Algorithmic Policing Technologies in Canada

SHAWN SINGH [*]

ABSTRACT

Canadian law enforcement agencies are applying algorithmic technologies to identify individuals at the regional, provincial, and federal levels. These technologies connect templated facial images to an array of informational fragments that are collected from databases scattered between the public and private sectors. While that is the case, these surveillance technologies continue to be authorized under SCC jurisprudence, as opposed to legislation enacted by Parliament. Algorithmic technologies collate and analyze disparate information from public and private databases to identify patterns, which are then used to generate formulas to 'predict' future trends. Kate Robertson and colleagues explain that implementation of APTs by Canadian police services holds serious deleterious potential for the *Charter* rights of Canadians, with consequences that disproportionately affect people of colour. Be that as it may, the most malevolent consequence of applying APTs may be their application of generalized formulas to generate recommendations used to intercept individuals based on biased and inaccurate information. Although not authorized by statute, surveillance technologies continue to be permissible under common law authorities. Richard Jochelson explains the inappropriate nature of this approach, arguing in the alternative that the court's traditional role calls for application of the *Oakes* test to determine if state surveillant practices fall within its constitutional limits. Considering APT's serious implications for *Charter* protected rights, this paper calls on legislators to implement dedicated legislation to govern the use of surveillant technologies in law enforcement, with a particular focus on regulating the use of APTs. Failure to do so risks an unprecedented expansion of prejudicial policing practices, which may act to crystallize the existing biases in law enforcement practices

[*] Third-year law student at Robson Hall, Faculty of Law, University of Manitoba.

into objective 'scientific' outputs that may hold serious deleterious potential for Canada's most vulnerable populations.

Keywords: Algorithm; Policing; Technology; Search; Detention; Ancillary; Equality

I. INTRODUCTION

Law enforcement agencies are currently applying algorithmic technologies to identify individuals in Canada. These technologies connect templated facial images to an array of informational fragments that are collected from databases scattered between the public and private sectors. These databases include state-held information like drivers' licencing information, as well as corporate records including social media information, facial recognition databases, CCTV recordings, and many others. Algorithmic technologies collate and analyze these disparate data fragments to identify patterns that are intended to generate formulas to 'predict' future trends. These formulae can also be applied to determine whether a particular target matches defined selection criteria. Results generated from these 'black-box' calculations may appear like an objective science, but closer analysis reveals this technology's foundational reliance on observational biases that are crystallized into the enforcement records used to train this technology.

Algorithmic Policing Technology (APT) is "trained" to identify patterns related to criminal behaviour using inputs of historical law enforcement data. This is troubling – a short review of Canada's criminal justice literature reveals a long history of racial prejudice in law enforcement practices. Police, prosecutions, and the courts have maintained a consistently disproportionate focus on people of colour, with particular attention on Indigenous individuals and communities. While this reality is resoundingly captured in the literature, it is unlikely that historical enforcement records maintain a critical perspective regarding the policing practices applied in the field. The combined effect of using biased enforcement records with the ongoing operation of prejudicial enforcement practices in the field holds serious deleterious potential towards the generation of APT formula and applying its outputs to identify prime intervention opportunities for patrolling officers. Police services in major metro centres like Vancouver, Calgary, and Saskatoon have trained and applied different forms of APT to

monitor citizen activity, respond to anti-social behaviour in 'real-time,' and, in some jurisdictions, predict optimal deployment of police resources.

Kate Robertson and her colleagues at Citizen Lab conducted a prospective analysis of APT use in Canada's police forces.[1] Although limited to obtainable information from these agencies, their research provides a comprehensive description of this new technology and projects its potential to alter the law enforcement landscape in Canada. They highlight the expansion of APTs in recent years, as well as several inherent flaws that are rooted in APT components, such as using biased information to "train" APTs, applying its vast data-processing capabilities and recommending arguably unreliable outputs to inform officer interventions. Police use APT outputs to make decisions about whether to interfere with an individual's liberty, whether that intervention is simple questioning, detention, or arrest. As agents of the state, execution of these powers against an individual activates *Charter* protected rights against unreasonable search and seizure, and arbitrary detention, as well as the residual guarantee of equality before the law at the social level.

While Canada's courts have yet to formally analyze the influences of algorithmic decision-making on broader policing practices, the Supreme Court of Canada continues to authorize the use of broader surveillance technologies under the common law ancillary powers doctrine. *Charter*-protected rights are engaged when agents of the state directly collect or access historical records.[2] This includes accessing fragmented bits of information, like photos or social media posts of disparate information contained in a variety of public records. Although engaged, our highest court finds that the 'examination' of abandoned informational material fails to constitute a search because the user cannot maintain a reasonable expectation of privacy.[3] Alternatively, access to corporate service records may be consented to under statute or implication, which allows the state to access these data fragments for enforcement purposes. This level of informational surveillance may be reasonable in the context of case-by-case access, but the invasive potential of algorithmic assembly and its application

---

1 Kate Robertson, Cynthia Khoo & Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (1 September 2020), online (pdf): *Citizen Lab: Transparency and Accountability in Research* <citizenlab.ca/wpcontent/uploads/2020/09/To-Surveil-and-Predict.pdf> [perma.cc/FBA9-V344].

2 *R v Morelli*, 2010 SCC 8 [*Morelli*]; *R v Spencer*, 2014 SCC 43 [*Spencer*].

