CRIMINAL LAW QUARTERLY
VOL. 52 (3)
FORTHCOMING 2007

EMANATIONS, SNOOP DOGS AND REASONABLE EXPECTATIONS OF PRIVACY

Ian Kerr[*] and Jena McGill[**]

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] and other Neo-Platonists,

---

[*] Canada Research Chair in Ethics, Law & Technology, Faculty of Law, Faculty of Medicine, Department of Philosophy, University of Ottawa (iankerr@uottawa.ca).

[**] LL.B/M.A. candidate, University of Ottawa, Faculty of Law and Carleton University's Norman Paterson School of International Affairs (jmcgi032@uottawa.ca).

The authors wish to express their thanks to the Social Sciences and Humanities Research Council, the Canada Research Chairs program, Bell Canada and the Ontario Research Network in Electronic Commerce for their generous contributions to the funding of the research project from which this article derives. Special thanks also to the amazing Susan Lightstone and the National Judicial Institute for providing the opportunity to examine the jurisprudence concerning the reasonable expectation of privacy as part of a special, one day workshop 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/content/view/529/89/>. Thanks also to Professor Valerie Steeves, Professor Jane Bailey and Carole Lucock for their insightful feedback, which substantially improved the quality of this article. Finally, we wish to convey our deep gratitude to Dr. Hilary Young, Katie Black, Cynthia Aoki and Shoshana Magnet for their extraordinary efforts, their brilliance, and for the high quality of research support that they so regularly and reliably provide.

[1] Plotinus developed a complex spiritual cosmology involving three hypostases: the One (god), the Intelligence and the Soul. In *The Six Enneads* (Book II, iii. 8), he asserts, "[o]ne principle must make the universe a single complex living creature, one from all." Plotinus' theory that all things are emanations *ex deo* ("out of god") confirms the omnipotence of god and makes the unfolding of the universe a consequence of god's existence. The emanations from god do not diminish or lessen god, and Plotinus uses the analogy of the sun which

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 world view, 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.

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, information about a body's temperature profile from radiating heat and sweat, 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,

---

radiates light indiscriminately without "lessening" itself. See Plotinus, *The Six Enneads* (Whitefish, MT: Kessinger Publishing, 2004).

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.[4] 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. Best of all, from the perspective of those who employ them, these techniques are generally non-invasive insofar as they can be used to obtain incriminating evidence without transgressing property lines or invading one's personal space.

In this article, we focus on a primitive example: using behavioural science techniques to train dogs to perceive the scent of illicit drugs. With an extremely high degree of accuracy,[5] 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. In fact, 'snoop

---

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); Roger Clarke, "Information Technology and Dataveillance" (1988) 31 Communications of the ACM 498.

4 Not to mention marketers and other private sector entities.

5 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% to 92% accurate.

dogs' can be trained to identify all sorts of smells or sounds emanating from all kinds of personal effects. For instance, in a recent anti-piracy campaign sponsored by the Motion Picture Association of America (MPAA), dogs were trained to sniff-out polycarbonates – a by-product of freshly burned CDs and DVDs. The MPAA now proposes the use of DVD-sniffing dogs at airports, seaports and other locations where bootleg songs and movies might be transported.[6]

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 *Charter* scrutiny?[7] 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?

These are questions that the Supreme Court of Canada has been asked to address on May 22, 2007, when it hears a joint appeal of two snoop dog cases - one from Alberta[8] and the other from Ontario.[9] Although it is tempting to view this hearing as a specialized criminal law inquiry circumscribed by the narrow confines of the law of search and seizure, we suggest that these cases, like the Supreme Court's earlier decision in *R. v. Tessling*,[10] raise broad and important questions about the nature of privacy and autonomy in a world of ubiquitous information emanation.

In anticipation of the *Kang Brown* and *A.M* hearing, our aim in this article is to explicate five main points. First, we contend that the majority of snoop dog decisions in Canadian

---

6 "Dogs Trained to Sniff Out Movie Piracy" *NBC4* (28 September 2006), online: NBC4.TV <http://www.nbc4.tv/news/9956775/detail.html>. Similarly, packet sniffers and other software are regularly used to achieve the same effect online. See *e.g.* Robert Graham, *Sniffing (network wiretap, sniffer) FAQ*, online: <http://web.archive.org/web/20050221103207/http://www.robertgraham.com/pubs/sniffing-faq.html>.

7 *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."

8 *Kang Brown*, *supra* footnote 5.

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

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

courts[11] have been wrongly decided; they rely on an inappropriate use of judicial analogy that stems from a misreading of *Tessling.* Second, we warn against an excessively reductionist approach to informational privacy adopted in many recent reasonable expectation of privacy cases.[12] Once police activities are understood as nothing more than 'capturing heat emanating from the wall of a building' or 'intercepting chemical emissions oozing through a backpack', it is no longer possible to appreciate the *deep social significance* of RCMP planes beaming infrared lights at our homes in the middle of the night or police officers and their guard dogs randomly patrolling our high schools, bus stations and city streets. Third, we warn against a non-normative approach to 'reasonable expectations' that is also gaining currency in several provincial courts across Canada.[13] No longer centered on democracy, rights, duties or even interests, privacy discourse is shifting towards an inquiry about state of the art technologies and current standards of police practice. As such, the 'reasonable expectations' test has become a strange kind of factual inquiry. Fourth, we propose a different reading of *Tessling*, one that is better suited to the snoop dog cases and, perhaps more importantly, for subsequent application in cases concerning emerging high tech surveillance. Finally, we point to the future, suggesting that *A.M.* and *Kang Brown* are not just about snoop dogs; these two cases foreshadow the future of emanation information in a networked society.

On the whole, we suggest that a failure to clarify *Tessling* in the snoop dog cases and in the broader context of ubiquitous information emanation, especially alongside the

---

[11] Of approximately fourteen lower court Canadian cases involving the admissibility of evidence gained through police use of snoop dogs, nine have found and five have held that the dog sniff does qualify as a search and attracts section 8 scrutiny. It is notable, however, that of these five cases, three were decided pre-*Tessling*. Of the nine cases finding that the use of snoop dogs did not qualify as a search, seven were made in the aftermath of the Supreme Court's 2004 decision in *Tessling, supra* footnote 10, and considered or relied on the *Tessling* decision.

[12] 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.

[13] See *e.g. R. v. McCarthy*, 2005 NSPC 49, 239 N.S.R. (2d) 23 [*McCarthy*]. Further discussion of the non-normative approach to expectations adopted in *McCarthy* is at Part 3 (iii), below.

maintenance of reductionist, non-normative approaches to informational privacy across Canadian courts could seriously diminish the privacy rights of Canadians in a manner that the Supreme Court of Canada has until now been very careful to guard against.

In Part 1, we commence with a discussion of the two snoop dog cases presently before the Supreme Court of Canada. 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 current approach adopted in the majority of snoop dogs cases decided in Canada to date: (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 Part 4, we offer what we think is a much more compelling reading of *Tessling*, arguing that its tailored conclusions concerning the current state of FLIR technology was never meant to provide a categorical approach of general application to other instances of information emanations, including police dogs sniffing odours emanating from backpacks. In Part 5 we offer our conclusions as well as some speculation about the future evolution of informational privacy in an age of ubiquitous information emanation.

1. The Snoop Dog Cases

In the dozen or so reported Canadian cases at bar, a slim majority[14] have held that the use of police dogs in an investigation *does not* constitute a 'search' within the meaning of section 8 of the *Charter* and therefore *does not* trigger the constitutional safeguards that accompany "the right to be secure against unreasonable search or seizure."[15] The legal basis for most of these 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

---

[14] See *supra* footnote 11 and accompanying text.

[15] *Charter, supra* footnote 7 at s.8.

had a reasonable expectation of privacy."[16] Extending the reasoning of this decision by way of analogy, many courts[17] have subsequently reasoned that external patterns of odour on the external surface of a backpack or locker are not information in which an accused has a reasonable expectation of privacy.

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.[18] 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*.[19] 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,[20] to dogs sniffing rental cars on public highways,[21] to dogs randomly sniffing school gymnasiums.[22] 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 should also come as no surprise that the Supreme Court has recently been asked to resolve cases from two appellate courts that seem to go in opposing directions. We now turn to those two appellate decisions.

