Digital Enlightenment Yearbook 2012
J. Bus et al. (Eds.)
IOS Press, 2012

doi:10.3233/978-1-61499-057-4-199

Reduction to Absurdity: Reasonable Expectations of Privacy and the Need for Digital Enlightenment

Jena McGILL[a] and Ian KERR[b,*]
[a] *Assistant Professor, Faculty of Law, University of Ottawa (jena.mcgill@uottawa.ca)*
[b] *Canada Research Chair in Ethics, Law & Technology, Faculty of Law, Faculty of Medicine, Department of Philosophy, School of Information Studies, University of Ottawa (iankerr@uottawa.ca).*

Abstract: This article seeks a deeper understanding of privacy in the digital age through an examination of a phenomenon the authors call "information emanation." Focusing on Canadian jurisprudence involving heat and odour emanations, the authors examine the current approaches of Canadian courts in decisions about the 'reasonable expectation of privacy'. The authors focus on three judicial trends that pose serious risks to privacy: 1) the tendency to equate different kinds of emanations and conclude that information emanations into public spaces never attract a reasonable expectation of privacy; 2) a reductionist approach to information privacy, which obscures the deep social significance of police investigative techniques; and 3) the adoption of a non-normative approach to 'reasonable expectations' ushering in a shift in privacy discourse away from democracy, rights and duties towards an inquiry about digital technology and standards of police practice. The authors conclude that while the Supreme Court of Canada attempted to guard against many of these risks, recent jurisprudence indicates an ongoing threat of backslide to the reductionist approach to informational privacy, especially in future cases involving emerging digital technologies.

Keywords: reasonable expectation of privacy, informational privacy, emanations, surveillance, Canadian Charter of Rights and Freedoms, search and seizure

Introduction

For all but the tiniest sliver in the history of human thought, the notion of *emanation* has been understood mostly as a cosmological concept; an unobservable *flow of being* derived from god alone. According to Plotinus,[1] chains of emergence, emanating from the godhead, provide a cosmological account of the relationship between a transcendent god and a finite, imperfect world. Interesting metaphysics notwithstanding, god's monopoly did not last forever. Empirical science has since rendered visible much that was previously imperceptible, revealing that humans, too, generate a flow of being. In the transformation from a cosmological to a technological worldview, many of our emanations are now observable. As we gain mastery over the assemblage of bits and bytes that make up the empirical world, it has become abundantly clear that things regularly flow from our bodies, our artefacts, and objects in our proximity. We constantly emanate: heat, light, particles, waves, smells, sounds, etc. Through these, we also emanate much information.

[1] Plotinus, *The Six Enneads* (Whitefish, MT: Kessinger Publishing, 2004).

Emanations containing valuable personal data include the potentially endless range of emissions that can be seen, heard, smelled or felt. Emanations radiate from our computers, our cell phones, our televisions and radios, our luggage, backpacks, clothing and homes. Our bodies also emanate information via electrical activity from brains and hearts, DNA from flaking skin cells and shedding hair, and data on health status from germs emitted when we cough, sneeze or spit. We are constantly *giving away*, knowingly or otherwise, emanations that contain information about our bodies, our homes and our lives. Like heat from our homes and scents from our luggage, these emissions are sometimes continuous and are often undetectable by naked human senses, meaning we cannot exert control over their dispersion or collection by third parties in the same ways that we might manage fixed data regarding our personal lives, property or bodies. We rarely notice when emanations from our bodies, homes or belongings go missing.

While emanations may seem innocuous in isolation, the ever-increasing number of technologies designed to: locate, track, store, process, mine, buy, use, break, fix, trash, change, melt, upgrade, charge, pawn, zoom, press, snap, work, erase, write, cut, paste, save, load, check, rewrite, plug, play, burn, rip, drag, drop, zip, unzip, lock, fill, curl, find, view, coat, jam, unlock, surf, scroll, pose, click, cross, crack, twitch, update, name, rate, tune, print, scan, send, fax, rename, touch, bring, obey, watch, turn, leave, stop and format[2] information gleaned from emanations means that single bits of *emanation information* can be manipulated with such significant degrees of control that it is now possible to build a comprehensive profile of an individual's biographical or biological life without that individual ever knowing that he or she is, was, or will be a subject of surveillance.[3]

Without question, uncovering the information bundled into these emanations has been of tremendous utility to the investigative sciences and the practice of law enforcement. The techniques by which particular emanations become known and understood are extremely powerful. They can be used to target individuals or groups with great precision and accuracy; sometimes, with amazing simplicity and often at little expense.

In this article, we focus on the judicial treatment of a seemingly primitive example: the use of behavioural science techniques to train dogs to perceive the scent of illicit drugs. With an extremely high degree of accuracy,[4] police pooches are able to quickly detect the presence of drugs in a backpack inside a gym locker and communicate this information to their handlers. No longer is there a need to hack the lock or call the principal; scents emanate with or without a search warrant.

Like tomorrow's digital devices and ubiquitous surveillance techniques, snoop dogs can be used to obtain incriminating evidence without transgressing property lines or invading one's personal space. And, so we ask: when police use snoop dogs to detect the emanation of odours in public spaces without a search warrant, are they conducting a search or otherwise interfering with privacy interests in a manner that should attract

[2] Daft Punk, "Technologic" on *Human After All* (Virgin Records, 2005) track 9. Thanks to Anne Cobbett for sharing the Daft Punk lyrics.

[3] See *e.g.* Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004).

[4] See *e.g. Her Majesty the Queen v. Gurmakh Kang Brown* (2006), 391 A.R. 218, 2006 ABCA 199 [*Kang Brown*] at para. 24, where the Alberta Court of Appeal noted evidence that the dog used in the *Kang Brown* case was 90- 92% accurate.

constitutional scrutiny?[5] More particularly, are the external patterns of smell on the outer surfaces of a locker or a backpack the kind of information in which a person holds a reasonable expectation of privacy?

Though these questions may seem narrow and obscure, how the courts answer them will prefigure the legal treatment of a range of emerging digital technologies. For this reason, we examine in detail the twin decisions of the Supreme Court of Canada in a joint appeal of two snoop dog cases – *Kang Brown v. R.* from Alberta[6] and *R. v. M.(A.)* from Ontario.[7] Like the Supreme Court's earlier decision in *R. v. Tessling*,[8] these cases raised broad and important questions about the nature of privacy and autonomy in a world of ubiquitous information emanation.

Indeed, having witnessed the snoop dog cases emanate both to and from the Supreme Court, there remains cause for concern about three jurisprudential trends that pose serious risks to privacy: (i) the growing number of wrongly decided information emanation decisions in Canadian courts,[9] and their continuing reliance on an inappropriate use of judicial analogy stemming from a misreading of *Tessling;* (ii) the excessively *reductionist* approach to informational privacy adopted in many reasonable expectation of privacy cases—in Canada and elsewhere—which obscures the deep social significance of police investigative techniques like sniffer dogs;[10] and (iii) the tendency in several provincial courts across Canada and throughout North America to adopt a non-normative approach to 'reasonable expectations', ushering in a shift in privacy discourse away from democracy, rights and duties towards an inquiry about digital technology and standards of police practice.[11]

Because these judicial trends are of global import and are being resolved using similar legal approaches in various courts of law in Europe and North America, our aim in this article is to reflect broadly upon the worries that arise in these cases, specifically within their Canadian context but, also, as instances of a larger global privacy trend: a diminishing of informational privacy by way of said shrinking privacy expectations.