3 *R v Patrick*, 2009 SCC 17 [*Patrick*].

is exponential. Rapid collection and collation of fragmented datasets to present profiled information to officers in 'real time' certainly reveals more biographical information of a person of interest than using heat-sensing equipment or sniffer dogs.[4] Further to this, standards of reliability regarding APT recommendations have yet to be established. This shortfall is concerning. Robertson and colleagues explain that reported matches remain highly uncertain because of inherent flaws in APT equipment, as well as the influence of surrounding environmental conditions at the time and spaces where APT recommendations are produced. Considering the application of these technologies by Canadian police to interfere with the *Charter*-protected rights of Canadians, this paper asserts that the legal authority to do so ought to stem from legislation, rather than the common law.

Police surveillance powers have promulgated under the auspices of the SCC's ancillary powers doctrine. Richard Jochelson explains the role of the *Waterfield* test in expanding police powers in the absence of legislative authorization by examining SCC decisions that sanction the use of investigative tools like roadblocks, sniffer dogs, and investigative detention.[5] While outside the traditional role of an adjudicative court, surveillant technologies have become constitutionally authorized under the common law, rather than legislation. This approach may have been reasonable when surveillant traces did not reveal core biographical information about an individual's life, but the power to assemble this information into suspect profiles and apply them to prevent a predicted breach of the peace likely exceeds the current scope of existing authorities.

Considering these risks, along with the inherent flaws of APT, it is clear that legislation is required in this area. The validity of technologically enhanced state surveillance has persisted under the common law, but the addition of APT goes well beyond established precedents. Rather than allow *Charter*-protected rights to be infringed on an ongoing basis, legislation from Canadian governments should be implemented to contour the field's development while it is still maturing. The research of Robertson and colleagues provides a strong foundation for the development of a robust

---

4 *R v Tessling*, 2004 SCC 67 [*Tessling*]; *R v Kang-Brown*, 2008 SCC 18 [*KB*]; *R v M(A)*, 2008 SCC 19 [MA].

5 Richard Jochelson, "Ancillary Issues with Oakes: The Development of the Waterfield Test and the Problem of Fundamental Constitutional Theory" (2017) 43:3 Ottawa L Rev 355; *Tessling*, *supra* note 4; *KB*, *supra* note 4; MA, *supra* note 4.

governing framework for APT surveillance by local law enforcement agencies.[6] This paper echoes the recommendations contained in *To Surveil and Predict* to urge Canadian governments to establish APT policies that can remain consistent with the *Charter*-protected rights of Canadians.

This paper offers a primer on the existence of algorithmic enforcement practices and their role in Canada. Using Robertson and colleague's research as a guideline, Part II reviews the fundamental concepts behind algorithmic policing, its preparation for field application, and the risks inherent to this process. We will review the historical, social environment that is captured in criminal justice records to highlight the systemic prejudice that risks becoming woven into APT outputs. In addition, we will also discuss data inaccuracies related to police interventions like detention and arrest. Part III describes the use of APTs in Canadian police services in Alberta and Saskatchewan to demonstrate different approaches to ATP development in this jurisdiction. Part IV provides a *Charter* analysis of the rights that can be engaged with APT deployment, with particular focus on rights against unreasonable search and seizure (s. 8) and arbitrary detention (s. 9). As part of this analysis, we will review the established bright-line standards, as well as the jurisprudence that authorizes modern surveillance practices as 'reasonable.' Part V reviews the work of Richard Jochelson, who describes the ancillary powers doctrine and its role in authorizing these investigative tools. His description of the *Waterfield* test will guide this discussion, as well as its contraposition to determining the constitutionality of state action under the *Oakes* test. Part VI reviews Robertson and colleague's recommendations to government regarding APT in order to contrast the benefits of implementing dedicated APT legislation against the risks that can arise under a more flexible regulatory regime. We build on these recommendations to assert that the only meaningful solution is firm legislation, at least in terms of criminal justice. Regulatory flexibility may be appropriate for the private sector but cannot address the prospective consequences for marginalized populations that can result from the implementation of APTs under the current framework. Concluding remarks are found in Part VII.

---

6 Robertson, Khoo & Song, *supra* note 1.

II. ALGORITHMIC POLICING FUNDAMENTALS

In response to the exponential expansion of technological surveillance in Canadian policing practices, Kate Robertson and her colleagues at Citizen Lab conducted research that highlights the potential they hold to infringe the *Charter*-protected rights of Canadians. Their prospective research focuses on several flaws inherent to APTs, which are rooted in historical record-keeping methods of local state services, the use of these records to train new APT software, and the reliability of its data outputs. But what is algorithmic technology?

Simply put, these technologies generate mathematical formulas using historical information to achieve defined outputs.[7] A computer automatically generates formulae by analyzing input information against historical outcomes to identify patterns that can be represented mathematically.[8] In general, some algorithmic technologies apply generated formulas to assist or substitute human decision-making, like artificial intelligence applications. When applied to the law enforcement context, APT applies these automatically generated formulae to rapidly collect, analyze, and collate mass database information to make on-the-spot identifications of targets. Tools like automated licence plate readers or cameras with access to facial recognition software are used to identify individuals and match them with databased information. Alternatively, APT outputs may be applied to predict unlawful activity before it happens by extrapolating on a series of factors.

A key feature of APT is its ability to adjust formulas as new input data is received to achieve stronger matches to desired APT outcomes. An APTs original rules are generated using large training data sets, which are autonomously updated as more data is provided. The system is designed to optimize outputs to achieve the desired goals of program administrators. The formulas are continuously optimized through "data mining" or the "practice of searching through large amounts of computerized data to find

---

7 *Ibid* at 29–31.