---

16 *Tessling*, *supra* footnote 10 at para. 63. *Tessling* did not involve snoop dogs. At issue was a more sophisticated emanation detection system called Forward Looking Infrared (FLIR) technology. We discuss this decision in greater detail in Parts 2 and 4, below.

17 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 13; *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 5.

18 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 9.

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

20 See *e.g. Kang Brown, supra* footnote 5; *McCarthy, supra* footnote 13; *R. v. Dinh*, *supra* footnote 18; and *R. v. Buhay, supra* footnote 18.

21 See *e.g. R. v. Davis*, *supra* footnote 17; *R. v. Peardon*, *supra* footnote 17.

22 See *e.g. A.M., supra* footnote 9.

In *R. v. A.M.*, the principal of a Sarnia high school issued a standing invitation to police officers to conduct searches as part of the high school's *zero tolerance* policy on drugs. Two years later, without any prompting from the school, 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. Based on the dog's reaction to the bag, the police conducted a search of the backpack where they 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 evidence from his backpack should be excluded under section 24(2) of the *Charter*[23] because it was obtained through an unreasonable search and therefore violated section 8 of the *Charter*.[24] Although the Crown argued on appeal that an abandoned backpack in the middle of a school gym was not a prime candidate for a reasonable expectation of privacy, the Ontario Court of Appeal dismissed the 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.* Writing for a unanimous majority, Armstrong J. was very 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.[25]

The core facts in the second case under appeal, *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

---

[23] *Charter*, *supra* note 7 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."

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

[25] *A.M., supra* footnote 9 at para. 47.

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.[26] After watching Kang Brown and identifying certain behaviours deemed 'suspicious,'[27] the officer spoke to the accused regarding the nature of his travel. Once the second officer in control of a police dog joined in the conversation, the trusty companion quickly indicated the presence of drugs in Kang Brown's baggage, leading the officers to search the bag, where they

---

[26] Operation Jetway was developed in the United States and has been employed across Canada for about ten years. The program is intended to target travelers who look 'out of the norm' with respect to their clothing, behaviour or demeanor. Once an officer has identified a 'suspicious' looking individual, the target is approached by the officer and his or her police dog, and is engaged in 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. Police describe these interactions as strictly consensual, since the officer identifies him or herself as a member of the police and the targeted individual is (in theory) free to walk away at any time. If the officer observes further 'unusual' behaviour by the target, the conversation may become more personal in nature, and the officer may demand to see travel tickets or identification documents or ask that the target 'consent' to a baggage search. Of course, most targeted individuals capitulate, believing that they do not have any real choice in the matter when faced with such a demand from a police officer. Even if a target refuses a baggage search, however, the police dog can do with its nose what the officer may not be permitted to do with his or her hands and eyes; that is, the dog will determine the contents of a target's baggage by reacting to certain forms of contraband. 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.

[27] These 'suspicious behaviours' included prolonged eye contact with a plainclothes officer who was watching passengers disembark from the bus, having luggage with no identification tags, stopping suddenly as he was about to leave the bus depot and looking behind him and picking up his luggage and hoisting it onto his shoulder at several intervals. See *R. v. Kang Brown,* 2005 ABQB 608, 386 A.R. 48 at paras. 53-54. It is notable that while there is no evidence that Operation Jetway explicitly encourages officers to rely upon race-based stereotypes and assumptions in choosing which passengers to stop and question, it seems reasonable to infer that this is a factor (unconscious or otherwise) in Operation Jetway, particularly considering the American experience with similar programs and in light of the evolving body of literature on the unconscious effects of race that inform suspicion. See *e.g.* David M. Tanovich, "Using the Charter to Stop Racial Profiling: The Development of an Equality-Based Conception of Arbitrary Detention" (2002) 40 Osgoode Hall L.J. 145 at 152; David M. Tanovich, "The Colourless World of *Mann*" (2004) C.R. (6th) 47; D.A. Harris, *Profiles in Injustice: Why Racial Profiling Cannot Work* (New York: New Press, 2002); D.A. Harris, "The Stories, the Statistics and the Law: Why 'Driving While Black' Matters" (1999) 84 Minn. L. Rev. 265 at 275-288.

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.[28]

At trial, the judge found no breach of Kang Brown's section 8 rights because emissions from a private place voluntarily placed into the public domain are easily detected by police (either using their own senses or technological enhancement). Therefore, the odour emanating from Kang Brown's bag was not information in which he could have held a reasonable expectation of privacy. The judge concluded there were no *Charter* breaches, admitted the evidence and convicted Kang Brown of possession for the purposes of trafficking.[29]

The majority sitting on this case for the Alberta Court of Appeal concurred, finding that

> No home was involved, the police were in a purely public place…, the dog only yielded a crude piece of information…, no intimate details of private lives could possibly be revealed, the odours 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.[30]

Consequently, the majority of the Alberta Court of Appeal concluded that there was no search and therefore that 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

---

[28] Kang Brown also alleged that his *Charter* rights under section 9 ("[e]veryone has the right not to be arbitrarily detained or imprisoned") and section 10 ([e]veryone has the right on arrest or detention (a) to be informed promptly of the reasons therefor; (b) to retain and instruct counsel without delay and to be informed of that right; and (c) to have the validity of the detention determined by way of *habeas corpus* and to be released if the detention is not lawful") had been violated in the course of his interaction with the Operation Jetway officers. See *Charter*, *supra* footnote 7 at s.9 and s.10. The trial judge dismissed both of these claims, and the Court of Appeal concurred.

[29] *R. v. Kang Brown, supra* footnote 27.

[30] *Kang Brown*, *supra* footnote 5 at para. 52.

to above, part of the explanation may turn on the unique facts of each case and the application of the totality of the circumstances test set out in *Edwards*[31] 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. *Tessling,* By Analogy

Tessling did not involve snoop dogs or emanating odours. Instead, heat emanations from a house were detected and measured by a technology known as Forward Looking Infrared (FLIR). The FLIR device was mounted in an RCMP plane that flew over Tessling's house and was used to generate a "structure profile."[32] Such evidence was necessary to get a search warrant to enter Tessling's home, since the police were merely suspicious that there was a marijuana grow-op in the basement but lacked reasonable and probable grounds to believe that this was in fact the case.

According to the Supreme Court of Canada, FLIR technology does not currently indicate the nature or source of the heat, but only warmer and cooler areas of a building. While it "…cannot 'see' through the external surfaces of a building," it does create "…an image of the distribution of escaping heat at a level of detail not discernible by the naked eye."[33] In essence, it is a camera that takes pictures of heat rather than light. The RCMP took a FLIR 'picture' of Tessling's home. The resulting 'map' of the heat patterns, combined with information from police informants, was deemed sufficient to secure a warrant. On the basis of that warrant, the police were able to conduct a search of Tessling's house wherein they discovered large quantities of marijuana and various firearms. This evidence was admitted in court and Tessling was charged with possession for the purposes of trafficking and related drug and weapons offences.

---

31 *Supra* footnote 19.
32 *Tessling, supra* footnote 10 at para. 34.
33 *Ibid.* at para. 5.

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.[34] His claim was unsuccessful, the evidence was admitted and Tessling was convicted at trial. However, the Ontario Court of Appeal 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. In arriving at its decision, the Court of Appeal emphasized the territorial privacy interests at stake, highlighting the fact that FLIR technology "…reveals information about activities that are carried on inside the home"[35], which is "…an environment whose privacy has consistently and insistently been designated by the courts as worthy of the state's highest respect."[36]

Unlike other decisions – where the analysis focused narrowly and reductively 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."[37] 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 all charges.

On appeal to the Supreme Court of Canada, Binnie J., writing for a unanimous Court, 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

---

34 *R. v. Tessling* (5 December 2000), London, (Ont. Sup. Ct.).

35 *R.. v. Tessling* (2003), 63 O.R. (3d) 1, 168 O.A.C. 124 [*Tessling Appeal*] at para. 61.

36 *Ibid.* at para. 33.