In Part 1, we commence with a discussion of the two snoop dog cases that made their way to the Supreme Court of Canada in 2007. This is followed by an investigation of the application of the *Tessling* decision by way of analogy in Part 2. In Part 3, we take a broader look at reasonable expectations of privacy, examining three possible danger zones inherent in the approach adopted in the majority of Canadian snoop dogs cases: (i) the narrow conception of informational privacy, (ii) the pickwickian relationship between searches and expectations of privacy, and (iii) the non-normative conception of reasonable expectations. With these concerns in mind, in

---

[5] *Canadian Charter of Rights and Freedoms*, s.8, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c.11 [*Charter*]. Section 8 of the *Charter* reads: "Everyone has the right to be secure against unreasonable search and seizure."

[6] Kang Brown, supra footnote 4.

[7] *R. v. M. (A.)* (2006), 79 O.R. (3d) 481, 209 O.A.C. 257 (ON CA) [*A.M*].

[8] *R. v. Tessling,* 2004 SCC 67, [2004] 3 S.C.R. 432 [*Tessling*].

[9] The Supreme Court has since ruled in *R. v. A.M*., 2008 SCC 19, [2008] 1 S.C.R. 569 [*A.M. SCC*]; *R. v. Kang Brown*, 2008 SCC 18, [2008] 1 S.C.R. 456 [*Kang Brown SCC*] that the police must have a "reasonable suspicion" that someone is in possession of a drug in order to justify a snoop dog search. Of the approximately seventeen cases decided since the Supreme Court's 2008 ruling, ten have found that this (relatively low) standard was met. The courts decided that the searches in these cases were conducted in accordance with the accused's privacy rights. See *e.g. R. v. MacKenzie*, 2011 SKCA 64, [2011] 12 W.W.R. 102.

[10] On the reductionist approach to informational privacy, see *e.g.* Luciano Floridi, "The Ontological Interpretation of Informational Privacy" (2005) 7 Ethics and Information Technology 185.

[11] See *e.g. R. v. McCarthy*, 2005 NSPC 49, 239 N.S.R. (2d) 23 (NL CA) [*McCarthy*].

Part 4 we look to the Supreme Court's analysis of the snoop dog cases, assessing whether and how they avoid the danger zones we warn against. In Part 5, we identify an ongoing risk of analytical backslide to the reductionist approach to informational privacy—particularly in future cases involving emerging digital technologies.

1. The Snoop Dog Cases

The legal basis for most of the Canadian snoop dog decisions is an application of the *Tessling* decision, wherein the Supreme Court of Canada held that, "external patterns of heat distribution on the external surfaces of a house is not information in which the respondent had a reasonable expectation of privacy."[12] Extending the reasoning of this decision by way of analogy, many courts[13] subsequently reasoned that patterns of odour on the external surface of a backpack or locker are not information in which an accused had a reasonable expectation of privacy. On this basis, most of those courts concluded that the dog sniff is *not* a search and therefore did not implicate constitutional scrutiny.

It is worth noting that a number of courts have gone the other way, holding that a warrantless use of snoop dogs *does* constitute a search and infringes the right to be secure against unreasonable search and seizure.[14] Part of the explanation for the apparent schizophrenia in Canadian caselaw is that the reasonable expectation of privacy jurisprudence has paid close attention to the "totality of the circumstances" approach adopted in *R. v Edwards*.[15] To be fair to the courts, the fact patterns for the dozen or so decisions range from dogs sniffing backpacks and lockers at bus depots,[16] to dogs sniffing rental cars on public highways,[17] to dogs randomly sniffing school gymnasiums.[18] It is not surprising that these different contexts have led to different judicial pronouncements regarding the reasonable expectation of privacy in at least *some* instances. Consequently, it came as no surprise that in 2007 the Supreme Court was asked to resolve cases from two appellate courts that seemed to go in opposing directions.

In *R. v. A.M.*, a high school principal issued a standing invitation to police officers to conduct searches as part of the school's *zero tolerance* policy on drugs. Two years later, three police officers showed up to conduct a random search of the school. In the course of their investigation, a police dog detected drugs in a backpack that had been left unattended in the school's gymnasium. The police searched the backpack and discovered illegal narcotics, associated paraphernalia and identification linking the backpack and its contents to A.M.. At trial, A.M. was acquitted on the basis that the

---

[12] *Tessling*, *supra* footnote 8 at para. 63.

[13] See *R. v. Hoang*, 2000 ABPC 200, 284 A.R. 201; *R. v. Mercer*, 2004 ABPC 94, 362 A.R. 136; *R. v. Davis*, 2005 BCPC 11; *R. v. Peardon,* 2005 BCPC 117; [2005] B.C.W.L.D. 4415; *R. v. Gosse*, 2005 NBQB 293, 92 N.B.R. (2d) 254; *McCarthy*, *supra* footnote 11; *R. v. McLay*, 2006 NBPC 6, 299 N.B.R. (2d) 207; *R. v. Gallant*, 2006 NBQB 114, 300 N.B.R. (2d) 289; and *Kang Brown*, *supra* footnote 4.

[14] See *R. v. Wong*, 2005 BCPC 24, [2005] B.C.W.L.D. 2570; *R. v. Donovan,* [1992] N.W.T.R. 75; *R. v. Dinh* (2003), 330 A.R. 63, (*sub nom*. *R. v. Lam*) 2003 ABCA 201; *R. v. Buhay,* 2003 SCC 30, [2003] 1 S.C.R. 631; and *A.M., supra* footnote 7.

[15] *R. v. Edwards*, [1996] 1 S.C.R. 128, 26 O.R. (3d) 736 (note), 132 D.L.R. (4th) 31 [*Edwards*].

[16] See *e.g. Kang Brown, supra* footnote 4; *McCarthy, supra* footnote 11; *R. v. Dinh*, *supra* footnote 14; and *R. v. Buhay, supra* footnote 14.

[17] See *e.g. R. v. Davis*, *supra* footnote 13; *R. v. Peardon*, *supra* footnote 13.

[18] See *e.g. A.M., supra* footnote 7.

evidence from his backpack should be excluded under section 24(2) of the *Charter*[19] because it was obtained through an unreasonable search and therefore violated section 8 of the *Charter*.[20] The Ontario Court of Appeal unanimously dismissed the Crown's appeal, finding that A.M. had a reasonable expectation of privacy in his backpack and the warrantless dog sniff and subsequent search of the pack constituted an unreasonable search for the purposes of section 8 of the *Charter.* Armstrong J. was careful to distinguish *A.M.* from *Tessling:*

I see a significant difference between a plane flying over the exterior of a building (on the basis of information received) and the taking of pictures of heat patterns emanating from the building, and a trained police dog sniffing at the personal effects of the entire student body in a random police search.[21]

The core facts in the second case, *Kang Brown v. R.,* are similar to *A.M.* insofar as a dog sniff of a shoulder bag resulted in a drug bust; however, the context differed significantly. Kang Brown was departing from a Calgary bus terminal with his bag over his shoulder when he was approached by an RCMP officer who was part of Operation Jetway, a program designed to curtail drug trafficking through police monitoring of travelers in public airports, train stations and bus depots.[22] After watching Kang Brown and identifying certain behaviours deemed 'suspicious,'[23] the officer spoke to the accused regarding the nature of his travel. A second officer with a police dog joined the conversation, and the pooch quickly indicated the presence of drugs in Kang Brown's baggage, leading the officers to search the bag, where they found 17 ounces of cocaine. Like A.M., the accused brought an application for the exclusion of that evidence under section 24(2) of the *Charter* on the basis that his right to be free from unreasonable search and seizure had been violated as a result of the dog sniff.