8 Royal United Services Institute, "Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges" (September 2018) at 2, online (pdf): *University of Winchester Centre for Information Rights* <rusi.org/sites/default/files/201809_whr_3-18_machine_learning_algorithms.pdf.pdf> [perma.cc/QJ6R-KKBJ].

useful patterns and trends."[9] Some household examples of machine learning include computer identification of images, as well as speech recognition that allows conversion-to-text that is a common feature of new cell phones.[10] Machine learning can be supervised, where input data sets are labelled with defined outcomes, or unsupervised, where the system determines which variables are relevant in unlabeled data sets. In both cases, APTs generate algorithmic formulas to represent the patterns identified by the software.[11]

While this can be beneficial, it also presents accountability and oversight concerns. Robertson and colleagues explain that machine learning is considered to be a "black-box" phenomenon, where people typically do not understand its inner workings because of its inherently amorphous nature.[12] This issue is compounded by proprietary concerns, like trade secrets, that work against revealing the processes that make algorithmic products unique in an increasingly competitive marketplace. This framework is especially concerning because it is difficult to assess the reliability of a given algorithm, including identification of flaws in its formula or inclusion of unintended factors in achieving defined outputs. For example, an algorithm may successfully identify images of wolves against dogs using snow in image backgrounds.[13]

In the context of law enforcement, the 'training' of algorithmic software using historical policing records presents a serious risk of recreating biases that influence the criminal justice system's disproportionate focus on marginalized populations. Robertson and colleagues assert that APTs must be trained on data that is accurate and representative of the subject matter being studied.[14] Failure to prevent inputs of inaccurate or biased information will result in tainted outputs that risk being hidden as a

---

9 Walter L. Perry et al, "Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations" (2013) at 34, online (pdf): <www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf> [perma.cc/M65M-DTZZ].

10 "Human Rights in the Age of Artificial Intelligence" (November 2018) at 10, online (pdf): *Access Now* <www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf> [perma.cc/7TSZ-NWGX].

11 Royal United Services Institute, *supra* note 2 at 18–19.

12 Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, Massachusetts: Harvard University Press, 2015) at 3.

13 Robertson, Khoo & Song, *supra* note 1 at 31.

14 *Ibid* at 31–32.

function of APTs "black-box" nature. They refer to this statistical concept as simply "garbage in, garbage out", where gaps or other problems in a data set cause an algorithm's outputs to be unrepresentative of reality. Algorithmic facial recognition software is subject to these concerns when trained on data sets that underrepresent or misrepresent certain populations, like groups categorized on the basis of gender, age, or race.[15] APT training presents a prime opportunity for systemic biases to taint output results because of the technology's primary reliance on historical policing information. The Government of Canada recognizes our history of systemic and institutional racism against people of colour, with a particular focus on Indigenous peoples.[16] These effects are exponentially pronounced in the criminal justice system, where police were historically deployed to control culturally heterogeneous groups to maintain the settler-colonial status quo. Training APTs with this type of data will generate inferential rules based on the patterns identified in law enforcement reports. "If systemic biases permeate data sets that are produced in Canada's criminal justice system, these biases may become embedded in and perpetuated by APT to the further detriment of individuals and communities that have been the subject of historic discrimination."[17]

The risk of amplifying historically systemic racism is serious. For those communities that have been disproportionately impacted by the criminal justice system in the past, the adverse effects of training APT on this data can be significant and long-lasting. Literature produced by researchers and government inquiries confirm that Canada has a long history of systemic and institutional racial bias in criminal justice. The Aboriginal Justice Inquiry explained that the over-representation of Indigenous peoples in the criminal justice system is directly rooted in this history.[18] Indigenous peoples in Canada are more likely to be arrested, charged, detained in

---

15 Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" (2018) 81:1 Proceedings of Machine Learning Research 1 at 1, online: <proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf> [perma.cc/B5EN-2ZY2].

16 Canada, Canadian Heritage, *Building a Foundation for Change: Canada's Anti-Racism Strategy* (17 July 2019), online: <www.canada.ca/en/canadian-heritage/campaigns/anti-racism-engagement/anti-racism-strategy.html> [perma.cc/6THR-SDF2].

17 Robertson, Khoo & Song, *supra* note 1 at 15.

18 *Report of the Aboriginal Justice Inquiry of Manitoba*, vol 1 (Manitoba: AJIC, 2001) at ch 4, online: <www.ajic.mb.ca/volumel/chapter4.html> [perma.cc/A9HQ-54EW].

custody without bail, convicted, and imprisoned.[19] Indigenous Canadians also suffer from higher rates of victimization by crime and violent crime,[20] as well as other negative criminal justice outcomes like overrepresentation in correctional institutions.[21]

The issue of systemic racial discrimination has been acknowledged by Canadian legislatures in recent years. Most recently, the Ontario Human Rights Commission issued an Interim Report into practices of racial profiling and discrimination by members of the Toronto Police Service. The Tulloch Report concludes that sample regions consistently conducted disproportionate policing of racialized communities.[22] Canada's Heads of Prosecutions also recognized the effects of racial bias on law enforcement practices in 2018.[23] At a more local level, provincial inquiry reports recognized the issue of racial bias in law enforcement much earlier and at more regular intervals. For example, racial bias was found to be a prominent

---

19 *Ibid*; Canada, Royal Commission on Aboriginal Peoples, *Bridging the Cultural Divide: A Report on Aboriginal People and Criminal Justice in Canada* (Ottawa: Canada Communication Group, 1995) (René Dussault & Georges Erasmus) at 309–11; Statistics Canada, *Victimization of Aboriginal People in Canada, 2014*, by Jillian Boyce, Catalogue No 85-002-X (Ottawa: Statistics Canada, 2016), online: <www150.statcan.gc.ca/n1/pub/85-002-x/2016001/article/14631-eng.htm> [perma.cc/2FXS-AELA]; "Set Up to Fail: Bail and the Revolving Door of Pre-trial Detention" (July 2014) at 19, online (pdf): CCLA <ccla.org/cclanewsite/wp-content/uploads/2015/02/Set-up-to-fail-FINAL.pdf> [perma.cc/T5UR-8YTJ]; Canada, *Office of the Correctional Investigator Annual Report 2019–2020*, by Ivan Zinger (Ottawa: CIC, 2020), online: <www.oci-bec.gc.ca/cnt/rpt/annrpt/annrpt20192020-eng.aspx#s10> [perma.cc/2QY8-56B2].