37 *Ibid.* at para. 66.

expectation of privacy."[38] In rendering this conclusion, Binnie J. focused less on the territorial implications of this case, emphasizing instead the informational privacy interests at stake. Binnie J. characterized current FLIR imaging "…as an external search for information *about* the home which may or may not be capable of giving rise to an inference about what was actually going on inside…".[39] While Tessling was found to have a subjectively reasonable expectation of privacy in the heat emanating from his home, this expectation was held not to be objectively reasonable for two basic reasons: (i) FLIR is an "off-the-wall" rather than a "through-the-wall" technology;[40] and (ii) the information gathered by FLIR technology was, *on its own*, "meaningless."[41] Since there was

---

38 *Tessling, supra* footnote 10 at para. 63.

39 *Ibid.* at para. 27.

40 "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. In *Tessling*, *supra* note 10 at para. 5, Binnie J. characterized FLIR technology as "off-the-wall" technology because while it can detect relative heat distribution patterns emanating from a home, "the FLIR camera cannot "see" through the external surfaces of a building". The distinction between "off-the-wall" and "through-the-wall" technologies employed by both the Supreme Court and the Ontario Court of Appeal in *Tessling* is borrowed from American judicial parlance. In *Kyllo v. United States* (2001), 121 S. Ct. 2038, the American equivalent to *Tessling*, the United States Supreme Court was asked to consider whether the warrantless use of FLIR technology constituted an unlawful search in violation of the Fourth Amendment. The majority in *Kyllo* ultimately found that the use of FLIR technology in this context *did* constitute a search, and Scalia J. for the majority rejected the possibility of any fundamental difference between "off-the-wall" observations and "through-the-wall" surveillance, stating at para.19:

> …just as a thermal imager captures only heat emanating from a house, so also a powerful directional microphone picks up only sound emanating from a house – and a satellite capable of scanning from many miles away would pick up only visible light emanating from a house. We [previously] rejected such a mechanical interpretation of the Fourth Amendment…Reversing that approach would leave the homeowner at the mercy of advancing technology – including imaging technology that could discern all human activity in the home.

Like Scalia J., in Part 5, we speculate that this distinction does not have a particularly long shelf life.

41 For Binnie J. in *Tessling, supra* note 10 at para. 58, "[t]he evidence is that a FLIR image of heat emanations is, on its own… meaningless. That is the bottom line." Binnie J. was able to reach this conclusion based on his understanding that the utility of the FLIR information was only as great as the inferences that could be drawn from it; without those inferences, the FLIR information in isolation was of no use. This conclusion contradicts that made by Abella J. at the Court of Appeal in *Tessling Appeal, supra* footnote 35. While Abella J. found (at para. 66) the surface emanations on their own to be meaningless, she emphasized that "…to treat them as having no relationship to what is taking place inside the home, is to ignore the stated purpose of their

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.[42] 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.[43] If Mr. Tessling does not have a

---

being photographed, that is, to attempt to determine what is happening inside the home."

[42] Prior to the *Tessling* decision, there seemed little confusion about whether or not a dog sniff constituted a search that attracted section 8 scrutiny. See *e.g.* the Supreme Court decision in *R. v. Buhay, supra* footnote 18, which provides authority for the conclusion that there is a reasonable expectation of privacy in lockers in a bus station even where the station staff members have a key. *Buhay* was subsequently relied on in *R. v. Dinh, supra* footnote 18, at the Alberta Court of Appeal in its holding that a dog sniff search of a bus station locker without reasonable grounds was a serious violation of section 8 which properly results in the exclusion of evidence. *R. v. Donovan*, *supra* footnote 18, similarly found a dog sniff to qualify as a search worthy of section 8 scrutiny. Post-*Tessling*, Canadian courts have distinguished *Dinh* and *Donovan* on the basis that they were decided before *Tessling*. In his article, "Police Use of Sniffer Dogs Ought to Be Subject to *Charter* Standards: Dangers of *Tessling* Come to Roost" 31 C.R. (6th) 255, Don Stuart notes (at 258), "[t]here is a mountain of case law on the issue of whether a smell of marijuana constitutes reasonable grounds for a police search. Section 8 protection has been assumed. It would be odd were the courts to hold that all the police need to avoid the reasonable ground, warrant, reasonable manner and other requirements in drug searches is to bring along a dog!"

[43] Although our position is that this view is incorrect, the Supreme Court of Canada does appears to have set a precedent for this sort of analogical reasoning between different forms of emanations in *Tessling*, *supra* footnote 10, when the Court likened the heat measurement pattern acquired by the FLIR in to the electricity consumption pattern records obtained in *R. v. Plant*, [1993] 3 S.C.R. 281, 145 A.R. 104 [*Plant*]. (The Supreme Court's affirmation of *Plant* in *Tessling* is subject to the caveat at para. 64 that, contrary to *Plant*, the seriousness of the offence under investigation is not a factor relevant to the determination of privacy but is better reserved for consideration under section 24(2) of the *Charter*). In *Plant*, Sopinka J. found (at para. 293) that the

reasonable expectation of privacy in the heat emanating from his home, some may argue, A.M. and Mr. Kang Brown similarly have no expectation of privacy in the smells emanating from their backpack and shoulder bag, respectively. Indeed 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.[44]

---

accused's section 8 rights were not infringed when police obtained computerized records of his electricity use because, in part, electricity consumption patterns are not "personal and confidential" in nature. He went on to state (at para. 293) that section 8 of the *Charter* seeks to protect "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." Given the relationship between heat and electricity, "it seemed that the constitutional fate of one technique foretold the fate of the other." 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 230. We share Pomerance's concern about the extension from one instance to the other by way of this rather weak analogy.

[44] See *e.g. R. v. Davis, supra* footnote 17, where police approached a van without a warrant and, on the basis of a dog sniff, conducted a search of the vehicle resulting in Davis' arrest for possession of marijuana for the purpose of trafficking. Relying on *Tessling,* the British Columbia Provincial Court found that intimate details of Davis' lifestyle were not revealed through the dog sniff and concluded (at paras. 21-23) that the target "did not have a reasonable expectation of privacy in the area surrounding his vehicle. The dog sniff did not constitute a search"; *R. v. Gosse*, *supra* footnote 17, a case involving an Operation Jetway -related dog sniff, where the New Brunswick Queen's Bench relied on the fact that the dog sniff for drugs did not reveal any intimate or core biographical information and found (at para. 40) that "[t]he dog sniff does not constitute a 'search' within the purview of section 8 of the *Charter*." The Court also stated (at para. 28) that the use of police dogs and other investigative tools designed to detect illegal substances on public buses "is not beyond the realms of reasonable expectations of the traveling public"; *R. v. McLay*, *supra* footnote 17, the Provincial Court for New Brunswick drew a direct analogy between emanating drug odours and the heat emanations in *Tessling* and noted (at para. 38) that "the technology of the dog's nose" did not infringe on a reasonable expectation of privacy and therefore that there was no search. The accused had (at para. 38) "knowingly expose[d] [the odour] to the public," even though it was not actually detectable by human smell alone, just as a house's heat profile is not detectable. The technology of the dog's nose was not so complex and mysterious as to alarm the public, and so the accused had no reasonable expectation of privacy, and there was no section 8 violation;

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 extremely 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,[45] the judicial analogy between *Tessling* and the snoop dog cases substantially diminishes the scope of section 8 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.[46] The current approach to protecting

---

and *R. v. Gallant*, *supra* footnote 17, where the New Brunswick Queen's Bench found an Operation Jetway dog sniff did not infringe the accused's section 8 rights, stating, (at para. 36) "[i]f the Supreme Court of Canada concluded that a device that measure heat escaping from a private home does not affect personal dignity, integrity and autonomy, it is hard to find that dog sniff of escaping odours in a public place, does."

[45] 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).

