Reasonable Expectations Make Unreasonable Inferences: The Reasonable Expectation Threshold is a Legal Doctrine Unequal to the Menace to Privacy Posed by Mass Surveillance and Algorithmic Analysis

ROBIN MCLACHLEN [*]

ABSTRACT

This article argues that the reasonable expectation of privacy threshold is a legal doctrine woefully inadequate to emerging technologies of surveillance and prediction. Findings of no REP create zones of section 8 inapplicability wherein the state is impliedly licensed to seize information without judicial oversight or constitutional restraint. Inexpensive automated surveillance technologies promise to radically augment the quantity and quality of information these zones of section 8 inapplicability yield. Increasingly powerful computing systems now threaten to use this gathered information to support inferences of alarming accuracy and devastating specificity.

Following the introduction, the body of this article is divided into four parts. Part II provides a brief history of the REP threshold. Part III describes the threshold's patchwork application to various forms of technological

[*] JD, 2021, University of Ottawa, Common Law. An earlier draft of this article was awarded the Dierdre G Martin Memorial Privacy Award by the University of Ottawa Centre for Law, Technology & Society. Thank you to Vivek Krishnamurthy for his sagacious advice, unfailing encouragement, and expert editorial eye. Without him, this article would not exist. Thank you to Katie Szilagyi for being a Tech-Law mentor and real-life friend. Finally, thank you to the reviewers and editors at MLJ: their efforts made this article better.

surveillance. Part IV projects these common law precedents onto future applications, highlighting the dangers posed to privacy by emerging powers of surveillance and inference. Part V argues that the REP doctrine, even if modified piecemeal to meet emerging technologies, is inadequate to these powers.

In light of developing powers of surveillance and prediction, the article concludes by suggesting that the threshold doctrine be abandoned entirely, with specifically delineated legal authorizations substituted in its place.

I. Introduction

Every time a Canadian court holds that a method of state search and seizure does not infringe upon an applicant's reasonable expectation of privacy, it makes a public policy decision. The effect of that decision is to impliedly create a zone of section 8 inapplicability wherein law enforcement is entitled to act without any judicial or constitutional restraining mechanism. Until recently, these were policy decisions of limited scope.

But this is no longer so. Inexpensive automated surveillance technologies and increasingly powerful computing systems promise to radically augment the quality of information these zones of section 8 inapplicability can yield. Massive amounts of seemingly impersonal data, when fed through powerful new tools of automated analysis, can produce highly accurate inferences, potentially revealing very personal information about the lives and actions of Canadians. The threshold, instead of supporting a sustainable balance between individual privacy and the interests of law enforcement, threatens to fatally subvert the purpose of section 8's protection against unreasonable search and seizure. The doctrine should be abandoned, with specifically delineated legal authorizations substituted in its place.

II. A Very Brief History of the Reasonable Expectation Threshold

The concept of a 'reasonable expectation of privacy' – REP – has been with us since the earliest section 8 jurisprudence. In *Hunter et al v Southam Inc*, Chief Justice Dickson (as he then was) held that:

> The guarantee of security from unreasonable search and seizure only protects a reasonable expectation. This limitation on the right guaranteed by s. 8, whether

> it is expressed negatively as freedom from "unreasonable" search and seizure, or positively as an entitlement to a "reasonable" expectation of privacy, indicates that 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.[1]

Put simply, if a person does not have a REP in the subject area of the search, state interference is not unconstitutional. A search or seizure of something that does not meet the REP threshold does not violate section 8.

Clearly, defining this threshold would be of paramount importance to delineating the scope of the Canadian right to privacy[2] and the legitimate arenas of warrantless state surveillance. The Court expounded upon the reasonable expectation threshold next in *R v Edwards*.[3] Whether an expectation of privacy is 'reasonable' within the meaning of section 8 depended upon an evaluation of the 'totality of the circumstances.'[4] Reviewing judges should consider the following factors when assessing this 'totality':

> (i) presence at the time of the search; (ii) possession or control of the property or place searched; (iii) ownership of the property or place; (iv) historical use of the property or item; (v) the ability to regulate access; (vi) the existence of a subjective expectation of privacy; and (vii) the objective reasonableness of the expectation.[5]

In *R v Tessling*, the Court conceptualized privacy interests in three broad categories: personal, territorial, and informational.[6] Broadly speaking, these categories range from more protected to less, though they will often overlap. In the case of informational privacy – i.e., the category of privacy at issue in this article – the totality of the circumstances should be measured by considering (i) the subject matter of the search, (ii) the applicant's direct interest in that subject matter, (iii) whether the applicant held a subjective

---

1 *Hunter et al v Southam Inc*, [1984] 2 SCR 145 at 159–60, 11 DLR (4th) 641 [emphasis in original] [*Hunter*]. The concept was borrowed from American jurisprudence. In *US v Katz*, (1967) 389 US 347, Justice Harlan, in concurrence, wrote that Fourth Amendment protection depended upon a "two-fold requirement: first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"

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

3 [1996] 1 SCR 128, 132 DLR (4th) 31.