20 Jonathan Rudin, "Aboriginal Peoples and the Criminal Justice System," *Ontario Ministry of the Attorney General* (9 March 2017) at 1–8, 36–40, online (pdf): <www.attorneygeneral.jus.gov.on.ca/inquiries/ipperwash/policy_part/research/pdf/Rudin.pdf> [perma.cc/DLL5-6LQL].

21 Boyce, *supra* note 18; CIC, *supra* note 18; Canada, *Justice on Trial: Report of the Task Force on the Criminal Justice System and Its Impact on the Indian and Metis People of Alberta*, vol 1 (Edmonton: Task Force, 1991) (Hon Justice Robert Allan Cawsey) at 2-5, 2-46 to 2-51.

22 Ontario Human Rights Commission, *A Collective Impact: Interim report on the inquiry into racial profiling and racial discrimination of Black persons by the Toronto Police Service* (Ontario: OHRC, November 2018), online: <www.ohrc.on.ca/en/public-interest-inquiry-racial-profiling-and-discrimination-toronto-police-service/collective-impact-interim-report-inquiry-racial-profiling-and-racial-discrimination-black> [perma.cc/HMH2-246A].

23 Public Prosecution Service of Canada, *Innocence at Stake: The Need for Continued Vigilance to Prevent Wrongful Convictions in Canada* (Ottawa: PPSC, 2019) at ch 10, online: <www.ppsc-sppc.gc.ca/eng/pub/is-ip/ch10.html> [perma.cc/ZWP4-K6SW].

feature in the convictions of Donald Marshal Jr., Thomas Sophonow, and many others.[24]

The pervasiveness of these issues has led the SCC to take judicial notice of its prevalence in Canadian law enforcement practices. The Court's majority recognized the systemic overrepresentation of Indigenous peoples in their landmark decision *R v Gladue*.[25] They found that Canada's criminal justice system has, in essence, assumed the role of residential schools in reclaiming Indigenous youth. Building on this finding, the Truth and Reconciliation Commission of Canada includes addressing this issue in their Calls to Action.[26] The SCC has also acknowledged the aggressive effects of racialized enforcement practices against other minority populations, like Black and Asian Canadians.[27]

Research shows that issues of racial bias continue to affect frontline policing practices. Police often intercept Indigenous and Black Canadians in circumstances where the individual in question is subjected to harsh treatment by law enforcement authorities, even when found to be doing nothing outside the liberty rights enshrined under s. 7 of the *Charter*. Robertson and colleagues reviewed recent studies in the Toronto area, which concluded that people of colour were more likely to be held in custody and brought to bail court, rather than released for simple marijuana possession.[28] Research conducted by Scot Wortley and Akwasi Owusu-

---

24 Nova Scotia, *Royal Commission on The Donald Marshall, Jr., Prosecution: Digest of Findings and Recommendations* (Halifax: Royal Commission, 1989) at 1–3, online: <www.novascotia.ca/just/marshall_inquiry/_docs/Royal%20Commission%20on%20the%20Donald%20Marshall%20Jr%20Prosecution_findings.pdf> [perma.cc/RK5W-E22G] [Royal Commission]; Manitoba Justice, *The Inquiry Regarding Thomas Sophonow* (Manitoba: Manitoba Justice, 2010) (Peter Cory), online: <digitalcollection.gov.mb.ca> [perma.cc/AG8P-DCJF]; Canada, *Report of the Commission of Inquiry into Certain Aspects of the Trial and Conviction of James Driskell* (Manitoba: Lieutenant Governor-in-Council, 2007) (Hon Patrick J. LeSage), online: <www.driskellinquiry.ca >[perma.cc/DDN9-4RPY].

25 *R v Gladue*, [1999] 1 SCR 688 at paras 60–65, 171 DLR (4th) 385.

26 Robertson, Khoo & Song, *supra* note 1 at 16; *Honouring the Truth, Reconciling for the Future: Summary of the Final Report of the Truth and Reconciliation Commission of Canada* (December 2015), online: <publications.gc.ca/pub> [perma.cc/EX26-XX6W].

27 *R v Le*, 2019 SCC 34 at paras 93–95 [*Le*]; *R v Grant*, 2009 SCC 32 at paras 133, 154–55 [*Grant*].

28 Jim Rankin & Sandro Contenta, "Toronto marijuana arrests reveal 'startling' racial divide" (6 July 2017), online: *Toronto Star* <www.thestar.com> [perma.cc/676U-TSCC]; Alex Luscombe & Akwasi Owusu-Bempah, "Why legalization won't change racial

Bempah into Toronto stop-and-search practices further confirm this reality.[29] Their study concluded that Black respondents were much more likely to report being stopped and searched by police, as opposed to respondents from other racial backgrounds. Black respondents were also found to be more likely to report vicarious experiences of racial profiling from police as part of routine information gathering. They noted that patrolling officers were much more likely to stop Black Torontonians in circumstances where the investigator could see the complexion of the suspect.