[46] The Supreme Court has specified the kinds of privacy interests protected by section 8 as falling into three main categories: personal privacy, territorial privacy and informational privacy. Personal privacy refers broadly to the protection of bodily integrity. See *e.g. R. v. Golden,* 2001 SCC 83, [2001] 3 S.C.R. 679 at paras. 90-92 (holding that the state cannot conduct warrantless strip searches unless they are incident to a lawful arrest and performed in a reasonable manner); *R. v. Stillman,* [1997] 1 S.C.R. 607, 185 N.B.R. (2d) 1

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 in the first place because the "guarantee of security from *unreasonable* search and seizure only protects a *reasonable* expectation [of privacy]."[47] 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".[48] 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.[49]

The courts have recognized that establishing what is 'reasonable' when it comes to our expectations of privacy is increasingly easier said than done. In *Tessling*, for example, a unanimous Supreme Court acknowledged that, "[p]rivacy is a protean concept, and the difficult issue is where the

---

(involving unauthorized collection of bodily samples by police); and *R. v. Dyment*, [1988] 2 S.C.R. 417, 73 Nfld. & P.E.I.R. 13 at paras. 431-432. Territorial privacy protects a hierarchy of locations with the home being worthy of the greatest level of protection as the place where our most intimate and private activities are most likely to take place (see *e.g. R. v. Evans,* [1996] 1 S.C.R. 8, 131 D.L.R. (4th) 654 at para. 42; *R. v. Silveira,* [1995] 2 S.C.R. 297, 124 D.L.R. (4th) 193 at para. 140; and *R. v. Feeney,* [1997] 2 S.C.R. 12, 146 D.L.R. (4th) 609 at para. 43), and spaces including the perimeter around the home (see *e.g. R. v. Kokesch,* [1990] 3 S.C.R. 3, 51 B.C.L.R. (2d) 157), commercial spaces (see *e.g. Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research* [1990] 1 S.C.R. 425, 72 O.R. (2d) 215 at para. 517) and private cars (see *e.g. R. v. Mellenthin* [1992] 3 S.C.R. 615, 135 A.R. 1). Informational privacy relates to "how much information about ourselves and activities we are entitled to shield from the curious eyes of the State" *R. v. B. (S.A.),* 2003 SCC 60, [2003] 2 S.C.R. 678.

47 *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 (emphasis in original).

48 *R .v. Wise*, [1992] 1 S.C.R. 527, 11 C.R. (4th) 253 [*Hunter v. Southam Inc.*] at para. 533.

49 The Supreme Court has amassed a fairly extensive body of section 8 jurisprudence to date. Some of the principal cases include, *Hunter v. Southam*, *supra* footnote 47, *R. v. Dyment, supra* footnote 46, *R. v. Evans, supra* footnote 46, *Plant, supra* footnote 43, and *Edwards*, *supra* footnote 19, as well as many of the other cases considered herein.

'reasonableness' line should be drawn.[50] As we have seen, all of this is further complicated by the totality of the circumstances test used to determine the existence of a reasonable expectation of privacy.[51] That test focuses on the existence of 1) a subjective expectation of privacy; and 2) the objective reasonableness of that expectation.[52] While it is generally up to the accused to demonstrate the former,[53] the objective reasonableness of an expectation of privacy includes a consideration of a number of contextual factors,[54] 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 both the subjective and objective aspects of this 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, these days, be understood in the context of our *risk society*[55] and the escalating trend towards high tech surveillance and greater

---

50 *Tessling*, *supra* footnote 10 at para 25.

51 This, according to some courts, is to be understood as a "no catalogues" approach. For example, Côté J. in the Alberta Court of Appeal decision in *Kang Brown, supra* footnote 5 at para. 38, described the totality of circumstances approach as follows: "[t]he Supreme Court of Canada now forbids the use of catalogues of banned and permissible techniques."

52 First described in *Edwards*, *supra* footnote 19 at para. 45 by Cory J.

53 *Edwards*, *supra* footnote 19 at para. 45. The burden on the accused to demonstrate a subjective expectation of privacy is subject to the Supreme Court's assertion in *Tessling, supra* footnote 10 at para. 38, that "…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."

54 The Court has noted that this aspect of the section 8 analysis is particularly problematic, going so far in *Tessling, supra* footnote 10 at para. 43, as to characterize the "objectively reasonable" analysis as "a major battleground in many of the s.8 cases…"

55 By this we mean a society that is organized primarily in response to risks. As Anthony Giddens once put it, "[i]t is a society increasingly preoccupied with the future (and also with safety), which generates the notion of risk." 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).

police presence as an appropriate response.[56] 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.[57] Our courts have recognized this.[58] So have our

---

[56] Operation Jetway, *supra* footnote 26, 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.

[57] Invasive technologies currently being tested include x-rays that bounce low intensity waves off the targeted person's skin to render weapons visible. These simultaneously make all clothing transparent, thus fully revealing intimate bodily parts. See 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>. Other technologies under development to test bodily emanations include the use of honeybees which "sniff" travelers exiting planes to locate drugs and explosives. See 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>. Variants on the use of security gates also are under trial. These closely resemble metal detectors, but circulate currents of air that bounce off human bodies. These currents are then reabsorbed by the machine and will identify traces of explosives on clothing, skin, and hair. The developers of these "sniffer" gates claim that they will be able to penetrate the target's shoes in order to detect illegal materials. See Ira Sager & Catherine Yang, "Travelers, Prepare to be Smelled" *Business Week* 16 (24 May 2004). Biometrics are also becoming increasingly invasive of bodily privacy. Dissatisfied with the physiological changes of aging that change the body's surface over time - inhibiting reliable identification - biometric technology manufacturers are developing technologies that will record information located beneath the skin's surface. Biometric scanners that identify the vascular network of blood vessels beneath the surface of the face are currently in development. See *e.g.* Pradeep Buddharaju et *al*., "Physiology-Based Face Recognition in the Thermal Infrared Spectrum" (2007) 29 IEEE Transactions on Pattern Analysis & Machine Intelligence 613. Vascular recognition of the veins in the hands is already in use. See W.D. Jones, "Blood Test" (2006) 43 IEEE Spectrum 16. Finally, in the latest bid to develop a reliable polygraph that could function as a technologized "thought police," research is being conducted on sensors that will scan crowds to determine whether anyone is planning to commit - or is even thinking of committing - an illegal act. These scanners are designed to detect malicious thoughts by measuring excessive blood-flow to the face. See Bijal P. Trivedi, "Heat-Detecting Sensor May be Able to Detect Lying" *National Geographic News* (22 January 2002), online: NationalGeographic.com <http://news.nationalgeographic.com/news/2002/01/0102_020102TVsensor.html>.

[58] The courts acknowledged it more than a decade before September 11, 2001. As La Forest J. famously stated 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:

legislators. The *Charter* was designed in large measure to safeguard individual interests from unreasonable intrusion by the state.

In a time where Operation Jetway and powerful forms of electronic surveillance programs[59] are quickly becoming the norm, courts must be particularly attuned to the effects of increased law enforcement practices on individual liberties, including our reasonable expectations of privacy. While balancing privacy interests with competing demands[60] has long been a part of any section 8 analysis,[61] in the midst of the war on drugs and the war on terror, we have seen this balance shift in favour of law enforcement at the cost of privacy interests. 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".[62] But the 'reasonableness' line is now

---

> …if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning.

See also David H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States* (North Carolina: The University of North Carolina Press, 1992).

59 See *supra* footnote 57. In the same world where dogs are being trained to sniff-out drugs and DVDs, technologists are perfecting new means of remote sniffing from simple devices that detect, measure and analyze electricity consumption to gas chromatography and other advanced forms of *machine olfaction* that are used to detect, measure and analyze odours in the air that even dogs cannot. See *e.g.* Wikipedia Contributors, "Gas-Liquid Chromatography" *Wikipedia, The Free Encyclopedia*, online: Wikipedia <http://en.wikipedia.org/wiki/Gas_Chromatography>.

60 The competing demands most often discussed by courts include "safety, security and the suppression of crime." See *Tessling*, *supra* note 10 at para. 17.

61 See *e.g. Hunter v. Southam Inc.*, *supra* footnote 47 at paras. 159-160, where Dickson J. (as he then was) states: "…an assessment must be made as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement."

62 Renee M. Pomerance, *supra* footnote 43 at 231. This concern was expressed by Abella J. in the *Tessling Appeal* decision, *supra* footnote 35 at para. 79,

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 Canadian courts' current 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 rather than normative) conception of reasonable expectations.