At trial, the judge found no breach of section 8 because the odour emanating from Kang Brown's bag was not information in which he could have held a reasonable expectation of privacy. The judge admitted the evidence and convicted Kang Brown of possession for the purposes of trafficking.[24] The majority of the Alberta Court of Appeal concurred, finding that "…the dog only yielded a crude piece of information…, no intimate details of private lives could possibly be revealed…There was no reasonable expectation of privacy for that limited information in that public space."[25] Consequently, section 8 of the *Charter* was not engaged.

There is something striking about the different, indeed *opposing*, conclusions of the Ontario Court of Appeal in *A.M.* and the Alberta Court of Appeal in *Kang Brown* with respect to the existence of a reasonable expectation of privacy in odours emanating from a backpack/shoulder bag. As alluded to above, part of the explanation

---

[19] *Charter*, *supra* footnote 5 at s. 24(2) reads: "Where…a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute."

[20] *R. v. M.(A.),* 2004 ONCJ 98, (2004) 120 C.R.R. (2d) 181.

[21] *A.M., supra* footnote 7 at para. 47.

[22] Operation Jetway targets travelers who look 'out of the norm' with respect to their clothing, behaviour or demeanor. A police officer will identify a 'suspicious' looking individual, approach the target with his or her police dog, and engage the target in a conversation with the goal of having the target consent to a search of his or her person and/or luggage to determine if he or she is carrying drugs. See *e.g. R. v. Arabi* (2002), 2 Alta. L.R. (4th) 358, [2002] 7 W.W.R. 542; *R. v. Rochat*, 1999 ABPC 10, 241 A.R. 201.

[23] See *R. v. Kang Brown,* 2005 ABQB 608, 386 A.R. 48 at paras. 53-54.

[24] *Ibid*.

[25] *Kang Brown*, *supra* footnote 4 at para. 52.

may turn on the unique facts of each case and the application of the totality of the circumstances test set out in *Edwards*[26] and developed in the subsequent section 8 jurisprudence. However, it is our contention that the tension between these opposing outcomes does not reflect factual differences as much as it does two very different interpretations of the legal precedent set in *Tessling*, to which we now turn.

2. The *Tessling* Analogy

Tessling did not involve snoop dogs or emanating odours. Instead, heat emanations from a house where police suspected there was a marijuana grow-op were detected and measured by a technology known as Forward Looking Infrared (FLIR). According to the Supreme Court of Canada, current FLIR technology "…cannot 'see' through the external surfaces of a building" to indicate the nature or source of heat, but can create "…an image of the distribution of escaping heat at a level of detail not discernible by the naked eye."[27] In essence, it is a camera that takes pictures of the heat on the outside of a building.

The RCMP took a FLIR 'picture' of Tessling's home, which was used, along with other information, to secure a warrant to search Tessling's house. During the search, the police discovered large quantities of marijuana and various firearms, and Tessling was subsequently charged with possession for the purposes of trafficking and related drug and weapons offences.

Like A.M. and Kang Brown, Tessling argued at trial that the evidence acquired during the search of his home should be excluded under section 24(2) of the *Charter* because the warrantless FLIR overflight amounted to an unreasonable search and the search warrant would not have been granted without the FLIR information.[28] His claim was unsuccessful, the evidence was admitted and Tessling was convicted at trial. However, the Ontario Court of Appeal unanimously reversed the trial judgment and acquitted Tessling, finding that he had a reasonable expectation of privacy in his home and that police use of FLIR technology to detect heat emanations infringed this expectation and breached his section 8 *Charter* rights. Unlike other decisions – where the analysis focused narrowly on a determination of whether the specific bits of information intercepted during emanation was core biographical information – the Ontario Court of Appeal characterized the information obtained through FLIR technology in light of the purpose for which it was being gathered, "that is, to attempt to determine what is happening inside the home."[29] Consequently, the Court concluded that the search warrant was not lawfully obtained and the evidence gathered in Tessling's home was excluded, resulting in his acquittal.

On appeal, Binnie J., writing for a unanimous Supreme Court of Canada, reversed the decision of the Ontario Court of Appeal, concluding that "[e]xternal patterns of heat distribution on the external surfaces of a house is not information in which the respondent had a reasonable expectation of privacy."[30] In rendering this conclusion, Binnie J. emphasized the informational privacy interests at stake, characterizing FLIR imaging "…as an external search for information *about* the home which may or may

[26] *Supra* footnote 15.
[27] *Tessling, supra* footnote 8 at para. 5.
[28] *R. v. Tessling* (5 December 2000), London, (Ont. Sup. Ct.).
[29] *R v Tessling* (2003), 63 O.R. (3d) 1, 168 O.A.C. 124 [*Tessling Appeal*] at para. 66.
[30] *Tessling, supra* footnote 8 at para. 63.

not be capable of giving rise to an inference about what was actually going on inside…".[31] Tessling's expectation of privacy in the heat emanating from his home was held not to be objectively reasonable for two reasons: (i) FLIR is an "off-the-wall" rather than a "through-the-wall" technology;[32] and (ii) the information gathered by FLIR technology was, *on its own*, "meaningless."[33] Since there was no reasonable expectation of privacy in the isolated, meaningless emanation of heat from Tessling's home, the FLIR overflight by police was not a search for the purposes of section 8 of the *Charter*, and Tessling's conviction was reinstated.

By now it should be clear that the relevance of the *Tessling* decision to *A.M.* and *Kang Brown* lies in the fact that its outcome seems to invite subsequent courts to consider adopting an extension of its logic to searches involving sniffer dogs, asking whether external patterns of smell emanating from backpacks and luggage is or is not information in which an individual holds a reasonable expectation of privacy. At first glance, it may appear to require only a small extension of the Court's logic in *Tessling* to make the case applicable to scenarios involving sniffer dogs; one need only accept the equation of heat emanations from a home with smells emanating from backpacks. If Tessling does not have a reasonable expectation of privacy in the heat emanating from his home, some may argue, A.M. and Kang Brown similarly have no expectations of privacy in the smells emanating from their backpack and shoulder bag, respectively. This analogy, and others paralleling the nature of the information gathered through FLIR technology with that obtained in dog sniffs, have formed the basis of the reasoning in a number of court decisions in various provinces interpreting *Tessling* in a manner that supports the proposition that no reasonable expectation of privacy exists in emanating odours and the consequent conclusion that a 'sniff' by a police dog does not qualify as a search for the purposes of section 8.[34]

While the logic of this analogy offers elegant explanatory surface appeal, deeper down, it has serious negative consequences and in fact requires a significant intellectual leap. The beauty of its logic invokes a mesmerizing sleight of hand through which our minds are misdirected away from police choppers slashing through the night and patrol dogs perambulating corridors – these things no longer qualifying as searches – towards an impersonal, non-social *and merely informational* scientific account of heat emanating from a building or odours emanating from luggage. By reducing potentially coercive or restrictive state action to atoms, molecules, bits and bytes, by stripping police investigation entirely of its social context,[35] the judicial analogy between *Tessling* and the snoop dog cases substantially diminishes the scope of section 8

---

[31] *Ibid.* at para. 27.