These results highlight the tainted nature of information captured in historical police reports. Police have access to vastly disproportionate amounts of information about racialized individuals and about marginalized neighbourhoods, which may form the basis of training APT algorithms.[30] Police data includes subjective, statistical, and biographical information that is collected by frontline and internal workers. Examples of information currently processed by APTs in Canada include, but are not limited to, criminal survey statistics, social media posts, geolocation data, crisis centre call logs, hospital injury data, and criminal activity data collected by non-police security personnel such as transit, campus, or mall cops or private security.[31] By using this data to inform future police interactions, the feedback effect of their use to predict future police interventions will likely exacerbate existing biases that are continuously recreated as part of the daily operations of the police.

The above is not an exhaustive representation of the data that can be used to train APTs but provides a snapshot of the systemically biased considerations that risk becoming assumed as part of APT outputs. These data are used to train algorithms in massive quantities from wide-ranging sources. APTs use this information to generate forecasts about people or locations, which police use to inform 'reasonable suspicions' that allow them to interfere with an individual's liberty. Considering these risks, Robertson and colleagues note that:

---

disparities in cannabis arrests" (19 April 2018), online: *VICE* <www.vice.com> [perma.cc/QY9U-P9GL].

29 Scot Wortley & Akwasi Owusu-Bempah (2011) "The Usual Suspects: Police Stop and Search Practices in Canada" 21 Intl J Research & Society 395 at 395–407.

30 Robertson, Khoo & Wong, *supra* note 1 at 19–20.

31 *Ibid* at 18–19, 47–58.

> [I]t is imperative that these new methods do not contribute to the historic disadvantage experienced by communities targeted by systemic bias. Preventing the perpetuation of systemic bias and discrimination includes asking questions such as whose personal information is being collected or used by the technology, and which individuals or communities will be most affected, and why?[32]

It is clear from this discussion that the training and deployment of APTs present a serious risk of crystallizing enforcement biases that are continuously recreated as a function of the structure of law enforcement practices in Canada. While that is the case, Robertson and colleague's research highlights how Canadian police services are developing and implementing these technologies, regardless of their knowledge of their deleterious effects against marginalized Canadians, such as people of colour.

III. APT Models in Canadian Police Services

Canadian police services have already started to acquire, train, and employ APTs in their jurisdictions. Services utilize this software in different ways: some apply APTs strictly as real-time surveillance tools, whereas others apply APT formulas to predict necessary police interventions. Robertson and colleagues analyzed the strategic planning and budget documentation of police services across the country to reveal their intentions to deploy APTs in their jurisdictions. Their research identifies the use of terms like "predictive," "data-driven," or "intelligence-led" policing, which all emphasize the development and application of data-analytic software.[33] APTs currently deployed in Canadian jurisdictions can be separated into two categories: location-focused APTs, like those employed by the Toronto Police Service, and person-focused APTs, like those acquired and employed by the Calgary Police Service (CPS), or those being developed internally by the Saskatchewan Police Predictive Analytics Lab (SPPAL). Our discussion remains focused on person-focused APTs, but many of the concerns raised apply to location-focused APTs as well. This section reviews two models of person-focused APTs (PFAPTs) in Canada to caution against latent predictive functions that are available in 'off-the-shelf' programs from

---

32 *Ibid* at 24–25.

33 *Ibid* at 36–37; "2011 Winnipeg Police Service Annual Report" (2011) at 9, online (pdf): *Winnipeg Police Service* <www.winnipeg.ca/police> [perma.cc/VB5D-DHP2]; "2018 Edmonton Police Service 2018 Annual Policing Plan" (2018) at 5–6, online: *Edmonton Police Commission* <edmontonpolicecommission.com> [perma.cc/P7GW-5YER].

international software developers, as well as to recommend a more localized approach to develop APTs and their databases.

Andrew Ferguson explains that PFAPTs are designed to assist police on two fronts: PFAPTs are used to identify individuals who may become involved in future criminal activity or to assess the level of risk held by an identified individual to engage in criminal activity or become a victim themselves. Assessments are made using personal details, like information about family, friends, associates, social media activity, criminal records, or appearances in auxiliary databases that are connected to the software.[34] This information is submitted to APT software, which generates risk score outputs that are used to inform police decisions to intervene.[35] The overarching result of APT application in these contexts is to bring suspected individuals into contact with the criminal justice system. All APT models implemented in Canada follow this structure, including the programs acquired by the CPS and under internal development by the Saskatchewan Police Service.

A. Calgary Police Service's Palantir Gotham

The CPS adopted an APT developed by Palantir Technologies, which operates in tandem with IBMs i2 Analyst Notebooks.[36] This APT program was developed by New Orleans-based Palantir, with an intended application of unifying a series of separate public record databases and conducting "Social Network Analyses" that could reveal hidden relationships in the massive, unified data set.[37] Palantir technology has been employed across the USA; their marketing team is intently focused on expanding into the Canadian marketplace.[38] Similar to its application in New Orleans, Calgary

---

34 Andrew G. Ferguson, "Policing Predictive Policing" (2017) 94:5 Wash UL Rev 1109 at 1137–134.

35 Robertson, Khoo & Song, *supra* note 1 at 45–46; "Strategic Subject List" (25 September 2020), online: *Chicago Data Portal* <data.cityofchicago.org/Public-Safety/Strategic-Subject-List/4aki-r3np> [perma.cc/77AM-8EWP].

36 Robertson, Khoo & Song, *supra* note 1 at 47–48; "Latest News" (2021), online: *Palantir Technologies* <www.palantir.com/media/>.