(i) The Narrow Conception of Informational Privacy

The concept of informational privacy was brought into the academic mainstream by Alan Westin, who famously characterized this notion 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.[63] Westin's conception of privacy has been adopted by the Supreme

Court of Canada on several occasions.[64] It was also the basis for an international standard for data protection known as *fair information practice principles.*[65] While data protection is indeed an important aspect of privacy, it remains

---

where she predicted that "[t]he nature of the intrusiveness [of FLIR technology] is subtle but almost Orwellian in its theoretical capacity."

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

64 See *e.g. Tessling, supra* footnote 10 at para. 23; *Edwards, supra* footnote 19 at para. 61; and *R. v. Dyment, supra* footnote 46 at paras. 17, 20.

65 These principles were set out by the Organization for Economic Co-operation and Development in its document, *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>. They were further developed by the Canadian Standards Association in its *Model Code for the Protection of Personal Information* (CSA Publications, 1996), online: Canadian Standards Association <www.csa.ca/standards/privacy/code/Default.asp?language=English>, and adopted in Canadian law in the *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5, Schedule 1 [*PIPEDA*], online: Office of the Privacy Commissioner of Canada <www.privcom.gc.ca/legislation/02_06_01_01_e.asp>.

unclear how effective it is in protecting privacy writ large.[66] It is also unclear whether informational privacy, so defined, is foundational or instrumental, whether it is a human right or merely an economic right.[67]

Informational privacy concerns have various dimensions. One essential dimension is Westin's concern about ensuring informational self-determination. The usual metric for establishing informational self-determination and its appropriate limits within data protection regimes is whether the information is about an 'identifiable individual'.[68] If the information does not identify an individual, there is generally

---

[66] The Government of Canada is currently reviewing its *PIPEDA, supra* footnote 65. Many experts have appeared before the Standing Committee on Access to Information, Privacy and Ethics raising legitimate concerns about the efficacy of the current regime in protecting the privacy of Canadians. See House of Commons Standing Committee on Access to Information, Privacy and Ethics, online: <http://cmte.parl.gc.ca/cmte/CommitteeHome.aspx?Lang=1&PARLSES=391&JNT=0&SELID=e17_&COM=10473>. For summaries of the Committee's hearings to date, see also The Canadian Internet Policy and Public Interest Clinic, online: <http://www.cippic.ca/en/>; and Michael Geist's Blog, online: <http://www.michaelgeist.ca/content/blogsection/0/126/>. For an excellent article on the value of informational privacy protection see Marc Rotenberg, "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)" (2001) Stan. Tech. L.Rev. 1.

[67] See *e.g.* Ann Cavoukian, "Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation" (1999) online: Office of the Information and Privacy Commission for Ontario <http://www.ipc.on.ca/images/Resources/up-1pr_right.pdf>. The human rights approach, construing privacy as a moral and social "good", has been the primary approach to privacy advocacy and is bolstered by a number of international human rights covenants including the *Universal Declaration of Human Rights*, G.A. Res. 217A (III), UN GAOR, 3d Sess., Supp. No. 13, UN Doc. A/810 (1948) 71, the *European Convention for the Protection of Human Rights and Fundamental Freedoms,* 4 November 1950, 213 U.N.T.S. 221 at 223, Eur. T.S. 5, and the *International Covenant on Civil and Political Rights,* 19 December 1966, 999 U.N.T.S. 171, arts. 9-14, Can. T.S. 1976 No. 47, 6 I.L.M. 368 (entered into force 23 March 1976, accession by Canada 19 May 1976). For a comprehensive overview of issues related to privacy and human rights around the world, see EPIC & Privacy International, *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* (Washington,D.C.: EPIC, 2005). The economic, or market-based approach to privacy posits individual choice to be the primary factor in privacy decision-making. See *e.g.* Lawrence Hunter & James Rule, "Toward Property Rights in Personal Information" in Colin J. Bennett & Rebecca Grant, eds., *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999); Kenneth C. Laudon, "Markets and Privacy" (1996) 39 Communications of the ACM 92;

[68] For example, *PIPEDA, supra* footnote 65 at s.2, defines personal information as "information about an identifiable individual (…)." The information must therefore be sufficient to identify a specific individual.

no need to justify its collection, use or disclosure.[69] The courts, however, have adopted a rather different threshold in the context of the reasonable expectation of privacy. In the language of the Supreme Court, developed by Sopinka J. in *Plant*, whether one holds a reasonable expectation of privacy in information depends 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".[70] 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 *Plant*

> [t]he computer records investigated … while revealing the pattern of electricity consumption in the residence cannot reasonably be said to reveal intimate details of the appellant's life since electricity consumption reveals very little about the personal lifestyle or private decisions of the occupant of the residence.[71]

Likewise, in *Tessling* it was held that "a FLIR image of heat emanations is, *on its own … meaningless*."[72] 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.[73]

---

69 This approach to protecting informational privacy is evident in *PIPEDA, supra* footnote 65, as well as Alberta's *Personal Information Protection Act,* S.A. 2003, c.P-6.5, British Columbia's *Personal Information Protection Act*, S.B.C. 2003, c.63 and *Personal Health Information Protection Act*, S.O. 2004, c.4 in Ontario.

70 *Plant, supra* footnote 43 at para. 27.

71 *Ibid.*

72 *Tessling, supra* footnote 10 at para. 58 (emphasis added).

73 *Kang Brown, supra* footnote 5 at para. 52 (emphasis added).

Of course, there is some truth to some of this. Indeed, it 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.[74] Namely, that in exactly the same way that wisdom is built from knowledge, knowledge from information, and information from data[75] — *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*[76] 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-established techniques in the field of information technology such as data-mining[77] 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,[78] in the language of the courts, "to reveal intimate details of the

---

[74] See *e.g.* the dissent of McLachlin C.J.C. in *Plant, supra* footnote 43, the dissent of Abella J.A. (as she then was) at the Ontario Court of Appeal in *Tessling Appeal, supra* footnote 35 and the dissent of Paperny J.A. in *Kang Brown*, *supra* footnote 5, all of which are discussed below in Part 4.

[75] 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>.

[76] A mashup is the combination of "content from a number of different sources to produce something new and creative." The term 'mashup' is derived from the "hip-hop music practice of mixing two or more songs together to form something new…" 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.

[77] Data mining may be defined as "the intelligent search for new knowledge in existing masses of data." Joseph S. Fulda, "Data Mining and Privacy" (2000) 11 Alb. L.J. Sci. & Tech. 105 at 106. See also Usama Fayyad, Heikki Mannila & Raghu Ramakrishnan, eds., *Data Mining and Knowledge Discovery* (Norwell, MA: Kluwer Academic Publishers, 2002); Lee Tien, "Privacy, Technology and Data Mining" (2004) 30 Ohio N.U.L. Rev. 389.

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

lifestyle and personal choices of the individual." In fact, the entire premise behind practically every data protection regime in the world (and the relatively uniform fair information practice principles that support them) is the concern that data and information can easily be re-purposed in ways that require fresh consent before information collected for some primary purpose is permitted to be combined with other information in order to achieve a secondary purpose.[79]

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*[80] 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.[81]

(ii) The Pickwickian Relationship Between Searches and Expectations of Privacy

As we have seen, the courts have deemed that there is no search where there is no reasonable expectation of privacy. In the context of the courts' narrow conception of informational privacy, this leads to the rather pickwickian logic described three paragraphs below. In what world, other than *Wonderland*,[82] would facts such as these *not be understood* as searches?