4 *Ibid* at para 31.

5 *Ibid* at para 45.

6 2004 SCC 67 at paras 20–24.

expectation of privacy, and (iv) whether that expectation is objectively reasonable.[7]

III. The Threshold's Application to Technological Surveillance

Because the REP threshold is measured against the 'totality of the circumstances' in a given case, its application to different forms of technological surveillance has been patchwork. In the case of Walter Tessling, infrared images of the heat patterns emanating from his house were found not to warrant constitutional protection as they did not reveal anything about his 'biographical core' of personal information.[8] Tessling's subjective expectation, per Justice Binnie (as he then was) for the majority, was not objectively reasonable.[9]

In *R v Plant*, the Court held that residents had no REP in their hydro records.[10] *R v Gomboc* extended the scope of *Plant* by finding that digital recording ammeters – devices placed outside a property that track hydro usage – give rise to no reasonable expectation, even if they are installed, not as a matter of course, but by a police officer's request.[11] In either instance, warrantless surveillance is justified.

Allowances for electronic audio and video surveillance are more nuanced. The Supreme Court of Canada, in *R v Duarte*, held that unauthorized electronic audio surveillance violates section 8.[12]

---

7 *Ibid* at para 32. Objective reasonableness, the fourth factor, is assessed by considering a host of sub-factors, some of which seem to have fallen into disuse. For one example, see Chris Hunt & Micah Rankin, "*R v Spencer*: Anonymity, the Rule of Law, and the Shriveling of the Biographical Core" (2015) 61:1 McGill JL 193.

8 *Tessling*, *supra* note 6 at para 63.

9 *Ibid.*

10 [1993] 3 SCR 281, 145 AR 104. It is a little more complicated than that, but not much: a REP exists only where the hydro company guarantees the customer's privacy. The reasonable expectation, here, is not technology-dependant but contract-dependant. So that: if the hydro company sees fit to guarantee your *Charter* right to privacy against state intrusion, the Court will condescend to guarantee it, too. If that seems a little bit backwards to you, dear reader, I humbly commend both your legal perspicacity and moral exactitude.

11 *R v Gomboc*, 2010 SCC 55.

12 [1990] 1 SCR 30, 65 DLR (4th) 240. However, and this is a pretty big 'however', a testifying officer, per *R v Fliss*, 2002 SCC 16, may 'refresh their memory' with the

Unauthorized video surveillance of an area in which an applicant has a REP is also unconstitutional.[13] Such state surveillance is governed by sections 487.01–487.019 of the *Criminal Code*.[14] More broadly, law enforcement's use of general video surveillance in public places (i.e., in places where an individual's REP has not been established) is instructed by guidelines published by the Office of the Privacy Commissioner of Canada.[15] Individually targeted video surveillance used on a case-specific basis, however, does not fall within their ambit.[16]

The installation and monitoring of tracking devices on vehicles by law enforcement is licensed only by section 492.1 of the *Code*.[17] This section was enacted following the Supreme Court of Canada's decision in *R v Wise* that the unauthorized installation of a tracking device on the applicant's vehicle violated section 8.[18] In a similar vein, the use of transmission data recorders[19] is governed by section 492.2.[20]

Perhaps of greatest concern, though, for the purposes of this article, is the legal doctrine of abandonment. *R v Dyment* drew a distinction between

---

transcript of an unconstitutionally obtained and excluded audio recording without that testimony being excluded.

13 *R v Wong*, [1990] 3 SCR 36, 1990 CanLII 56. "Where an applicant has a REP" is an admittedly large caveat – one whose too-broad ambit basically makes up the central subject of this paper – but its scope, as least for the purposes of video surveillance, appears to be shrinking. The video-surveillance REP has been recently extended beyond that which has been established for in person surveillance, existing in both the classroom, per *R v Jarvis,* 2019 SCC 10, and the common areas of multi-unit residential buildings, per *R v Yu*, 2019 ONCA 942, app for leave ref'd 2020 CanLII 41795 (SCC).

14 *Criminal Code*, RSC 1985, c C-46, ss 487.01–487.019 [*Code*]. The reasonableness /constitutionality of s 487.01 was affirmed in *R v Kuitenen and Ostiguy*, 2001 BCSC 677, and *R v Lucas*, 2014 ONCA 561. The constitutionality of 487.014 (and, presumably, the accompanying sections from 487.011–487.019) was affirmed in *R v Jones*, 2017 SCC 60.

15 "Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities" (2 March 2006) online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/vs_060301/> [perma.cc/VT97-MEH8].

16 *Ibid.*

17 *Supra* note 14, s 492.1.

18 [1992] 1 SCR 527, 51 OAC 351.

19 Per the *Code*, *supra* note 14, subsection 492.2(6), "a device … that may be used to obtain or record transmission data or to transmit it by a means of telecommunication."