37 Andrew Papachristos & Michael Sierra-Arévalo, "Policing the Connected World" (2018) at viii, online: *Office of Community Oriented Policing Services* <cops.usdoj.gov.pdf>.

38 Robertson, Khoo & Song, *supra* note 1 at 50–51; Justin Ling, "Palantir's big push into Canada" (25 October 2019), online: *OpenCanada.org, Centre for International Governance Innovation* <opencanada.org/palantirs-big-push-into-canada/> [perma.cc/GP8R-FQ9A]; Murad Hemmadi, "Palantir's MacNaughton says data-mining firm is working with Ottawa, three provinces on COVID-19", *The Logic* (30 April 2020), online:

first implemented Palantir Technology products to unify disparate databases to reveal latent relationships disbursed within the separated information. Although inactivated by the CPS, operational Palantir documentation indicates that its APTs can expand data collection protocols to process open-source information like publicly available social media data, email, and telecommunications records, as well as third-party information like financial records and credit history. The associations and connections generated by Palantir Technologies are used to inform officers of the relationships and behaviours that individuals exhibit in public and quasi-public spaces. Profiled information is stored for every individual who interacts with police, including witnesses and victims. Further, auxiliary information is often collected about an accused, like religious affiliation. Palantir uses this information to make immediate intervention recommendations to officers on duty and to map out locations where service calls are taking place."[39]

The CPS appropriately recognizes that police assessments informed by Palantir outputs may present false associations between innocent individuals and broader criminal suspects. While that is the case, they failed to disclose that CPS's Palantir system does not have a critical oversight mechanism activated while applying the software in the field. The "Governance Entity" is not currently in operation but is designed to provide oversight mechanisms for data quality, implementation of new features, acceptance of new data sources, and review of privacy implications related to Palantir outputs. Rather than engage the Governance Entity, the CPS prefers to depend on general oversight mechanisms that are already in place for broader CPS activities. As an internationally accredited software suite that continues to be endorsed in leading jurisdictions like the USA, Palantir offers software that can support law enforcement objectives, reduce government expenditures on internal software development costs, and provide access to databased information from Palantir's jurisdictional partners. While this approach has its merits, the following section highlights the alternative model being developed by the SPPAL.

<thelogic.co/news/exclusive/palantirs-macnaughton-says-data-mining-firm-is-working-with-ottawa-three-provinces-on-covid-19/> [perma.cc/YNS2-CBRX]; *Wakeling v United States of America*, 2014 SCC 72.

39 Robertson, Khoo & Song, *supra* note 1 at 47–50.

B. Saskatchewan Police Predictive Analytics Lab

Rather than purchase an 'off-the-shelf' APT program, the Government of Saskatchewan, the Saskatoon Police Service (SPS), and the University of Saskatchewan partnered to establish the SPPAL.[40] This program was originally intended to be a project to locate missing persons but was expanded to address a series of community safety issues. The SPPAL examines risk factors and behaviour patterns detected among Saskatchewan youth who are later reported as missing. Social patterns in this behaviour became identifiable and were used to develop an algorithmic model to identify children who may be at risk of going missing in the future. The program is being developed for integration with Saskatchewan's broader HUB risk assessment model, which connects marginalized individuals with social service interventions, where appropriate. The HUB model systemically shares information between social service and law enforcement agencies to provide a whole-of-government approach to encourage proactive intervention before a report is made to a HUB service provider like police or mental health services.[41] This software is still in testing phases, but Robertson and colleague's research notes that output information will be shared with the government beyond law enforcement.

Distinct from the broad "unifying" approach that is applied by Palantir software, SPPAL only works with municipal policing data from the SPS. SPPAL has expressed intent to expand data access to include data sets from the RCMP "F" Division but has yet to take place. As a government enterprise, SPPAL has openly expressed their intention to include social media data in APT training and development in the future. While that is the case, measures are simultaneously being taken to ensure that strong privacy safeguards related to data encryption, confidentiality, and storage are put in place.[42]

In its current form, the SPPAL is uniquely focused on the preemptive identification of victims and those who may cause harm to themselves. The purpose of this software is to execute needs-based analyses to connect vulnerable individuals with prevention strategies, as opposed to predicting

---

40 *Ibid* at 51–52.

41 Abeba Taddese, "Saskatchewan, Canada: The Hub Model for Community Safety" (2017), online: *Results for America* <results4america.org> [perma.cc/UR3P-RGA6]; Nathan Munn, "Police in Canada Are Tracking people's 'Negative' Behavior In a 'Risk' Database", *Vice* (27 February 2019), online: <www.vice.com > [perma.cc/SE7C-DDSX].

42 Robertson, Khoo & Song, *supra* note 1 at 51–52.

potential perpetrators in jurisdictions that apply APTs like those developed by Palantir. Robertson and colleague's qualitative research found that SPPAL team members maintain priority on complex issues that can meaningfully be addressed by supporting vulnerable people, helping them be safe and, by extension, improving community safety overall.[43]

This review demonstrates that Canadian police services are adopting different approaches to the implementation of APT in their jurisdictions. With consideration of Robertson and colleague's concerns, the SPPAL approach appears to be the more appropriate model. Data collection and analysis procedures used by global entities like Palantir Technology risk the application of formulae informed by enforcement data from far-away jurisdictions, rather than regional enforcement concerns of local police. The SPPAL model addresses these concerns by restricting APT access to data sets that reflect the behaviour of residents and their responses from local enforcement officials. In a broader sense, internal development of this software can also ensure that backdoor actions, like Palantir's Governance Entity, are not permitted to change output expectations or database access. On this basis, I recommend that Canadian police forces adopt the SPPAL approach, rather than outsourcing APT development to international providers that may latently influence the rights of individuals from the outside.