---

79 See *e.g.* Marc Rotenberg, *supra* footnote 66.

80 Roger Clarke, *supra* footnote 3, 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."

81 See Daniel J. Solove, *supra* footnote 3.

82 One is here reminded of Humpty Dumpty's rather scornful reply to Alice in *Through the Looking Glass* in which he makes the rather bold claim that, "[w]hen I use a word, it means just what I choose it to mean, neither more nor less." To which Alice replies, "[t]he question is, whether you can make words mean so many different things." Humpty Dumpty then replies, "[t]he question is: which is to be master - that's all." Lewis Carroll, "Through the Looking Glass" in Martin Gardiner, ed., *The Annotated Alice* (London, Penguin Books, 1970) at 269. The American jurist, Lon Fuller, used to worry about the introduction of such sweeping changes in linguistic usage by arbitrary fiat. Fuller was concerned that the end result of any such attempt "would only result in encumbering the law with a grotesque assemblage of technical concepts

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 elements and examples of a 'police search' in most situations. The opposite is true in the case of privacy; the constitutive elements in the veritable plethora of tangible and intangible interests that together form our varying conceptions of privacy are exceedingly difficult to define.[83] Yet Canadian courts tend to embrace and employ the idea that we cannot identify the former (search) until we know if an individual can reasonably expect the latter (privacy), making a judicial determination about the existence of a search wholly contingent upon the murky concept of privacy. This seems neither logical nor practical.

Moreover, the seemingly fact-oblivious[84] 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.[85]

---

lacking the slightest utility." Lon L. Fuller, *Legal Fictions* (Chicago: Stanford University Press, 1967) at 21.

83 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. Recall also that in *Tessling, supra* footnote 10 at para. 25 Binnie J. noted this fact, describing privacy as "a protean concept." The divides between majority and minority decisions of the courts regarding what 'qualifies' as private lend support to this proposition. See *e.g.,* the polarized viewpoints in *Plant, supra* footnote 43, of Sopinka J. for the majority, concluding that electricity consumption patterns reveal little about one's personal lifestyle and the dissent by McLachlin J. (as she then was), holding that this same information has the potential to reveal much about the internal workings of a home.

84 Admittedly, 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.

85 In *Tessling, supra* note 10 at para. 27, Binnie J. emphasized the informational aspect of privacy in characterizing the FLIR overflight as "an external investigation for *information* about the home which may or may not be capable of giving rise to an inference about what was actually going on inside…" As a result of this very narrow focus on the nature of the *information* collected, Binnie J. was able to conclude that the heat emanation patterns are, on their own, "meaningless." This was Binnie's "bottom line" (at para. 58). This

For these reasons we suggest, once again, that courts must take care not to engage in an excessively reductionist approach to informational privacy. As soon as we begin characterizing police activities outside of their social context – once a warrantless night-overflight beaming police infrared devices at houses is rationalized as nothing more than the *meaningless* capture of heat emanations from a building, once three 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 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.[86]

(iii) The Non-Normative Conception of 'Reasonable Expectations'

In one sense, it does not really matter whether the police's use of snoop dogs in cases like *Kang Brown* are deemed to be searches. Regardless of whether a given court finds that an individual has a reasonable expectation of privacy in odours emanating from luggage or whether police snoop dog investigations are deemed 'searches' worthy of section 8 protection, Operation Jetway evidence is almost always admitted in courts of law.[87] To exclude the evidence, most

---

interpretation has been applied to dog sniff cases, including *R. v. McLay, supra* footnote 17 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.

86 This point was not lost on Abella J. in her decision in *Tessling Appeal*, *supra* footnote 35, where she contextualized FLIR imaging within the broader purpose for which the information was collected, stating at para. 61, "the sole reason that police photograph heat emanations is to attempt to determine what is happening inside the house." She thus treated the FLIR overflight as equivalent to a search of the home, and emphasized at para. 33 the accused's reasonable expectation of privacy in activities carried on within his residence.

87 It is notable that the evidence in *A.M.*, *supra* footnote 9, where the dog sniff took place at a high school, was excluded by the Ontario Court of Appeal, while in *Kang Brown*, *supra* footnote 5, where the evidence was obtained as part of Operation Jetway, it was not excluded. The majority of recent court cases dealing with police snoop dogs stem from Operation Jetway searches, where the evidence is almost always admitted.

courts have held,[88] would bring the administration of justice into disrepute.[89] By admitting the evidence in spite of the fact that it was obtained through an unreasonable breach of privacy, and by failing to provide any alternative remedies in the case of such privacy breaches, the courts relinquish the strongest deterrent available to prevent police from orchestrating investigations designed to interfere with privacy. This is an unfortunate outcome since there is a considerable need for such deterrents. Without 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*,[90] 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, stating:

> [i]n conclusion, I am of the opinion the accused did not have a subjective expectation of privacy that could reasonably be supported. The accused chose to travel by public transport which would provide no control or protection from others entering his immediate space. The

---

88 See *e.g. R. v. Mercer, supra* footnote 17, *R. v. Kang Brown*, *supra* footnote 27, *R. v. McLay*, *supra* footnote 17 and *R. v. Gosse, supra* footnote 17.

89 This conclusion is often based on a number of considerations under the *Collins* test (see *R. v. Collins*, [1987] 1 S.C.R. 265 (*sub nom. Collins v. R.*) 13 B.C.L.R. (2d) 1) including the police's good faith actions and the conclusion that admitting the evidence would not affect that fairness of the trial. See *e.g.*, the cases cited *ibid.*

90 *McCarthy*, *supra* footnote 13.

> 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*.[91]

This line of reasoning completely 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."[92] 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, which the *Tessling* Court expressly rejects, 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.[93] 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.

The reasoning illustrated by *McCarthy* and adopted broadly across the snoop dog jurisprudence is reminiscent of Herbert Hart's famous distinction between internal and external aspects of a rule, which he sets out in his seminal jurisprudential text, *The Concept of Law*.[94] Briefly put, Hart showed that it is possible to be concerned with rules either as a mere observer who does not himself accept them, or as one who uses them as reasons for his conduct as a member of a

---

91 *Ibid.* at para. 36.

92 *Tessling, supra* footnote 10 at para. 42. Interestingly, Binnie J. presciently anticipated the possibility of this fallacious mode of reasoning using the *Watergate* inquiry as his example.

93 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.

94 H.L.A. Hart, *The Concept of Law* (New York: Oxford University Press, 1961).

group that does accept them. The former he called the "external" point of view and the latter the "internal" viewpoint. Hart's distinction shows that the external observer, who lives a detached, scientific existence, is unable to reproduce the way in which the rules function in the lives of most lawyers and judges who do adopt the internal point of view. In particular, judges:

> use [rules], in one situation or another, as guides to the conduct of social life, as a basis for claims, demands, admissions, criticism, or punishment, viz. in all the familiar transactions of life according to rules. For them it is not merely a basis for prediction that a hostile reaction will follow but a *reason* for hostility.[95]

Here, Hart was responding to what Oliver Wendell Holmes Jr. once characterized as the "bad man" theory of law. The 'bad man' is someone who has not accepted and internalized the law as a *reason* for behaving a certain way but sees legal rules as *mere predictions about what the courts will do in fact*. The bad man "…cares only for the material consequences which such knowledge enables him to predict."[96] Similarly, Hart's external point of view leads us to expect something to happen based solely on what we have observed about reactions to certain patterns of conduct. It is *amoral* reasoning, based solely on predictions and without regard to social norms.

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. As such, the courts' examination of the reasonable expectation of privacy is essentially reduced to a strange sort of factual inquiry. 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

---

95 *Ibid.* at 88.

96 Oliver Wendell Holmes Jr., "The Path of the Law" (1897) 10 Harv.L.Rev. 457. Holmes contrasts the 'bad man' with the 'good man' "…who finds his reasons for conduct, whether inside the law or outside of it, in the vaguer sanctions of conscience."

external prediction, all one needs to do to alter the reasonable expectation of privacy standard is to engineer a change in peoples' expectations. (This can be achieved through the adoption of new technologies.) The same holds true in the other direction. In order to change people's expectations, one need only change the standard.

It is a circle that rolls round upon itself; a circularity that is particularly disconcerting in light of concurrent surveillance programs in the private sector and rapidly developing surveillance technologies.

