricity consumption data did not attract a reasonable expectation of privacy.[82] The courts in these cases found that conclusions reached by police by comparing electrical consumption records with grow-op consumption patterns were informational outcomes that attracted a reasonable expectation of privacy. This approach recognizes that, without the consumption data collected from the home, law enforcement would not have been able to reach this conclusion. The decisions recognize that, while the consumption data themselves may not fall within the individual biographical core, the resulting conclusions that the police reached did attract a reasonable expectation of privacy. The same logic should be applied to metadata from smart home devices in future cases.

---

79 *Ibid.*

80 *Orlandis-Habsburgo, supra* note 43 at para 75.

81 In *R. v. Tran*, 2018 ONSC 132, 2018 CarswellOnt 7687 (Ont. S.C.J.) at para. 60, Justice Munroe engages in a sophisticated analysis of the strength of the inferences before her ("I acknowledge that the strength of the inference between the data and the activity should be considered. . . . And I do. But it is the tendency of the data to support the inference sought which must be the focus. . . . Here the inference is strong when considered in context of other information collected by the police including the specific energy consumption data from these two houses. We are dealing here with a small and identifiable group of homes . . . It is the small and identifiable size that makes the inference sought by the police possible. If the sample size was large, the information would be little more than a statistic making any inference impossible and useless to the police. That is not the case here").

82 See Hasan et al, *supra* note 69 at 60.

CONCLUSION

Smart home devices implicate both territorial and informational privacy interests. Courts should not be led astray by the intangible nature of the collection of metadata from smart home devices. These devices are found in people's homes, and their seemingly innocuous metadata can be leveraged to reveal much more sensitive information about the individual and their home. Searches of metadata from smart home devices should be conducted with prior judicial authorization in order to be reasonable. Police should be required to obtain a search warrant pursuant to section 487 of the *Criminal Code* or a production order pursuant to section 487.014 of the *Criminal Code*.

Home searches engage territorial privacy interests, which in turn protect informational privacy interests by blocking access to where such information may be found. Searches of smart home devices are home searches. Protection from physical intrusion into someone's territory in and around the home can be translated to reflect the changing connection that networked technology introduces between the physical interior of the home and the outside world. Smart home devices communicate from inside the home to outside the home without seeking constant permission to do so from the home dweller. The use of such devices is likely to grow due to their utility and convenience. Individuals should not lose the reasonable expectation of privacy in their homes because they choose to introduce smart devices into these intimate spaces.

Smart home devices also engage informational privacy interests due to the inferences and informed predictions that can be made as a result of their metadata. *Spencer* and the *Orlandis-Habsburgo* decision are starting points that encourage courts to engage with the complex technological reality of data processing. Section 8 jurisprudence is still developing in its treatment of inferences. Information that serves as the basis of inferences and predictions that touch on the "biographical core" should be protected by section 8 even if it does not yield perfect outputs.