20 *Ibid*, s 492.2. Warrants under section 492.1 and section 492.2 are issued on a reasonable suspicion standard.

the 'seizure' and 'gathering' of evidence: items in which an individual has abandoned their REP are not seized but merely gathered (i.e., they are not subject to section 8 protection).[21]

R v Patrick is the controlling case on this doctrine.[22] Its circumstances involved garbage left for collection outside a fence but still within property boundaries. Police officers seized the garbage and searched it, using the obtained evidence to ground a search warrant. The Supreme Court of Canada found that, though Russel Patrick maintained a subjective REP, this expectation was not objectively reasonable. Abandonment, Justice Binnie (as he then was) found for the majority, is a question of fact inferred from the totality of the circumstances, with specific attention paid to the applicant's behaviour toward the subject matter of their privacy claim.[23] By placing his garbage out for pick up, Patrick had abandoned any reasonable claim of privacy in its contents.

Applying the *Patrick* framework, *R v Delaa* found no REP in DNA evidence obtained through an undercover sting involving a fictional 'gum survey.'[24] Similarly, *Usereau c R* found no REP in a glass and straw left at a restaurant that police then submitted for DNA analysis.[25]

The courts may be revising these precedents, however, at least insofar as they relate to genetic material. The Quebec Court of Appeal, in *D'Amico c R*, recently found that abandoning a cup at a diner as a result of an undercover police operation did not equate to abandoning a REP in the genetic material found on the cup.[26] When a reasonable person leaves a used cup at a diner, they are not intending to abandon their DNA, Justice Vauclair found for the majority:

> [O]ne abandons [genetic material] everywhere, all the time without even giving the slightest thought to it. It is "the inevitable consequence of the normal functioning of the human body." One simply cannot infer, from the being of a person, one's intention to abandon the privacy interest in one's DNA information.[27]

---

21 [1988] 2 SCR 417, 55 DLR (4th) 503.

22 2009 SCC 17.

23 *Ibid* at para 25.

24 *R v Delaa*, 2009 ABCA 179.

25 *Usereau c R*, 2010 QCCA 894.

26 *D'Amico c R*, 2019 QCCA 77 at para 96–97 [*D'Amico*].

27 *Ibid* at para 99, citing *R v Stillman*, [1997] 1 SCR 607, 144 DLR (4th) 193.

Though the circumstances of DNA collection were nearly identical to that in *Usereau*, Justice Vauclair did not explicitly overrule that prior decision. Instead, he distinguished the precedent's factual scenario on the narrow basis that the DNA obtained by police in that instance had not been the result of an undercover operation.[28] Whether Canadians maintain a REP in genetic material that is abandoned in the normal course of daily activity, and not as a result of an undercover police operation thus remains an open question.[29]

IV. Projecting This Application Into the Future

The structure of section 8 applications *vis-à-vis* warrantless search and seizure is well established. To ground a claim of *Charter* breach, an applicant must demonstrate that a legally meaningful search has occurred by proving a reasonable expectation of privacy. Once this REP in the search's subject area has been demonstrated, the warrantless search in question becomes presumptively unreasonable and thus unconstitutional. If no REP is established, the *R v Collins* criteria – i.e. the meat on the bone of section 8's guarantee: that warrantless search and seizure must be authorized by a reasonable law and performed in reasonable manner – does not apply.[30]

The first step in this process is the critical inflection point for this article's thesis. Wherever courts have found no REP, they have simultaneously acknowledged, by implication, a lawless state power of search and seizure. Such 'search and seizure' is just called 'gathering' instead. By way of euphemism, the courts have thus created wide arenas of surveillance wherein Canadians' section 8 rights do not apply, and thus cannot reasonably constrain state interference.

To wit: *Tessling* found no REP in a building's heat emanations captured by infra-red imagery. This finding, without ever explicitly creating any

---

28 *D'Amico*, *supra* note 26 at para 116.

29 In Quebec, at least. In Alberta, where *Delaa*, *supra* note 24, remains the controlling precedent, they presumably do not, as they do not have a REP even in genetic material obtained by way of an undercover police operation. For more on the intersection between AI, genetic information and the Courts, see Jill R Presser & Kate Robertson, "AI Case Study: Probabilistic Genotyping DNA Tools in Canadian Criminal Courts" (June 2021), online (pdf): *Law Commission of Ontario* <www.lco-cdo.org/wp-content/uploads/2021/06/AI-PG-Case-Study-Final-EN-June-2021-2.pdf> [perma.cc/TR27-T352].

30 *R v Collins*, [1987] 1 SCR 265, 38 DLR (4th) 508.

reasonable power of search and seizure, authorizes infra-red surveillance by the police of every single building in Canada at all times, provided that the images obtained do not pictorially reveal what is going on inside. Similarly, per *Plant*, police are authorized to actively monitor all records of hydro consumption. Per *Gomboc*, the police are authorized to request (but not demand) that utility companies install digital recording ammeters outside every residence in the country and remit all recovered data to law enforcement. *Patrick* authorizes police sifting and examination of all garbage placed out for collection from all Canadian households. None of these powers of 'gathering' are subject to court review under the *Collins* criteria.