This 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.[97] 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,[98] including powerful though physically unobtrusive forms of surveillance that lie just around the corner.[99] These predictions should give courts pause, not only

---

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

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

99 Current technologies include digital recording ammeters (DRAs), which are capable of measuring the flow of electricity to a residence and providing a graph of the cycles of electrical consumption. DRA technology is non-invasive and gathers data on distribution loads and power quality. DRA meters are connected to the electrical supply line of a residence of interest on public property, making it valuable to law enforcement because it allows for controlled surveillance of a property without the need for law enforcement officers to physically enter the territory of the home. For instance, marijuana growing operations generally utilize a great deal of electricity in the specific patterns necessary to stimulate photosynthesis in the plants – light for a certain number of "daytime" hours, and darkness to simulate "night." If DRA graphs reveal consumption cycles approximating 12 hours of high consumption followed by 12 hours of low consumption in a 24-hours period, police can interpret this as consistent with the growth demands of a marijuana crop. This technology is particular useful to law enforcement if an individual has bypassed the electricity meter in order to steal electricity and avoid consumption patterns being shown on billing information. The DRA calculates inflow of electricity prior to the bypass. See *e.g. R. v. Le*, (2005) 30 C.R. (6th) 124; *R. v. Cheung*, (2005) 199 C.C.C. (3d) 260.

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.

Interestingly, emerging technologies to monitor electrical activity in and around the human body are also under development, including a new application of electroencephalograms (EEG) technology, which measures electricity emanating from the human skull in a non-invasive, highly precise and cost effective manner. EEG fingerprinting allows researchers to use EEGs to determine whether or not an individual is in possession of knowledge related to a crime scene. A subject is shown a series of pictures or words and when the brain recognizes crime related information, it emits a specific EEG response. While conventional polygraph technology measures physiological markers associated with lying, like blood pressure, EEG brain fingerprinting measures the brain waves that are spontaneously emitted when the individual recognizes information that is already stored in the brain, making the latter technology somewhat more reliable. (Though recent work indicates that EEG fingerprinting can be defeated by simple countermeasures like physical movement during testing or visualizing emotionally charged scenes.) See *Harrington v. Iowa* (659 N.W. 2d 509 2003), where EEG evidence was accepted by the Court and contributed to the exoneration of a wrongly convicted individual. See also J.P. Rosenfeld *et. al*., "Simple, effective countermeasures to P300-based tests of detection of concealed information" (2004) 41 Psychophysiology 205.) On EEG fingerprinting see *e.g.* L.A. Farwell & S.S. Smith, "Using brain MERMER testing to detect knowledge despite efforts to conceal" (2001) 46 J. Forensic Sci. 135; 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 measures the surplus of oxygenated blood that is recruited to specific, active regions of the brain. Like EEG fingerprinting, fMRI technology is being used by law enforcement for truth verification and lie detection purposes. Studies have shown that the neural baseline of an fMRI reading corresponds to telling the truth; when someone is being deceptive or inhibiting the truth, more neural circuits are activated. fMRI technology reveals the relevant brain regions involved in deception. While this technology is still in the nascent state of its development, commercial usages are already available. See *e.g.* Kozel *et. al*. "A pilot study of functional magnetic resonance imaging brain correlates of deception in healthy young men" (2004) 16 J. Neuropsychiatry Clin. Neurosci. 295; Langleben et. al. "Telling truth from lie in individual subjects with fast event-related fMRI" (2005) 26 Hum. Brain Mapp. 262.

See also Ian Kerr, "Tessling on my Brain: Reasonable Expectation of Privacy, Technology and the Future" (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/Kerr_NJI.mp3> (podcast) and <http://www.idtrail.org/files/tessling_on_my_brain_ian_final_nji.pdf> (presentation slides).

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, there is 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.[100] We conclude by considering this more compelling reading.

4. A More Compelling Reading of *Tessling*

In the preceding Parts of this article, we have tried to demonstrate why the majority of snoop dog cases in Canada were wrong in reducing their decisions to a simplistic equation between heat and odour emanations, and thereby wrong in applying the outcome in *Tessling* by way of simple analogy. We have also tried to highlight the likely dangers in a narrow use of this analogy and its ultimate effects on our reasonable expectations of privacy in light of vast amounts of knowable information emanation.

All of this having been said, perhaps the danger zones that we have articulated are exaggerated. Perhaps the opposing conclusions of the Ontario Court of Appeal in *A.M.* and the Alberta Court of Appeal in *Kang Brown* can in fact be resolved without reference to the *Tessling* analogy applied in the snoop dog cases discussed above. In other words, maybe there is a better reading of *Tessling* which does not "eradicate all privacy interests in 'emissions' that occur from private to public."[101]

Since the Supreme Court released its decision in 2004, *Tessling* has been interpreted by several courts as a precedent of general application.[102] Might a more fitting approach to

---

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

101 *Kang Brown*, *supra* footnote 5 at para. 106, Paperny J., dissenting.

102 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

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? While this is a less popular interpretation of *Tessling* (in terms of the total number of judges that have weighed in on the matter), it is the one that we believe is most plausible. If our interpretation is correct, all that would be required to resolve the existing tensions in the two dozen conflicting cases on snoop dogs and digital recording ammeters is a clarification from the Supreme Court of Canada along these lines.

Despite the plethora of decisions to the contrary, there is authoritative support for the view that the outcome in *Tessling* – its determination 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"[103] – is inapplicable as a general analogy for other information emanation cases. After all, as Binnie J. explicitly stated in *Tessling* "given the bewildering array of different techniques available to police (either existing or under development), the...approach of a judicial "catalogue" of what is or is not permitted by s.8 is scarcely feasible.[104]

Further, as one extremely knowledgeable and well respected commentator put it, *Tessling* is "itself fact specific and does not readily generalize beyond the specific issue before the Court."[105] A number of scholars and practitioners have expressed similar concerns about the application of *Tessling* to other police practices.[106] Courts have recently begun to recognize this as well, with significant traction in the *A.M.* decision at the Ontario Court of Appeal alongside a strong dissent by Paperny J. in *Kang Brown* at the Alberta Court of Appeal.

---

digital recording ammeters (DRA) cases: See, *supra* footnote 100 and see *e.g*. *R. v. Rayment*, 2006 ABQB 132; *R. v. Haskell,* 2004 ABQB 474; (2004) 33 Alta. L. R. (4th) 200.

103 *Tessling, supra* footnote 10 at para 63.

104 *Ibid.* at para. 19.

105 Renee M. Pomerance, *supra* footnote 43 at 229-30.

106 See *e.g.* Don Stuart, *supra* footnote 42; 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.

The reasoning in *A.M.* is particularly noteworthy in light of our discussion above in Part 3; it stands alone as the only case on point that commences its section 8 analysis with the factual circumstances surrounding the police investigation. Rather than attempting to determine whether *A.M.* had a reasonable expectation of privacy in the smells emanating from his backpack, Armstrong J. took judicial notice that two of the officers involved in the visit to *A.M.*'s school testified that they were engaged in a search. He also cited the submission of an intervener, the *Canadian Civil Liberties Association,*[107] and concluded in four brief paragraphs that he was satisfied that the dog sniff of the backpack constituted a search for section 8 purposes. This conclusion was arrived at *without invoking the reductionist approach, which seeks to determine in a generalized way whether there exists a reasonable expectation of privacy in odour emanations.* Instead, *A.M.*'s expectations of privacy were measured in the context of the Court's analysis of the reasonableness of the police search of the school including, of course, the use of the snoop dog. This method of analysis allowed the Ontario Court of Appeal to avoid altogether the danger zones associated with the reductionist 'heat-equals-odours' analogy.

As mentioned in the description of *A.M.* above in Part 2, Armstrong J. explicitly concluded that he was not "persuaded that the judgment of the Supreme Court of Canada in *Tessling* is supportive of the…position that a dog sniff is not a search."[108] He noted a number of critical differences between the facts of *Tessling* and those characteristic of situations in which dog sniffs take place, stating, "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 an entire student body in a random police search."[109] Consequently, the unanimous Ontario Court of Appeal in *A.M.* adopted a

---

[107] The quoted submission read: "[t]he dog is a necessary, direct, and integral part of the police officers' search of the classrooms, gymnasium and backpacks. The dog is, in essence, a physical extension of its handler and is directly and immediately connected to the consequent physical search of the backpack."

[108] *A.M., supra* footnote 9 at para. 47.

[109] *Ibid.*

very different reading of *Tessling;* one that transcends the excessively simplistic 'heat-equals-odours' analogy.