[32] "Off-the-wall" technologies are those that detect or observe only the exterior of a building, while "through-the-wall" technologies are, in theory, those that can see through the walls of a structure to observe details inside. *Tessling*, *supra* footnote 8 at para. 5. See also *Kyllo v. United States* (2001), 121 S. Ct. 2038 at para. 19, where Scalia J. for the majority of the United States Supreme Court rejected the distinction between "off –the-wall" and "through-the-wall" surveillance in finding that the warrantless use of FLIR technology did constitute a search.

[33] *Tessling, supra* footnote 8 at para. 58.

[34] See *e.g. R. v. Davis, supra* footnote 13 at paras. 21-23; *R. v. Gosse*, *supra* footnote 13; *R. v. McLay*, *supra* footnote 13 at para. 38; *R. v. Gallant*, *supra* footnote 13 at para. 36.

[35] We are indebted to Professor Valerie Steeves for this point. See Valerie Steeves, "Reasonable Expectation of Privacy: The Sociological Perspective" (Presented at The True Colours of Judging: Workshop on the Reasonable Expectation of Privacy for the Canadian Association of Provincial Court Judges, 14 September 2006), online: On the Identity Trail
<http://www.idtrail.org/files/nji%20workshop/Steeves_NJI_edit.mp3> (podcast) and
<http://www.idtrail.org/files/nji%20workshop/Steeves_NJI_edit.mp3> (presentation slides).

protection in a manner that can only have the effect of significantly shrinking our reasonable expectations of privacy.

3. Reasonable Expectations of Privacy

The reasonable expectation of privacy standard provides a general benchmark for circumstances in which the state is constitutionally permitted to interfere with an individual's privacy interests. The current approach to protecting privacy under section 8 relies first and foremost on establishing the existence of a reasonable expectation of privacy; it is the reasonable expectation that engages section 8 because the "guarantee of security from *unreasonable* search and seizure only protects a *reasonable* expectation [of privacy]."[36] No matter how much a police action may appear intuitively to qualify as a 'search' or 'seizure,' from the point of view of the courts, if no reasonable expectation of privacy can be shown to exist, section 8 will not be engaged. It is only "[i]f the police activity invades a reasonable expectation of privacy, [that] the activity is a search".[37] Determining how much privacy it is reasonable to expect in a given set of circumstances is thereby foundational to any section 8 claim. However, despite prior jurisprudence on this issue, there remains a high level of ambiguity regarding the exact ambit of the section 8 inquiry.[38] In *Tessling*, a Supreme Court acknowledged that, "[p]rivacy is a protean concept, and the difficult issue is where the 'reasonableness' line should be drawn.[39]

Determining the existence of a reasonable expectation of privacy requires consideration of the totality of the circumstances, focusing especially on the existence of 1) a subjective expectation of privacy; and 2) the objective reasonableness of that expectation.[40] The reasonableness of an expectation of privacy includes a consideration of a number of contextual factors, including: (i) the place where the alleged search occurred; (ii) whether the subject matter of the search was on public view; (iii) whether the subject matter had been abandoned or was already in the possession of third parties; (iv) the intrusiveness of the police technique utilized in the alleged search; and (v) whether the information obtained by police exposed core biographical or intimate details of an individual's life. If the accused can demonstrate a subjective expectation of privacy and the objective aspects of the reasonableness test are satisfied, then a reasonable expectation of privacy exists and the court can proceed to ask if the state conduct at issue violated that expectation.

In addition to its legal components, the determination of the reasonable expectation of privacy must be understood in the context of our *risk society*[41] and the escalating

[36] Canada (Director of Investigation & Research, Combines Investigation Branch) v. Southam Inc., (sub nom. Hunter v. Southam Inc.), [1984] 2 S.C.R. 145, 55 A.R. 291 at para. 159 [Hunter v. Southam Inc.] (emphasis in original).

[37] R .v. Wise, [1992] 1 S.C.R. 527, 11 C.R. (4th) 253 at para. 533.

[38] The Supreme Court has amassed an extensive body of section 8 jurisprudence to date. Some of the principal cases include, Hunter v. Southam, supra footnote 36, R. v. Dyment, [1988] 2 S.C.R. 417, 73 Nfld. & P.E.I.R. 13; R. v. Evans, [1996] 1 S.C.R. 8, 131 D.L.R. (4th) 654; Plant, [1993] 3 S.C.R. 281, 145 A.R. 104 [Plant]., and Edwards, supra footnote 15, as well as many of the other cases considered herein.

[39] Tessling, supra footnote 8 at para 25.

[40] First described in Edwards, supra footnote 15 at para. 45.

[41] By this we mean a society that is organized primarily in response to risks. See e.g. Anthony Giddens, "Risk and Responsibility" (1999) 62 Mod. L. Rev. 1. See also Ulrich Beck, Risk Society: Towards a New Modernity, trans. by Mark Ritter (New Delhi: Sage Publications Ltd., 1992).

trend towards high tech surveillance and greater police presence as an appropriate response.[42] In the post-9/11 world, where more and more law enforcement operations are adopting state-of-the-art electronic surveillance technologies capable of tracking and monitoring our day-to-day lives, where with each year we see the establishment of more invasive police practices, privacy, especially for the poor and other disadvantages groups, is an increasingly scarce resource.[43] Our courts have recognized this.[44] So have our legislators. The *Charter* was designed in large measure to safeguard individual interests from unreasonable intrusions by the state.

In a time where electronic surveillance is becoming ever more common, courts must be particularly attuned to the effects of increased law enforcement practices on individual liberties, including our reasonable expectations of privacy. In the past, "Canadian courts have almost instinctively decried the use of technological surveillance without warrant, expressing concern over the grim spectre of an Orwellian society".[45] But, in the midst of the wars on drugs and terror, the 'reasonableness' line is being re-drawn; and there is reason to be concerned about the social implications of its new location.

In light of these deep concerns, we offer a brief analysis of what we believe are the three central danger zones in the judicial approach to the reasonable expectation of privacy: (i) the narrow conception of informational privacy; (ii) the pickwickian logic in the courts' understanding of the relationship between searches and expectations of privacy; and (iii) the non-normative (predictive) conception of reasonable expectations.

3.1. The Narrow Conception of Informational Privacy

The concept of informational privacy was introduced into the academic mainstream by Alan Westin, who famously characterized it 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.[46]

Westin's conception of privacy has been adopted by the Supreme Court of Canada on several occasions.[47] It was also the basis for an international standard for data protection known as *fair information practice principles.*[48]

---

[42] Operation Jetway, *supra* footnote 22, and the war on drugs can be understood as components of the risk society and its correspondent increase in law enforcement and expansion of police presence.

[43] See e.g. John Roach, "New Security Scanner Sees Through Clothes, But With Modesty" *National Geographic News* (27 March 2007), online: NationalGeographic.com <http://news.nationalgeographic.com/news/2007/03/070327-security-scanner.html>; Dan Vergano, "Honeybees Join the Bomb Squad" *USA Today* (27 November 2006), online: USAToday.com <http://www.usatoday.com/tech/science/2006-11-26-bees-bomb-sniffing_x.htm>.

[44] See *e.g.* La Forest J. in *R. v. Sanelli* (1990), 37 O.A.C. 322, (*sub nom. R. v. Duarte)* [1990] 1 S.C.R. 30, 71 O.R. (2d) 575 at para. 24.

[45] Renee M. Pomerance, "Shedding Light on the Nature of Heat: Defining Privacy in the Wake of *R. v. Tessling*" 23 C.R. (6th) 229 at 231. This concern was expressed by Abella J. in the *Tessling Appeal* decision, *supra* footnote 29 at para. 79, where she predicted that "[t]he nature of the intrusiveness [of FLIR technology] is subtle but almost Orwellian in its theoretical capacity."