Emerging smart city applications suggest a host of other zones of section 8 inapplicability where law enforcement might use automated surveillance systems to gather evidence without concern for the *Charter* right to privacy: traffic patterns on public roadways and through public parks; household water and gas consumption; and, possibly, social media information.[31]

---

[31] In February 2020, the Office of the Privacy Commissioner announced investigations into Clearview AI's facial recognition software (software created from publicly scraped images and the RCMP's use of it. See "Commissioners Launch Joint Investigation into Clearview AI Amid Growing Concerns Over the Use of Facial Recognition Technology" (21 February 2020), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200221/> [perma.cc/V5S3-CJR5]; and "OPC Launches Investigation into RCMP's Use of Facial Recognition Technology" (28 February 2020) online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200228/> [perma.cc/3DRK-UCXY].
In July 2020, Clearview AI ceased operations in Canada. See "Clearview AI Ceases Offering its Facial Recognition Technology in Canada" (6 July 2020), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_200706/> [perma.cc/ZFT3-ACEE].
In October 2020, the OPC co-sponsored an international resolution on facial recognition technology, calling for principles of transparency, necessity, and proportionality in its usage and implementation by law enforcement. See "Adopted Resolution on Facial Recognition Technology" (October 2020) online (pdf): *Global Privacy Assembly* <globalprivacyassembly.org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-on-Facial-Recognition-Technology-EN.pdf> [perma.cc/6TAF-96YW].
In February 2021, the OPC found that Clearview AI's facial recognition software violated federal privacy laws. See "Clearview AI's Unlawful practices Represented Mass Surveillance of Canadians, Commissioners Say" (3 February 2021), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210203/> [perma.cc/M5V9-Z287].

The doctrine of abandonment suggests more still: as well as garbage, recycling, and compost, household wastewater seems plainly abandoned once it leaves the house and should thus, per *Patrick*, lie outside of any one individual's REP (whether DNA analysis is permitted or not,[32] it seems unlikely that chemical or viral analysis would be subject to section 8 review).

To date, these zones of section 8 inapplicability have not, broadly speaking, fundamentally altered the relationship between Canadian law enforcement and the public.[33] However, this has less to do with the prudence and foresight of our courts' decisions than it does with simple economics and manpower. To date, mass public surveillance, though implicitly sanctioned, has been economically and practically unfeasible.

In June 2021, the OPC found that the RCMP's use of Clearview AI's software constituted a significant violation of Canada's privacy laws and called for clearer laws on facial recognition technology, specifically. See "RCMP's Use of Clearview AI's Facial Recognition Technology Violated *Privacy Act*, Investigation Concludes" (10 June 2021), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/opc-news/news-and-announcements> [perma.cc/YDK3-HM64]; "Police use of Facial Recognition Technology in Canada and the Way Forward" (10 June 2021), online: *Office of the Privacy Commissioner of Canada* <www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/> [perma.cc/9EWK-PFBV].

It seems likely that facial recognition will soon come under much stricter regulation; continued indiscriminate and warrantless use seems manifestly unjustifiable. But facial recognition technology is far from the only use that social media information might be put to. If publicly available information were generalized, instead of specific – e.g., based on publicly available data, residents with IP addresses in postal code *x* are 53% more likely than the national average to 'like' social justice Facebook feeds, or feature pictures of a minivan, or post selfies in which the person pictured is wearing a blue hat, etc. – then it seems even more likely, by present common law doctrine, not to meet the REP threshold.

[32] ... and to what extent and for what purposes. For example, while current trends point towards the courts eventually protecting 'abandoned' DNA for purposes of personal identification, one can plausibly imagine the courts allowing 'de-identified' genetic (and viral and chemical) analysis. So that, just as CHEO Research Institute, in partnership with the City and the University of Ottawa, presently tests Ottawa's wastewater for COVID-19 viral copies (See "Ottawa COVID-10 wastewater surveillance" (last viewed 29 March 2022), online: *Ottawa COVID-19* <613covid.ca/wastewater/> [perma.cc/65JR-V4T9]), one can imagine a future in which public health and safety considerations might warrant wastewater testing for other infectious, or even hereditary diseases (e.g., West Nile, Zika, HIV, or sickle cell anemia) or chemical composition (e.g., banned substances). Given the rubric within which the courts are presently operating, it is difficult to imagine any one applicant persuasively asserting a REP in this sort of de-identified information.

[33] By which I mean: we do not, as yet, live in a police state.

Police departments have not had the manpower to place an observer outside every building in the country. Nor has it been economically feasible to employ officers to count every car that passes every intersection in the country; sift through every container of garbage, compost, or recycling collected each day across Canada; or review every Canadian household's hydro, gas, and water consumption daily, weekly, or monthly.

In the past, these zones of section 8 inapplicability could be reasonably designated by the courts as such because they were, practically speaking, information poor. The underlying reasoning is almost mathematical in the simplicity of its equation: the Court could fairly acknowledge no REP in these areas because, by and large, surveillance of these areas did not reveal much in the way of private information.