Paperny J., in her Alberta Court of Appeal dissent in *Kang Brown*, takes the A.M. reading of *Tessling* a step further. Recall that the majority in *Kang Brown* had affirmed the trial judge, who interpreted *Tessling* as saying that there is no reasonable expectation in odour emanations because, "emissions from a private place into the public domain may be detected by police using their own sense or technological enhancement".[110] Paperny J. disagreed entirely, stating that *Tessling* does not in fact support this conclusion. In making this claim, she emphasized that the reasoning of both the trial judge and the majority of the Court of Appeal in *Kang Brown* "rests on the overly broad and, in my view, incorrect interpretation of *Tessling* that all emissions into the public domain do not engage a privacy interest."[111]

According to Paperny J.: "[a] careful reading of *Tessling*…does not support an interpretation that there is no privacy interest in an "emission" emanating from private to public…Moreover, *Tessling* does not hold that a dog sniff is not a search.[112]

Perhaps the most important aspect of this dissent is its acknowledgment of the impact of the majority's interpretation of *Tessling* on the scope of the right to be secure against unreasonable search and seizure. According to Paperny J., the majority's reading of *Tessling,* which precludes the possibility of reasonable expectations of privacy in these sorts of information emanations,

> renders a vast range of common human activities subject to police surveillance without prior judicial authorization…In my view *Tessling* was not intending to eviscerate s.8 by granting police a license to intercept information in this manner.[113]
>
> . . . .
>
> I disagree with the majority's position that the Supreme Court in *Tessling* stated that devices which detect something emanating from a private place is not the equivalent of a search inside that place.

---

110 *Kang Brown*, *supra* footnote 5 at para. 99.

111 *Ibid.* at para. 108

112 *Ibid.* at para. 100. She also notes the concurrence of the Ontario Court of Appeal with these propositions.

113 *Ibid.* at para. 106.

> Rather, the Supreme Court's statements in this regard are consistently confined to the factual situation and the type of technology before it.[114]

Did the *Tessling* Court truly intend to grant police a license to intercept *any* information that emanates from a private place into the public domain?

It is hard to imagine so given that the Court was explicit in its distinction between emanation and abandonment.[115] According to the Court, people do not surrender their subjective expectations of privacy just because information about them escapes their control. Binnie J. was extremely careful to distinguish run-away emanations (which are not easily within our control) from other kinds of information surrendered (that are within our control). Only the latter is subject to the abandonment theory.[116] Rather, the question that is the "major battleground in many of the s.8 cases"[117] is whether an expectation of privacy in the run-away information that is made knowable by modern investigative techniques is *objectively* reasonable. According to *Tessling,* this requires a contextual analysis which, as we have seen, does not lend itself well to generalization. As we also saw, the key determinant in the *Tessling* facts was the finding that "FLIR's usefulness depends on what other information the police have." [118] The same cannot be said of information obtained from a snoop dog. Once a dog has correctly identified the kind of emanating odour she was trained to detect, no other information is needed. The investigation is a done deal. The same is and will be true for a range of emerging machine-based information emanation surveillance technologies.[119]

As we have seen, many courts across Canada have interpreted *Tessling* to apply generally to other kinds of

---

114 *Ibid.* at para. 134.

115 Binnie J. distinguishes heat that escapes from a building from a very different situation in which an accused was said to "abandon" his privacy interest in the garbage he put out on the street for collection, as was the case in *R. v. Kennedy* (1996), 3 C.R. (5th) 170, (*sub nom. R. v. Joyce*) 95 O.A.C. 321 (C.A.), at paras. 4-5.

116 *Tessling, supra* footnote 10 at para 41.

117 *Ibid.* at para 43.

118 *Ibid.* at para 53. Although, as we suggest in our conclusion below, this has little to do with whether the information is "meaningless."

119 See *supra* footnotes 57 and 99 and accompanying text.

emanations – such as odour – by way of the following simple analogy:

> external patterns of [X] on the external surfaces of [Y] is not information in which the respondent had a reasonable expectation of privacy.

However, as we have argued, a much more compelling reading is that the *Tessling* Court never intended any such generic *ratio*.

5. Conclusion

It remains a convention in academic prose to finish each article with a neat and tidy conclusion, a summation expositing a position reached after much thoughtful consideration. We often do this as though it were a singular event the occurrence of which brings the matter to an end. In this article, we have examined an increasingly problematic judicial approach to the reasonable expectation of privacy in odour emanations, tried to point out its potential dangers and offered what we believe is a superior understanding of the issue.

This ending, however, is really just a beginning. It is a realization and an appreciation of that which lurks around the corner. 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,[120] we suggest that the resolution of the snoop dog cases will not end 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."[121]

---

120 See Ray Kurzweil, *supra* footnote 98.

121 *Plant*, *supra* footnote 43 at para. 48.

If we are to maintain our "dignity, integrity and autonomy"[122] 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 confront the social implications of informational privacy much more deeply than they have, interrogating its meaning in an empirical universe of information emanation.

In this regard, it is difficult to imagine that the debate about "drawing the reasonableness line"[123] has finally been resolved. The escalating challenge that informational privacy is sure to present will require Canadian courts to realize that the *Tessling* decision was *never meant* to end this inquiry. *Tessling* tells us that difficult decisions lie ahead about: (i) when it is appropriate to focus specifically on the 'nature and quality' of the information that a given technology can currently deliver,[124] and (ii) when it is appropriate to look more broadly at its 'theoretical capacity'.[125] As should by now be evident from our analysis, it is our contention that Binnie J. preferred the former to the latter *for the specific facts that arose in Tessling*, but left the door wide open for broader approaches in light of the emergence of more powerful and telling surveillance technologies.[126]

It is also difficult to imagine that Binnie J.'s *"bottom line"* in *Tessling* (that a FLIR image of heat emanations is, on its own … "meaningless" [127]) was ever meant as a generalization that would be used to characterize the 'nature and quality' of all possible forms of emanation information that have been reduced to data points. In fact, as new and emerging information technologies continue to come before the courts, we predict that the current reductionist inclination which asks

---

122 *Ibid.* at para. 26.

123 *Tessling, supra* footnote 10 at para. 25.

124 *Ibid.* at para. 28-29.

125 *Tessling Appeal, supra* footnote 35 at para. 79.

126 As he stated in *Tessling, supra* footnote 10 at para. 29, "[i]f, as expected, the capability of FLIR and other technologies will improve and the nature and quality of the information hereafter changes, it will be a different case, and the courts will have to deal with its privacy implications at that time in light of the facts as they then exist."

127 *Ibid.* at para. 58.

whether the intercepted data is, *on its own*, meaningless will and ought to give way to the very opposite approach, namely: whether the bundle of information that is made available by means of the search, *once assembled*, ought to attract a reasonable expectation of privacy.

This latter approach recognizes the jigsaw nature of the data/information/knowledge/wisdom chain[128] 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. In our information age, perhaps the notion of a hyperlink is a more appropriate metaphor. While, on its own, it is meaningless html code, a hyperlink is both a point of reference and a navigational element that *automatically* brings the desired information to the user when the navigation element is engaged.[129]

With the continuing logarithmic growth of information networks, we predict that in the coming decade or two, the courts will be forced to rethink the accepted hierarchy of privacy interests. This hierarchy currently privileges personal and territorial privacy over informational privacy by restricting the latter to core, biographical information which, as we described above, can be conveniently (and *merely* temporarily) stripped away through various empirical techniques during its collection, in order to avoid *Charter* scrutiny. 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 these records tell our lifestories, 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[130] might, like the wall itself, come tumbling down.

Fortunately or unfortunately, the ultimate realization of any of our prognostications offered here is unlikely to be necessary in order to resolve the conflicting approaches in *A.M.* and *Kang Brown.* That said, when the Supreme Court of

---

[128] See Jonathan Hey, *supra* footnote 75.

[129] See James M. Nyce & Paul Kahn, eds., *From Memex to Hypertext: Vannevar Bush and the Mind's Machine* (San Diego, CA: Academic Press, 1991).

[130] See *supra* footnote 40.

Canada addresses the question of odour emanations, it ought and it must do so with a cautious eye toward the future. As the song goes, "the future is but a question mark."[131]

[131] Sting, "Bring on the Night" on *Bring on the Night* (A&M Records: 1986) track 1.