[46] Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 7.

[47] See *e.g. Tessling, supra* footnote 8 at para. 23; *Edwards, supra* footnote 15 at para. 61; and *R. v. Dyment, supra* footnote 38 at paras. 17, 20.

Informational privacy concerns have various dimensions. One essential dimension is Westin's concern about ensuring informational self-determination. The Supreme Court has adopted a specific threshold for determining whether one holds a reasonable expectation of privacy in personal information, depending on whether it reveals:
a biographical core of personal information …[that] … would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[49]

In other words, as long as identifiable information about an individual is *deemed not to be* core biographical information, there is no reasonable expectation of privacy in that information.

The problem with this approach, as alluded to above, is that information can always be reduced to smaller and smaller bits of data which, through the reductive process, eventually no longer reveal a biographical core of information. For example, in Tessling it was held that "a FLIR image of heat emanations is, on its own … meaningless."[50] The snoop dog cases generally apply the same basic reasoning. Recall in Kang Brown that the majority of the Alberta Court of Appeal held that:

> the dog only yielded a crude piece of information (yes or no to the presence of an unknown quantity of an unknown illegal drug), no intimate details of private lives could possibly be revealed, the odors came out passively, and they were detected by something similar to … an ordinary human nose. There was no reasonable expectation of privacy *for that limited information* in that public place.[51]

Indeed, this is true of every bit of information that is stripped down to its bare datum! But if the courts seriously "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", then it is absolutely imperative that they realize something that only a handful of judges to date have recognized.[52] Namely, that in exactly the same way that wisdom is built from knowledge, knowledge from information, and information from data[53] — *the very same process can be achieved in reverse*. Social meanings are constructed. They are built from bits. In our proliferating world of information technology, where *mashup*[54] is not only an art but a science, the tautology that "[a particular bit of datum] is, on its own, meaningless" is a dangerous proxy for determining which privacy interests get protected and which do not. Well-

---

[48] See *e.g. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD Publications, 1980), online: OECD <www.oecd.org/document/18/0,230,en_269_3255_1815186_1_1_1_1,00.html>.

[49] *Plant, supra* footnote 38 at para. 27.

[50] *Tessling, supra* footnote 8 at para. 58 (emphasis added).

[51] *Kang Brown, supra* footnote 4 at para. 52 (emphasis added).

[52] See *e.g.* the dissent of McLachlin C.J.C. in *Plant, supra* footnote 38, the dissent of Abella J.A. (as she then was) at the Ontario Court of Appeal in *Tessling Appeal, supra* footnote 29 and the dissent of Paperny J.A. in *Kang Brown*, *supra* footnote 4, all of which are discussed below in Part 4.

[53] Jonathan Hey, "The Data, Information, Knowledge, Wisdom Chain: The Metaphorical link" (2004), online: OceanTeacher: A Training Resource for Data and Information Management Related to Oceanography and Marine Meteorology <http://iodeweb5.vliz.be/oceanteacher/index.php?module=contextview&action=contextdownload&id=gen11Srv32Nme37_1590>.

[54] A mashup is the combination of "content from a number of different sources to produce something new and creative." Damien O'Brien & Brian Fitzgerald, "Mashups, Remixes and Copyright Law" (2006) 9 Internet Law Bulletin 17, online: QUTePrints <http://eprints.qut.edu.au/archive/00004239/01/4239.pdf>. See also Declan Butler, "Mashups Mix Data into Global Service" (2006) 439 Nature 6.

established techniques in the field of information technology such as data-mining[55] make it possible for those so-called meaningless bits zooming in and out of the ether of global networks and public and private databases to be quickly and inexpensively re-assembled,[56] in the language of the courts, "to reveal intimate details of the lifestyle and personal choices of the individual."[57]

In light of the challenges created by primary and secondary uses of information within and without global digital networks, wireless communications and computational devices, the courts must adopt a much broader conception of informational privacy, one which recognizes the power of *dataveillance*[58] and the ease with which data shadows and clusters can be used to construct digital personae that precisely and accurately link them to their meatspace counterparts.[59]

3.2. The Pickwickian Relationship Between Searches and Expectations of Privacy

When approaching the matter from the perspective of basic intuitions and common sense, most folks would likely acknowledge that it is relatively easy to identify the constituent factual elements of a 'police search' in most situations. Yet as we have seen, the courts have deemed that there is no search where there is no reasonable expectation of privacy, making a judicial determination about the existence of a search wholly contingent upon the murky concept of privacy.[60] This seems neither logical nor practical.

Moreover, the seemingly fact-oblivious[61] approach to defining police searches for the purposes of section 8 is particularly problematic in light of the recent trend toward conceptualizing and defining the nebulous notion of privacy in terms of informational privacy.[62]

For these reasons we suggest, once again, that courts must take care not to engage in an excessively reductionist approach to informational privacy—*lest we risk a reduction to absurdity.* As soon as we begin characterizing police activities outside of their social context – once uniformed police officers locking down a high school while their search dog randomly snoops the halls (without reasonable and probable grounds to believe that an offence has been committed) is explained away as a *crude, passive*

---

[55] See Joseph S. Fulda, "Data Mining and Privacy" (2000) 11 Alb. L.J. Sci. & Tech. 105 at 106.

[56] See Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (California: O'Reilly Media Inc., 2000).

[57] *Plant, supra* footnote 38 at para. 27.

[58] Roger Clarke defines dataveillance as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons." Roger Clarke, "Information Technology and Dataveillance" (1988) 31 Communications of the ACM 498,

[59] See Daniel J. Solove, *supra* footnote 3.

[60] Judges and academics alike continue to struggle with what, exactly, privacy looks like or includes. See *e.g.* Adam D. Moore, "Privacy: Its Meaning and Value" (2003) 40 American Philosophical Quarterly 215; Shaun MacNeill, "A Philosophical Definition of Privacy" (1998) 78 Dalhousie Review 437; Richard Volkman, "Privacy as Life, Liberty, Property" (2003) 5 Ethics and Information Technology 199.

[61] This approach is *not* fact-oblivious in the sense that no facts or circumstances are considered. It is fact-oblivious in the sense that the fact of whether there was a search is contingent on conceptual rather than factual determinations of informational privacy and how that concept is understood by a particular court.

[62] See *Tessling, supra* footnote 8 at para. 27. This trend is further exemplified in *R. v. McLay, supra* footnote 13 at para. 34, where, relying on the finding in *Tessling* that FLIRs were an external, non-intrusive police technique and "mundane in the data produced," the Court held that the same could be said of dog sniffing.

and ordinary smell of chemical compounds seeping through a backpack – we are sure to fail to appreciate the broader social significance of these forms of State action.

3.3. The Non-Normative Conception of 'Reasonable Expectations'

Without Constitutional deterrents or remedies in place, privacy-invasive investigatory techniques will inevitably become standard police practice and, once they are accepted as such, this will have an impact on people's reasonable expectations. Whether privacy-invasive or not, once an investigatory technique is standard practice, it soon becomes *unreasonable* for people to expect the police to act in any other way. This ultimately leads to an erosion of the normative commitment to privacy-friendly police practice.