But cheap mass surveillance and algorithmic analysis are quickly altering the environment within which these findings of no REP have been made. An abundance of cheap surveillance technologies means that, for the first time in history, law enforcement can harvest vast amounts of data without busting their budgets. The development of powerful algorithmic analysis tools means that police departments need not employ armies of statisticians to sift through the mountains of data potentially at their disposal – computer programs can do it instead.

Even so, a profusion of mass surveillance of public areas would not represent any sort of major shift in Canadian public policy if these zones of section 8 inapplicability were actually as information poor as they seem. But they are not.

To take the first famous example: in 2002, Target, the US-based retailer, asked Andrew Pole if he could devise a way to determine whether a customer was pregnant without her revealing it. He could. Analyzing the recorded purchases of customers who had signed up for Target's baby registry service, Pole identified 25 key pregnancy-related products. He applied his findings to the rest of the Target database, and the company sent out a flurry of fliers and coupons. One customer thusly targeted was still in high school. Her father did not know she was pregnant, but Target did and, effectively, told him.[34]

---

[34] Charles Duhigg, "How Companies Learn Your Secrets", *New York Times Maganize* (16 February 2012), online: <www.nytimes.com/2012/02/19/magazine/shopping-habits.html> [perma.cc/SES5-646G].

One might reasonably wonder why a company would want to pry so deeply into its customers' lives. The explanation is, of course, money. Pregnant women are a much-

All of which is to say that publicly available, non-private information, when gathered and analyzed in bulk, potentially reveals, by inference, some very private and sensitive information. Even de-identified information can be privately revealing. The neighbourhoods in which we live, their traffic patterns, median income, utility usage, and foot traffic; the chemical and genetic composition of our wastewater; the contents of our garbage, recycling, and compost; the pictures we post online, the Facebook pages we like, and Twitter feeds we follow, when taken together, potentially reveal massive amounts of information about the ways in which we live and act, the things we think and believe in and care for. This is information that, up until now, law enforcement has not had easy access to. It is very much worth asking whether, and exactly how much, we want that to change.

In the past, the representations of the world that law enforcement could build from the common law's zones of section 8 inapplicability were simple and information poor. Police knew which neighbourhoods were relatively wealthy or impoverished or whether they had a particular ethnic or cultural identity. But the sum total of publicly available information supported few inferences about the specific identities, beliefs, lifestyles, and actions of individual Canadians.

Mass surveillance makes these seemingly information poor zones increasingly information rich. Algorithmic analysis has transformed the powers of inference that publicly available information can support. Clearview AI can create a saleable facial recognition program built entirely on publicly scraped data.[35] Predictive policing software – like GeoDASH – can use historical police data to anticipate the likelihood of break-and-enter crimes, allowing the Vancouver Police Department to deploy officers to high-risk areas.[36] Online, ubiquitous mass surveillance has become the

---

desired target demographic for marketers. Newborns disrupt their parents' lives and by implication, their purchasing habits, making new parents uniquely vulnerable to directed advertising. Birth records are public and so after a baby is born, parents are inundated with advertisements for diapers, formula, wet wipes, etc. If Target could detect a customer's pregnancy before the fact of the newborn made it a matter of public record, it could potentially capture a uniquely pliable audience well before any of its competitors knew of their existence.

35 See Kashmir Hill, "The Secretive Company that Might End Privacy as we Know It", *New York Times* (18 January 2020), online: <www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html> [perma.cc/R9BM-LUQ5].

36 See Kate Robertson, Cynthia Khoo & Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (September 2020) at 42–

defacto norm.[37] The internet of things[38] increasingly threatens to extend ubiquitous online surveillance into the real world, too.[39]

Combined with algorithmic analysis, mass surveillance threatens to dramatically augment the specificity and accuracy of the representations inferable from data gathered from the zones of section 8 inapplicability created by the common law. The theoretical endpoint of this trend, though still far off, should alarm anyone invested in liberty, democracy, and reasonably limited powers of state surveillance and control – namely, that algorithmically derived inferences could well become so rich and detailed to effectively mirror the world. With such an accurate representation, law enforcement could effectively surveil each and every citizen at all times without ever technically violating any individual's REP. Practically speaking, of course, such a picture could never be totally accurate. Algorithmically derived inferences are just that: inferences. But each inference, given enough data, would be very likely accurate; accurate enough, perhaps, to ground a search warrant.

The patchwork of common law rulings on reasonable expectations of privacy based on the inferences that can be drawn from a single mode of surveillance is a legal doctrine that is simply unequal to this future (and increasingly present)[40] world. If we want concrete, constitutional restraints against devolution into the sort of 1984-esque police state described above,

---

44, online (pdf): *Citizen Lab* <citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf> [perma.cc/42PP-TWZG].

37 "Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights" (2019) at 15–17, online: *Amnesty International* <www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF> [perma.cc/E5CX-HLD3].

38 Networked, physical objects (e.g., appliances, fixtures, thermostats, home security systems, cameras, etc.) connected to the internet and embedded with sensors that collect, exchange, and process data.