The concerns raised here are heightened with consideration of their potential to validate police infringements on the *Charter* rights of Canadians. Importantly, the concerns identified in Robertson and colleague's report only relate to the information known about the use of these technologies in Canada. The full extent may never be known, but based on those raised here, action must be taken to address these encroachments. The following section reviews the SCC's authorization of surveillance technologies under common law jurisprudence, which continues to empower investigative encroachment of spaces protected by s. 8 and s. 9 of the *Charter*. It is from this foundation that we consider the true implication of regional APT deployment and its consequences for human rights in Canada.

---

43 "Saskatoon police analytics lab will try to predict crime before it happens", *CBC News* (14 January 2016), online: <www.cbc.ca/news> [perma.cc/E6JV-7MCK]; Meaghan Craig, "Saskatoon police lead the country with Predictive Analytics Lab", *Global News* (15 January 2016), online: <globalnews.ca/news/2455063/saskatoon-police-lead-the-country-with-predictive-analytics-lab/> [perma.cc/2HX2-D8HA]

IV. *CHARTER* PROTECTED RIGHTS AND ANCILLARY EXPANSION OF SURVEILLANCE POWERS

A. Section 8 Protections

To Surveil and Predict provides a comprehensive review of the *Charter* rights that are engaged by APTs. The report considers the deployment of APTs using a human rights perspective to review the consequences of its implementation in different jurisdictions. In the context of privacy rights, Robertson and colleague's analysis concludes that APTs threaten commonly held notions of privacy in very meaningful ways. APT processes were found to engage s. 8 considerations in several processes, including training protocols, generation of formulae, as well as their application in the field. On this basis, their report recommends establishing strong oversight mechanisms to protect against unreasonable extensions of APT capacities, as well as instituting firm limits on how law enforcement agencies can apply APTs in the field to maintain liberties that fall within a "reasonable expectation of privacy."

In Canada, the right to privacy is captured in s. 8 of the *Charter*, which protects individuals against unreasonable search and seizure by actors of the state.[44] The SCC issued a bright-line interpretation of s. 8 protections in *Hunter v Southam*.[45] In that case, Chief Justice Dickson explained s. 8 as protecting an individual's right to privacy from unjustified state intrusions. Its protection applies to people, not places, and establishes a rebuttable presumption that police must secure prior judicial authorization in order to validly conduct a search or seizure. The evidentiary burden is placed on the state to demonstrate the superiority of its interest to those of the individual on the standard of "reasonable and probable" grounds.[46] Failure to meet this expectation means that an impugned search is *prima facie* unreasonable and amounts to a breach of s. 8.

While the bright-line decision of *Hunter v Southam* is strong, the SCC proceeded to delineate a series of legal tests to refine judicial considerations of whether an accused could validly maintain a reasonable expectation of privacy in the circumstances of a search or seizure. In *R v Patrick*, police collected garbage from within the accused's residential property line via

---

44 *Constitution Act, 1982*, s 8, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.

45 *Hunter et al v Southam Inc*, [1984] 2 SCR 145, 11 DLR (4th) 641 [*Hunter*].

46 *Ibid* at 159–62.

aerial trespass. In considering the validity of this act, the SCC provided the governing test used to determine whether Patrick held a reasonable expectation of privacy in his garbage.[47] In conducting this analysis, a court considers the nature of the evidentiary subject matter, as well as whether the accused had a direct interest in its contents, whether the accused held a subjective expectation of privacy in the search's subject matter, whether this subjectively held expectation is reasonable, as well as several contextual factors that compose the "totality of the circumstances." These factors can include whether the subject of the search was in plain view, was abandoned, or was already in the hands of third parties; consideration of whether the investigative techniques in question were intrusive and objectively reasonable; and whether the subject matter of the search exposed any intimate details of the accused's lifestyle or biographical nature. On the facts of Patrick's case, the majority determined that his privacy interest in the garbage was abandoned, meaning that he could not maintain a validly reasonable expectation of privacy (REP). In essence, they concluded that officer recovery of the garbage did not amount to a search.[48] Reviewing previous jurisprudence to justify their conclusion, the majority delineated several stratified REP considerations that are now distinguished between the levels of bodily integrity, the residential territory, and personal information about an individual's behaviour. The bag of garbage was found to fall in the "informational" category, meaning that diminished REP considerations were applied. By abandoning his interest in the information contained in his waste, the police were permitted to reclaim it without activating s. 8 protections.

The SCC's model of informational privacy rights was further refined in *R v TELUS* to diminish REP considerations for investigative requests involving retained user information from corporate service providers, like telecommunications companies.[49] In that case, police requested access to tracked SMS information from two suspects who were TELUS customers. They requested text message history for the previous two weeks, as well as message information for two weeks following their request to monitor the activities of the accused. Justice Abella likened this request to a wiretap, finding that prospective authorization to seize communications before they took place amounted to an interception of communications while they were

---

47 *Patrick*, *supra* note 3.

48 *Ibid* at paras 27–28.