Some may argue that our concern about a diminishing normative commitment to the reasonable expectation of privacy standard is sheer conjecture, and that a *Charter* protected right like privacy is not so fragile. There is, however, caselaw that perfectly illustrates our concern. For example, in *R v. McCarthy*,[63] a case dealing with evidence obtained through an Operation Jetway dog sniff at a train station in Truro, the Provincial Court for Nova Scotia was explicit in asserting that since the accused must have known that the use of dogs to sniff out drugs was regular police practice, he could not reasonably expect to maintain his privacy with regard to smells emanating from his belongings:

> The accused chose to travel by public transport which would provide no control or protection from others entering his immediate space. The use of dogs by police was known and he was aware of the effect of passing in close proximity of such a dog. The use of trained police dogs to detect the scent of contraband in public areas such as train, bus and airplane depots is a legitimate police investigatory tool and does not infringe on any legitimate privacy interest protected by section 8 of the *Charter*.[64]

This line of reasoning strips the notion of 'expectation' of its normative commitments and is *highly problematic* in light of *Tessling*, where Binnie J. forcefully proclaimed that, "[e]xpectation of privacy is a normative rather than a descriptive standard."[65] The contrary approach, adopted in *McCarthy* and a number of other cases, reduces our privacy expectations to little more than factual *predictions* about police behaviour and guesses about the kinds of technologies they are likely to employ. On this approach, our privacy expectations are no longer about how police *ought* to behave, only about how they *will* behave. Such an approach eradicates the expectation of privacy from the realm of what is *reasonable* in a given situation, recasting it in light of that which is merely *foreseeable* in a particular set of circumstances.[66] The emphasis is no longer on the individual and her or his right to be secure from unreasonable state intrusions, but instead concentrates on police action, relegating rights, at best, to an incidental consideration.

---

[63] *McCarthy*, *supra* footnote 11.
[64] *Ibid.* at para. 36.
[65] *Tessling, supra* footnote 8 at para. 42.
[66] See *Bolton v. Stone*, [1951] A.C. 850 (H.L.), where Lord Reid discussed the distinction between foreseeability and reasonableness in the context of torts, holding that whether the defendant had a duty to the claimant to take precautions had to take into account the foreseeability of the risk and the cost of measures to prevent the risk.

By adopting a *predictive* rather than a normative approach to our expectations of privacy, the snoop dog jurisprudence, for the most part, departs from the domain of democracy, rights and interests. Instead, it concerns itself primarily with current standards of police practice and the technological state-of-the-art. The *McCarthy* case nicely demonstrates the crucial problem with stripping the reasonable expectation standard of its normative meaning: once an expectation is understood as nothing more than an external prediction, all one needs to do to alter the reasonable expectation of privacy standard is to engineer a change in peoples' expectations. The same holds true in the other direction. In order to change people's expectations, one need only change the standard.

The predictive rather than normative approach adopted in the snoop dog jurisprudence and in other section 8 cases is a danger zone because it has the inevitable effect of diminishing our reasonable expectations of privacy, especially, the level of privacy we enjoy in public spaces.[67] Without a normative dimension to the analysis firmly in place, those so-called reasonable expectations are quickly eroded in light of easily engineered factual circumstances.

We live in interesting times. There is good reason to *predict* swift and extraordinary technological developments in the coming decade,[68] including powerful though physically unobtrusive forms of digital surveillance that lie just around the corner.[69] These predictions should give courts pause, not only with regard to a narrow conception of informational privacy and a logic that renders the determination of privacy standards conceptually prior to the characterization of the nature and scope of police activity, but also with regard to the courts' increasingly predictive rather than normative approach to reasonable expectations of privacy.

Thankfully, none of the three danger zones discussed above is an inherent element of a sound approach to the reasonable expectation of privacy, even within the context of *Tessling* and other informational emanations such as the snoop dog cases.

In fact, the reasoning of the majority of the Supreme Court in the snoop dog cases advanced a more compelling reading of *Tessling* that leads to a different and superior result not only in the resolution of the snoop dog jurisprudence but also from the perspective of those who wish to carve out a democratic and autonomous space for reasonable expectations of privacy in spite of shifting police standards and a rapidly developing surveillance society.[70]

---

[67] See Helen Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public" (1998) 17 Law & Phil. 559.

[68] See *e.g.* Ray Kurzweil, *The Singularity is Near: When Humans Transcend Biology* (New York: Viking Penguin, 2005).

[69] For instance, technologies to monitor electrical activity in and around the human body are under development, including a new application of electroencephalograms (EEG) technology, which allows researchers to determine whether or not an individual is in possession of knowledge related to a crime scene based on electricity emanating from the human skull. See *Harrington v. Iowa* (659 N.W. 2d 509 2003). See also Paul Root Wolpe, Kenneth R. Foster & Daniel D. Langleben, "Emerging Neurotechnologies for Lie-Detection: Promises and Perils: (2005) 5 Am. J. of Bioethics 39. Another technology used to capture information emitted by the brain is Functional Magnetic Resonance Imaging (fMRI), which is being used by law enforcement for truth verification and lie detection purposes. See *e.g.* Langleben et. al. "Telling truth from lie in individual subjects with fast event-related fMRI" (2005) 26 Hum. Brain Mapp. 262.

[70] See *e.g.* David Lyon, *Surveillance Society: Monitoring Everyday Life* (Philadelphia: Open University Press, 2001).

4. Snoop Dogs at the Supreme Court

In the preceding parts of this article, we have highlighted the likely dangers in a narrow application of *Tessling* to analogize generally to other kinds of emanations, like odours, and its ultimate effects on our reasonable expectations of privacy in light of vast amounts of knowable information emanation.[71]

Did the *Tessling* court truly intend to grant police a licence to intercept *any* information that emanates from a private place into the public domain? Or might a more fitting approach to *Tessling* be that its outcome is *not* generally applicable to searches involving snoop dogs, or for that matter, to any other surveillance technology involving information emanations?[72]

The Supreme Court of Canada answered these questions in its 2008 reasons in *A.M.* and *Kang Brown*,[73] concluding that both A.M. and Kang Brown had reasonable expectations of privacy in the odors emanating from their bags. In both cases, the majority of the Supreme Court concluded that the warrantless police dog sniff of the accused's bag was a violation of his constitutional right to be secure against unreasonable search and seizure. In doing so, the Court explicitly addressed our three concerns articulated above, (i) rejecting the notion that, by analogy, *Tessling* stands for the general proposition that emanations into public spaces never attract a reasonable expectation of privacy; (ii) rejecting the reductionist approach to informational privacy; and (iii) affirming the importance of the normative content of the reasonable expectation of privacy. These cases represent significant advancement towards a robust privacy protection in a digital age.

In *A.M.* Binnie J. put to rest any notion that *Tessling* is a precedent of general application by way of analogy. The outcome in *Tessling* – that a FLIR image of heat emanations is, on its own … "meaningless" [74] - was never intended to be a generalization used to characterize all possible forms of emanating information that could be reduced to abstract bits of data. Acknowledging that both the heat in *Tessling* and the odor in *A.M.* and *Kang Brown* could be characterized as emanations, Binnie J. was of the view that the similarities between the cases stopped there:

> …[T]he information provided by a drug-dog sniff…is entirely unlike a FLIR image in that it most definitely permits inferences about the precise contents of the source that are of interest to the police. Under the Operation Jetway program at issue in *Kang-Brown*, a positive alert by a sniffer dog was *itself* taken by the police as reasonable and probable grounds for an arrest. However, the subject matter of the sniff is not public air space. It

[71] In addition to its application in the snoop dog cases, *Tessling* has also been widely referred to in other section 8 jurisprudence, including about a dozen digital recording ammeters (DRA) cases: See *e.g. R. v. Rayment*, 2006 ABQB 132; *R. v. Haskell,* 2004 ABQB 474; (2004) 33 Alta. L. R. (4th) 200*; R v Gomboc,* 2010 SCC 55, [2010] 3 S.C.R. 211 [*Gomboc*].