39 A close-to-home example, here, is Sidewalk Toronto – the recently abandoned development project proposed by Google's subsidiary, Sidewalk Labs, for Toronto's Quayside waterfront area. The proposed plan envisioned digital and physical layer integration, with data collection and storage built into the physical infrastructure of the community. See "Plan Development Agreement Between Toronto Waterfront Revitalization Corporation and Sidewalk Labs LLC" (31 July 2018) at 31, 47-50 online (pdf): *Sidewalk Toronto* <web.archive.org/web/20181127094844/https://sidewalktoronto.ca/wp-content/uploads/2018/07/Plan-Development-Agreement_July312018_Fully-Executed.pdf> [perma.cc/Q74Y-YK7Y].

40 See Bruce Schneier, "Modern Mass Surveillance: Identify, Correlate, Discriminate" (27 January 2020) online (blog): *Schneier on Security* <www.schneier.com/blog/archives/2020/01/modern_mass_sur.html> [perma.cc/P94S-A795].

we will need surer restraints on law enforcement than those the REP threshold provides.

V. Two 'Reasonables' Don't Make a Right

The foundational problem with the REP threshold, from the outset, has actually been one of grammar – namely, that the threshold doctrine inserts an extra adjectival modification into the constitutional guarantee.

The text of section 8 seems plain: it protects against unreasonable search and seizure. Unreasonableness describes the limit of legitimate police action. If one is free from unreasonable search and seizure, only reasonable search and seizure, by implication, is lawful. The question of reasonableness is asked of the state's action: was the search or seizure in question reasonable or not?

So far so good, but complications surfaced almost immediately. In *Hunter*, Chief Justice Dickson (as he then was) held that the limitation suggested by the word 'unreasonable' could be expressed either negatively, as a freedom from unreasonable search and seizure ("FUSS"), or positively, as a reasonable expectation of privacy.[41]

Whatever the necessarily 'liberal' and 'purposive' ambit of constitutional interpretation, this is plainly bad grammar. These adjectival modifications are simply not equivalent. They are not 'positive' and 'negative' expressions of the same limitation. In both instances, the same adjective is used, but it is modifying fundamentally different things.

With respect to the 'negative' limitation – FUSS – 'reasonableness' limits police powers and methods of search and seizure (i.e., if search and seizure powers or methods are unreasonable, they are unconstitutional). The Supreme Court of Canada laid out the process for determining this 'reasonableness' in *Collins*: a search or seizure must be authorized by a reasonable law and carried out in a reasonable manner.[42]

Conversely – as this article has hopefully made plain – the so-called 'positive' expression, REP, modifies the applicant's access to the section 8 right itself. 'Reasonableness,' here, does not limit state action. Instead, it limits the courts' powers of oversight to an examination of an applicant's expectations.

---

41 *Supra* note 1 at 159.

42 *Collins*, *supra* note 30 at para 23.

Though there is only one 'reasonable' in the constitutional text, practically speaking, an applicant must pass through two before their section 8 right carries any legal weight. Only where the 'totality of the circumstances' admits of a reasonable expectation of privacy can the right to be free from unreasonable search and seizure be invoked.[43]

The problem with the REP doctrine should, thus, be obvious: it is an extra-constitutional threshold test – an extra 'reasonable' – effectively inserted into the constitutional text. This extra 'reasonable' stands between Canadians and their section 8 guarantee. No such precondition exists for other *Charter* rights.[44]

Proponents of the REP threshold, of course, would argue that this precisely expresses its necessity. After all, not every state action is a search. Courts need a threshold to determine whether a given state action amounts to a search or seizure at all. The REP threshold, this argument goes, simply distinguishes 'searches' and 'seizures' from not.[45]

The problem with this argument is that the REP threshold has proven to exclude from section 8 protection numerous types of 'collection' that seem to be 'searches' or 'seizures' by another name (i.e., precisely the sort

---

43 That the 'totality of the circumstances' must be analyzed in order to determine whether a search or seizure has taken place means that, *contra* the principles of *Hunter*, *supra* note 1, the constitutionality of particular instances of warrantless search can only ever be assessed after the fact. Practically speaking, police officers do not know exactly what is constitutional, nor does the public.

44 Though the explicit/analogous analysis under section 15 bears some resemblance. As well, reasonable restrictions are licenced by section 1, but only where certain pre-conditions are met. The Court has never undertaken an *Oakes* analysis of the REP threshold doctrine, but it is interesting to consider whether it could pass the section 1 analysis if it were considered as a law limiting section 8's guarantee (proponents of the threshold, of course, would reason it would not (and does not) need to: the threshold itself is not *Charter* infringing; rather, it distinguishes infringement from non-infringement. Tomayto/tomahto.

45 The practical necessity of a threshold test is, I think, arguable, to say the least. People are not flooding the courts with section 8 applications in a vexatious demand for remuneration or positive state action; they are trying to get evidence excluded in response to the laying of criminal charges against them. Practically speaking, there seems to be little necessity to 'weed out' the fake searches and seizures from the real ones – whatever their name, the state actions in question have almost certainly yielded some form of evidence against the applicant. Whether these actions are 'reasonable' or not goes, I think, to the very purpose of constitutional review (whatever the reasonableness of the applicant's privacy expectations).

of state incursions that the *Charter* right was designed to protect against in the first place).

One need not look to algorithmic analysis to find obvious examples of the threshold's insufficiency. Despite *Wong*'s strong language about the dangers of state video surveillance, it yet impliedly authorizes mass video surveillance provided no individual's REP is violated. In the absence of effective constitutional interpretation, the Office of the Privacy Commissioner was obliged to step in, publishing guidelines on general purpose video surveillance by law enforcement of public places.[46] These guidelines are, of course, better than nothing, but they are also a far cry from robust constitutional protection. And the underlying legal difficulty remains: a seemingly tautologically correct application of the threshold doctrine[47] removed manifestly rights-eroding practices from court review on a constitutional basis.

As previously indicated, this doctrinal problem is only compounded when it comes to algorithmic analysis of masses of 'non-rights infringing' data. After all, not every bit of data, nor each method of collection will, on its own, rise to the REP standard. If collecting the data itself does not amount to a search or seizure, how can a court reasonably hold that analyzing the data amounts to a section 8 infringement? If no one was searched and nothing was seized, how can section 8 possibly apply?

Sandra Wachter and Brent Middelstandt suggest, in a different context, the assertion of a new human right – namely, a right to reasonable inferences. Wachter and Middelstandt further suggest that such a right, in a commercial context, would go some way towards mitigating the danger posed by algorithmic bias and inaccuracy.[48]

But it is hard to see how this proposed right maps neatly onto Canadian laws of search and seizure. A court's jurisdiction to constitutionally review under section 8 an inference derived from algorithmic analysis would depend upon characterizing that inference, or the analysis from which it was derived, as a search or seizure. An inference is neither – it is, instead, the outcome of the analysis of seized or gathered data. Characterizing an

---

46 See *supra* note 13.

47 Requiring a REP before section 8 protection can be invoked is, after all, the entire purpose of the REP threshold.

48 Sandra Wachter & Brent Middelstandt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI" (2019) 2 Columbia Bus L Rev 294.

algorithmic analysis as a search or seizure is similarly problematic. If the collection and human analysis of the same data would not amount to a constitutionally meaningful search or seizure, it is difficult to see why algorithmic analysis should meet that definition. After all, the gathered evidence in *Plant*, *Gomboc*, *Patrick*, and *Tessling* each led to inferences sufficient to ground search warrants. What is really so different about algorithmic analysis?

A right to reasonable inferences has the further problem of adding yet another extra-constitutional step to our already exceedingly complicated section 8 constitutional review procedure. Such a right also threatens to push purposive interpretation past its natural limits: the *Charter* contains no right against unreasonably perspicacious inferences, only unreasonable search and seizure.

A more likely solution lies in the piecemeal expansion of Canadians' recognized reasonable expectations of privacy as technological intrusions surface. The Supreme Court of Canada took this approach in *R v Marakah*,[49] *R v Reeves*,[50] *R v Mills*[51] and, most significantly for the purposes of this article, *R v Jarvis*.[52]

Jarvis involved a high-school teacher charged under the voyeurism provisions of the *Code* for taking surreptitious videos of his female students. The majority made three significant findings *vis-à-vis* reasonable expectations of privacy. First, people, in certain circumstances, maintain a REP in observable public places.[53] Second, REPs are more expansive with respect to technological surveillance than human observation.[54] Third, the Court affirmed and expanded upon its prior holdings that privacy is not an all or nothing concept: a lack of REP for one purpose does not mean that a REP is abandoned entirely.[55] Just because a person does not have a REP *vis-à-vis* short-circuit surveillance cameras installed to further public safety, for example, does not mean that they have no REP with respect to private surveillance for sexualized purposes.

---

49 2017 SCC 59, which extended applicants' REPs to include their text messages stored on recipients' phones.

50 2018 SCC 56, which acknowledged a REP in shared computers.

51 2019 SCC 22, which recognized a REP in online communications.

52 2019 SCC 10.

53 *Ibid* at para 38.

54 *Ibid* at paras 52, 62–63.

55 *Ibid* at paras 41, 61.

Going forward, reasonable expectations should be evaluated against these non-exhaustive considerations: the location where the surveillance took place, the type of surveillance/gathering, the presence or absence of consent, the manner of surveillance, the subject matter of the surveillance, any applicable rules or regulations, the relationship between the surveillor and surveilled, the purpose for which the information was seized/gathered, and the personal attributes of the person recorded/observed.[56]

Speaking generally, the courts' piecemeal expansion of applicants' REP is not without some rationale to recommend it. For one, it assures that legal evolution does not over-correct to a perceived problem before it has fully manifested itself. Relatedly, such piecemeal evolution allows the common law to specifically address evolving technologies of surveillance, each according to their individual intrusiveness, as they appear.