[72] This was the position of Paperny J.A. in dissent in *Kang Brown*, *supra* footnote 4 at paras. 106-108 and 134, and Armstrong J.A. for the Ontario Court of Appeal in *A.M.*, *supra* footnote 7 at para. 47. A number of scholars and practitioners have expressed similar concerns about the application of *Tessling* to other police practices, see e.g. Renee M. Pomerance, *supra* footnote 45 at 229-30; Don Stuart, "Police Use of Sniffer Dogs Ought to Be Subject to *Charter* Standards: Dangers of *Tessling* Come to Roost" 31 C.R. (6th) 255; James A.Q. Stringham, "Reasonable Expectations Reconsidered: A Return to the Search for a Normative Core for Section 8?" 23 C.R. (6th) 245; Lisa Austin, "One Step Forward or Two Steps Back? *R. v. Tessling* and the Privacy Consequences for Information Held by Third Parties" (2004) 49 Crim. L.Q. 22.

[73] *A.M. SCC*, *supra* footnote 9; *Kang Brown SCC, supra* footnote 9.

[74] *A.M. SCC, supra* footnote 9 at para. 58.

> is the concealed contents of the backpack. Dog sniffing is…a "through-the-wall" technology…[75]

Binnie J. further distinguished *Tessling* by pointing out that in *Tessling* the heat information captured by the FLIR had "…already escaped the possession and control of the suspect" whereas A.M. had a continuing expectation of privacy in the enclosed space of his backpack.[76] As a result, the *Tessling* precedent was of little direct relevance in the snoop dog analysis at the Supreme Court.

Avoiding the danger zones of the reductionist 'heat-equals-odor' analogy, Binnie J. measured A.M.'s expectations of privacy in the context of the factual circumstances surrounding the police investigation, including, of course, the use of the snoop dog. Recognizing that police dog sniffing "…cannot be treated as an isolated phenomenon…detached from the broader police conduct,"[77] the majority noted the sole reason the police attended the high school in *A.M.* was to conduct a "random search" for drugs; the actual "sniff" of A.M.'s backpack could not be removed from this broader police context.[78] Also relevant were the investigatory objectives of police in conducting the search; that is, a consideration of *why* the police were interested in the item or place being searched.[79] It was clear that the police in *A.M.* were not interested in the backpack itself, which was in plain view in the school gymnasium, but rather its contents, which were protected from public scrutiny. Because snoop dogs can "sniff through the wall," the information gleaned from dog sniffs was characterized by the majority of the Court not as a meaningless "scrap" of data relevant only as part of a bigger picture, but significant in and of itself, "…the sniffer dog's equivalent of a smoking gun."[80]

Even if the dog sniff revealed information about A.M. that was significant to police, the Crown argued that the information was not part of a "biographical core of personal information", and thus did not attract section 8 protection. Binnie J. clarified that the "biographical core of personal information" classification for finding a reasonable expectation of privacy, first recognized in *Plant*, was not intended to be conclusive of the informational privacy analysis. It does not automatically exclude from protection all information that fails to meet this threshold.[81] The information about A.M. collected by the dog sniff was entitled to constitutional protection regardless of whether it fell into the "biographical core" basket because it "…was specific and meaningful information, intended to be private, and concealed in an enclosed space in which the accused had a continuing expectation of privacy."[82]

The fact-specific, contextual approach adopted by the majority in *A.M.* makes real the assertion by Binnie J. in *Tessling* that the "[e]xpectation of privacy is a normative

---

[75] *Ibid* at para. 66.
[76] *Ibid* at para. 67.
[77] *Ibid* at paras. 38, 76.
[78] *Ibid* at para. 76.
[79] *Ibid* at para. 37-38
[80] *Ibid* at para. 38.
[81] *Ibid* at paras. 67-68.
[82] *Ibid* at para. 67. See Jane Bailey, "Across the Rubicon and into the Apenninies: Privacy and Common Law Police Powers after *A.M.* and *Kang Brown*" (2009) 55 Crim. L. Q. 239 at 266, who points out that despite the clarification in *A.M.* that more than core biographical information is protected by section 8, "...it still remains unclear exactly what other kinds of information are covered an in what situations the non-biographical nature of the information will be fatal in terms of crossing the constitutional threshold."

rather than a descriptive standard."[83] In *A.M.,* Binnie J. reiterated that any judicial assessment of the reasonable expectation of privacy must be made with a view to the "…type of society which Canadians, by their adoption of the *Charter*, have elected to live in."[84] In contrast to the descriptive approach adopted by Deschamps and Bastarache JJ., in dissent in *A.M.*, the majority declined to find that the regulated school environment, the existence of a well-publicized zero-tolerance drug policy at A.M.'s school, and warnings given to students about the possibility of random drug searches, were sufficient to render A.M.'s expectation of privacy in the backpack objectively unreasonable.[85]

In denying the application of *Tessling* as a general standard and adopting a fact-specific, context-sensitive vantage point imbued with normative content, the majority of the Supreme Court in *A.M.* and *Kang Brown* (where Binnie J. conducted a similar analysis to assess the reasonable expectation of privacy) took a decisive step away from the decontextualized, abstract reasoning we caution against in this article and previously.[86] Instead of endorsing the reductionist inclination, which asks whether the intercepted data is, *on its own*, meaningless, the majority of the Supreme Court adopted the very opposite approach, namely: asking whether the bundle of information that is made available by means of the search, *once assembled,* ought to attract a reasonable expectation of privacy. The Court's more robust approach recognizes the jigsaw nature of the data/information/knowledge/wisdom chain[87] and the importance of each piece of the puzzle in telling a story despite the fact that no single piece could do so on its own, suggesting a broader threshold of protection for informational privacy.[88]

5. An Ongoing Risk of Reductionism?

The express rejection of the reductionist approach in *A.M.* and *Kang Brown* is good news for informational privacy—and other countries should take notice. Yet, it is difficult to imagine that the debate about "drawing the reasonableness line"[89] has been finally and definitively resolved in Canada, let alone across the global privacy jurisprudence. For example, one particularly incisive scholar has called into question the usefulness of the distinctions drawn between *Tessling* and the snoop dog cases for aiding future courts in making principled distinctions between different kinds of emanations captured by different kinds of technologies.[90] We agree and maintain that courts will need to continue to remind themselves over and over about the absurdity of information reductionism and its opaque tendency to obliterate existing social norms,

[83] *Tessling, supra* footnote 8 at para. 42.
[84] *A.M. SCC, supra* footnote 9 at para. 38.
[85] *Ibid* at para. 65; and see Deschamps J. in dissent, *ibid* at paras. 159-160.
[86] *Kang Brown SCC*, *supra* footnote 9 at para. 26. The *Kang Brown* appeal focused primarily on the question of whether police have a common law power to use sniffer dogs in the course of their investigations, and if so, what standard of suspicion the police must have to undertake a sniffer search.
[87] See Jonathan Hey, *supra* footnote 53.
[88] See James M. Nyce & Paul Kahn, eds., *From Memex to Hypertext: Vannevar Bush and the Mind's Machine* (San Diego, CA: Academic Press, 1991).
[89] *Tessling, supra* footnote 8 at para. 25.
[90] See Bailey, *supra* footnote 82 at 269-270, who argues that if the approach taken in *A.M.* – focusing on the *inferences* that could be drawn about the contents of the backpack based on the odour emanating from within – had been applied to the heat emanating from the home in *Tessling*, "…the subject-matter would not have been the uncontrollable heat emanations, but the inferences the FLIR images of those emanations allowed police to draw regarding the otherwise concealed activities going on in Tessling's home."

particularly given the rapid pace of technological change in fields like biometrics, ubiquitous computing, genetics, robotics and nanotechnology.