On the downside, this method of piecemeal response means that the law of search and seizure in Canada is always playing catch-up, responding to potentially widespread *Charter* violation only after the damage is done.[57]

More fundamentally, the problem of mapping algorithmic analysis and inference onto the existing law of search and seizure remains. The analysis in *Jarvis* focussed particularly on the modes of surveillance and the purposes for which the data in question is collected. The greater problem, at least with respect to algorithmic analysis, is what is done with all the collected and stored data after it has been gathered. Electricity usage is gathered for the purpose of billing users. Search histories are stored to target advertisements. Wastewater analysis is performed to measure population-level rates of COVID infection.

The issue is not how, why, or where the information is collected; it is what it can reveal. The courts to date have, quite understandably, misconceived the nature of private information. It is ubiquitous and fundamentally uncontainable. Whatever our reasonable expectations, collectible, highly personal data about us is everywhere, shed in dandruff, saliva, stray hairs, and finger-nail clippings. Sensitive, private information can be extracted from our utility consumption, wastewater, garbage, and travel patterns. It is inherent in our search, browsing, and streaming histories, our app usage and social media interactions, our publicly available images and videos, and the location data stored on our phones. Like genetic

---

56 *Ibid* at para 29.

57 And only once a litigable set of facts have entangled a sufficiently wealthy applicant and come under the scrutiny of a technologically proficient criminal defence attorney.

material, we emanate information wherever we go, whatever we do, [58] and it is being assiduously collected.[59] Infringements upon privacy no longer occur solely in easily delineated spheres – personal, territorial, informational. They can happen anywhere, in occurrences invisible to the human eye, in analyses impossible to the human intellect, in inferences unimaginable to our powers of supposition.

The hard and simple truth is that mass surveillance and algorithmic analysis are revealing bad legal doctrine. The distinction between 'gathering' and 'seizure' that the REP threshold demands has always been quibbling and subversive of robust section 8 protection.[60] It merely took the advent of ubiquitous surveillance and predictive analytics to demonstrate how inadequate our constitutional interpretations already were.

Instead of gradually expanding Canadians' REP or an acknowledging a right to reasonable inferences, this article advocates abandoning the threshold doctrine entirely. If the state wishes to search and surveil its citizens, it should be forthright about it and should do so only as authorized by law. The section 8 right is not, after all, absolute, but it may be limited, per *Collins*, by reasonable state restrictions. The tools in its kit are many. The common law authorizes a bevy of warrantless search powers like implied licence, plain-view, *Macdonald*, *Mann*, *Caslake*, etc. These could be adapted, restricted, or expanded where necessary. The ancillary powers doctrine licences courts to create new powers of search and seizure and to specify the conditions under which a given technological surveillance tool might be reasonably deployed. Parliament, as it has in other instances, could step in, and precisely delineate the circumstances and proper procedures for using algorithmic tools on legally gathered data, for sifting garbage, or for seizing genetic material.

The overbroad and patchwork allowances created by the REP threshold doctrine are cumbersome, confusing, and ultimately unnecessary.[61] In

---

58 See Ian Kerr & Jena McGill, "Emanations, Snoop Dogs and Reasonable Expectations of Privacy" (2006) 52:3 Crim LQ 392.

59 And, in the era of Big Data, most often without any single, particular purpose in mind.

60 Not that this should be determinative, but it is also the sort of distinction that makes everyone hate lawyers.

61 These broad allowances also contribute to the widespread uncertainty about exactly what may be legally searched or seized. To take but one example, absent the REP threshold doctrine, RCMP officers may not have imagined that they could utilize facial recognition technology absent legal authorization.

Wong, Justice La Forest (as he then was) cautioned that it would be wrong to limit to that specific technology *Duarte*'s finding that audio surveillance constituted a search and seizure:

> Rather what the Court said in *Duarte* must be held to embrace all existing means by which the agencies of the state can electronically intrude on the privacy of the individual, and any means which technology places at the disposal of law enforcement authorities in the future.[62]

It is past time that Canadian courts made good on that promise.

VI. Conclusion

The law of search and seizure in Canada has yet to come to terms with our increasingly powerful technologies of surveillance and analysis. Mass surveillance and algorithmic assessment threaten to bring section 8 jurisprudence into a state of crisis. But crisis brings both danger and opportunity. The danger is evident: court-created zones of section 8 inapplicability threaten to fatally undermine Canadians' right to privacy from unreasonable state intrusion. But the happy prospect presented by this looming crisis is equally significant – namely, the courts have a rare opportunity to clarify section 8 jurisprudence, resolving 30 years' worth of mounting confusion about 'reasonable expectations' and the distinguishing features of 'gathering' versus 'search and seizure.' In the process, the courts would streamline the process for bringing these *Charter* applications before the court, thereby eliminating tortuous and time-consuming arguments about the REP threshold. As it presently stands, the REP threshold subverts the purpose of section 8; it should be discarded.

---

62 *Wong*, *supra* note 13 at 43–44.