Indeed, information reductionism has already reared its head in the early days of the digital era in *R. v. Gomboc*—a 2010 decision where the Supreme Court of Canada had its first opportunity to consider the reasonable expectation of privacy in digital information (about residential electricity use) disclosed by the unauthorized use of a digital recording ammeter (DRA) by police.[91] DRAs are connected to the electrical supply line of a residence of interest, where they track the cycles of electrical consumption, distribution loads and power quality.

The facts of *Gomboc* were similar to *Tessling*. Based primarily on their observations of Gomboc's home, Calgary police suspected that the accused was growing marijuana and asked the local utility company to install a DRA to monitor the electricity consumption at the property. The utility company complied. The DRA analytics of the hydro consumption patterns at Gomboc's home—sufficiently sophisticated to recognize the cyclical pattern of plant-based photosynthesis—revealed the likelihood of a marijuana grow-op. Based on their observations and the DRA evidence, a warrant was obtained and police searched the house, seizing bulk marijuana and items relating to a grow-op. Gomboc was charged with producing marijuana and possession for the purpose of trafficking, and at trial he was convicted.[92]

The majority of the Alberta Court of Appeal allowed the appeal, concluding that the warrantless use of the DRA by police had violated Gomboc's reasonable expectation of privacy in the information contained in his electricity consumption patterns. Martin J.A. distinguished the DRA from the FLIR technology in *Tessling*, finding that the DRA evidence was "…more intrusive and more revealing" and "…must, as a matter of common sense, also disclose biographical or private information; for example, the approximate number of occupants, when they are present in the home, and when they are awake or asleep."[93] In dissent, O'Brien J.A. applied *Tessling* by analogy, finding there was little to distinguish heat emanations from electricity consumption patterns and concluding that, "[l]ike the FLIR image, the disclosure of the DRA graph scarcely affects the 'dignity, integrity and autonomy of the person whose house is subject of' the graph."[94]

In three separate decisions, the majority of the Supreme Court ultimately allowed the Crown's appeal and restored Gomboc's conviction.[95] On the specific question of whether the information captured by the DRA attracted section 8 protection, the Court split 5:4 in favour of the non-reductionist approach established in *A.M.* and *Kang Brown*. In separate decisions penned by Abella J., and McLachlin C.J. with Fish J., five members of the Court endorsed an analysis situating the DRA information in the context of the investigatory objectives of police. Both decisions focused on the

[91] *Gomboc*, *supra* footnote 71.

[92] *R. v. Gomboc*, 2007 ABQB 794, [2007] A.J. 1576.

[93] *R. v. Gomboc*, 2009 ABCA 276, [2009] 247 CCC (3d) 119; 11 Alta LR (5th) 73 at paras 16-17 [*Gomboc Appeal*].

[94] *Ibid* at para.77, citing *Tessling, supra* footnote 8 at para. 63.

[95] The ultimate disposition of the appeal turned on varying interpretations of the impact of a provincial statutory scheme governing the relationship between homeowners and utility companies, which included a provision stipulating that a homeowner may request that his/her "customer information" be kept confidential. In the absence of such a request, the utility company is authorized by the statute to disclose customer information to the police for the purpose of investigating an offence: *Gomboc*, *supra* footnote 71 at paras. 55-56.

electrical consumption information not as an isolated data byte but as giving rise to a "…strong and reliable inference…" of very personal information – the presence of a marijuana grow-op in Gomboc's home.[96]

However, Deschamps J., writing for herself and three other judges, revitalized the reductionist approach to informational privacy. Finding no reason to distinguish the DRA data from the heat signature information in *Tessling*,[97] Deschamps J. concluded that the DRA technique "…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".[98] Relying on the "biographical core data" standard qualified by Binnie J. in *A.M.*, Deschamps J. was of the view that the disclosure of electricity consumption information to police yielded no meaningful information "…in terms of biographical core data that attracts constitutional protection."[99]

The narrow margin by which the Supreme Court divided on its reasonable expectation of privacy analysis in *Gomboc* suggests an ongoing concern for privacy advocates as we migrate deeper and deeper into digital environments: the continuing risk of the resurgence of the reductionist approach to informational privacy in the context of new and emerging information-capturing technologies. As the art and science of discovering and understanding the information that people and things emanate surges fast-forward toward the future, proliferating exponentially in an era where our intelligence will become increasingly nonbiological and trillions of times more powerful than it is today,[100] we suggest that the resolution of the snoop dog cases has not ended the debate that started well over a decade ago in the dissenting position in *Plant,* where our Chief Justice (as she now is) had the somewhat prescient realization that intangible data of this sort "are capable of telling much about one's personal lifestyle ... The records tell a story."[101]

Conclusion

In this article, we have examined a problematic judicial approach to the reasonable expectation of privacy in odour emanations and tried to point out its potential dangers as we skip forward to the digital age. We highlighted the promising move by the Supreme Court away from the treacherous terrain of information reductionism and warned of the ongoing risk of reductionist reasoning in light of new and emerging digital technologies designed to capture our information emanations.

This ending, however, is really just a beginning. It is a realization and an appreciation of that which lurks around the corner. If we are to maintain our "dignity, integrity and autonomy"[102] in the face of emerging surveillance technologies that are capable of assembling bits and bytes in order to re-tell the stories of our personal lives without our permission and yet in ways that are personally and territorially unobtrusive, our courts must continue to confront the social implications of informational privacy, interrogating its meaning in an empirical universe of information emanation. The

[96] *Ibid* at para. 81 (Abella J.). McLachlin C.J. and Fish J. agreed, *ibid* at para. 124.
[97] *Ibid* at para. 38.
[98] *Ibid* at para. 14 (Deschamps J.).
[99] *Ibid* at para. 43 (Deschamps J.). See also *ibid* at para. 36.
[100] See Ray Kurzweil, *supra* footnote 68.
[101] *Plant*, *supra* footnote 38 at para. 48.
[102] *Ibid.* at para. 26.

escalating challenge that informational privacy is sure to present will require Canadian courts to confront difficult decisions that lie ahead: (i) when it is appropriate to focus specifically on the 'nature and quality' of the information that a given technology can currently deliver,[103] and (ii) when it is appropriate to look more broadly at its 'theoretical capacity'.[104]

Once the power of information technology (and its ability to reconfigure what was once meaningless bits of information) sufficiently reinforces the Chief Justice's concern about the extent to which it tells our life stories, we predict that the courts will be forced to advance a much more robust approach that significantly increases the threshold of protection for informational privacy. It is perhaps even possible that that the "off the wall/through the wall" distinction[105] might, like the wall itself, come tumbling down.

As the song goes, "the future is but a question mark."[106]

[103] *Tessling, supra* footnote 8 at para. 28-29.
[104] *Tessling Appeal, supra* footnote 35 at para. 79.
[105] See *supra* footnote 32.
[106] Sting, "Bring on the Night" on *Bring on the Night* (A&M Records: 1986) track 1.