49 *R v TELUS Communications Co*, 2013 SCC 16 [*TELUS*].

happening. On this basis, she concluded that stronger prior authorization is required before police can validly request prospective information about an individual's actions, even if this information will likely be retained by private companies.[50]

Although *TELUS* signified strong *dicta* regarding the preservation of s. 8 protections, the majority proceeded to distinguish investigative requests for information retained for historical tracking purposes in *R v Jones*.[51] Rather than request historical and prospective message information under a production order, the police only requested historical information from the service provider. In the previous case, the majority focused on the issue of collecting prospective messages from the service provider about customers. The majority distinguished Jones' case from *TELUS*, finding that the production order in question failed to activate s. 8 protections because retrieval of historically tracked information did not amount to an intercept, as previously described by Justice Abella. Writing in dissent, Justice Abella blasted the majority's distinction as artificial, highlighting her statements in *TELUS*: the court's focus should be on the "acquisition of informational content and the individual's expectation of privacy at the time the communication was made."[52] Regardless, the majority proceeded to authorize the collection of historically tracked message information from the service provider without amounting to a breach of s. 8.[53]

Like in *TELUS*, the SCC proceeded to establish bright-line s. 8 considerations related to computers and internet access in *R v Spencer*.[54] In that case, the SPS identified the accused as a provider of child pornography on a file-sharing platform in Saskatchewan. Police accessed his share using publicly available software, which allowed police to view the contents of the accused's folders and to confirm his IP address. Police secured the customer's information from Shaw Communications on request, which was used to obtain a warrant that permitted police to search Spencer's computer. In considering whether the search was reasonable, the SCC considered the purpose of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) related to disclosures of personal information. They found *PIPEDA* to imply that internet users can maintain a REP as it

---

50 *Ibid* at paras 25–29.
51 *R v Jones*, 2017 SCC 60 [*Jones*].
52 *TELUS*, *supra* note 49 at paras 25–29.
53 *Jones*, *supra* note 51 at paras 60–65.
54 *Spencer*, *supra* note 2.

relates to the disclosure of personal information. Under this arrangement, the Court found that police did not have the power to request such intimate details from an Internet Service Provider (ISP). The majority rejected Crown arguments that s. 487.014(1) of the *PIPEDA* permits police to secure consent from ISPs, which allows them to collect this information as a form of consent search, rather than securing the appropriate warrant authorizations. The majority concluded that police are only be permitted to secure such digital information based on exigent circumstances, which were not present in the case-at-bar.[55] On this basis, the Court excluded the evidence under s. 24(2) of the *Charter* and exonerated the accused.

In addition to the jurisprudential protections established in bright-line decisions like *Spencer*, the *Privacy Act* also restricts the investigative collection of personal information from corporate and public entities. This *Act* regulates how public and private sector agencies can share semi-public information about individuals between 'trusted' organizations. The Office of the Privacy Commissioner of Canada (OPCC) is empowered to investigate privacy concerns under this *Act* and adjudicate charges levied against breaching organizations. A recent example of this adjudication is a recent consideration of corporate sharing of customer information by Toronto Dominion Bank with third-party service providers in India. OPCC ultimately permitted the exchange but noted that privacy legislation in Canada must be strengthened.[56] Donalee Moulton explains that OPCC's decision is an about-turn from previous decisions to strengthen corporate customer consent requirements. He explains that corporate consultations with the government steered away from positively requiring consumer consent before internal information could be shared with international third parties.[57] The departed-from decision may have resulted from OPCBC's conclusion that the use of facial recognition technology and driver's licence photographs by law enforcement amounted to a breach of provincial privacy legislation. In that case, the OPCBC ruled that BC's public automotive insurer was not permitted to use its databases for

---

55 *Ibid* at paras 38–40, 54–58.

56 Office of the Privacy Commissioner of Canada, *Bank Ensures Openness and Comparable Protection for Personal Information Transferred to Third Party* (Report), No 2020-001 (Ottawa: PCC, 4 August 2020), online: <www.priv.gc.ca> [perma.cc/6Q2C-3NCN].

57 Donalee Mouton, "Privacy commissioner reaffirms original position on transborder transfer of data", *Lawyer's Daily* (2 September 2020), online: <www.thelawyersdaily.ca>.

purposes not disclosed to its customers.[58] Be that as it may, Moulton confirms that OPCC has restored the status quo. In writing, he notes that positivistic consumer consent requirements are antithetical to international business practices and hold negative potential for competitiveness for Canadian financial organizations, among others. While his comments are focused on financial markets, the jurisprudence of partner nations highlights an international trend towards expanding access to ISP records and personal account information.

Although outside of Canada, recent American jurisprudence may influence future consideration of the limits defined in *Spencer*. US District Courts are hearing cases against Facebook and Google for violations of consumer privacy related to user profiles.[59] These organizations were previously permitted to share user information with law enforcement agencies around the world, so long as they complied with local law enforcement laws and regulations. In the Canadian jurisdiction, the *PIPEDA* is the governing legislation that requires consumer consent to share corporate user information with others, particularly state agents. Under this legislation and its provincial counterparts, private corporations are only permitted to share information with law enforcement without consumer consent when they have "lawful authority" to do so. "Lawful authority" is determined using the REP analysis described here.[60] Like other comparable jurisdictions, American privacy advocates are mobilizing against these quasi-monopolistic data giants. While inconclusive at the time of writing, these cases are worthy of attention in the future.

Based on this jurisprudence, it is clear that privacy is a fundamental right in Canada. While that is the case, SCC jurisprudence delineates instances where police conduct does <u>not</u> amount to a search. S. 8 protects people, not places, meaning that an individual may fail to maintain a valid REP in the relevant context. By failing to activate s. 8 protections, an individual cannot reasonably expect privacy from state actors. Alternatively, this means that an individual must come to expect state examination in

---

58 Office of the Information & Privacy Commissioner of British Columbia, *Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia* (Report), No F12-01 (BC: IPCBC, 16 February 2012) at para 96, online: <www.oipc.bc.ca/investigation-reports/1245> [perma.cc/4EN8-LQKZ].

59 *In re Facebook, Inc, Consumer Privacy User Profile Litig,* 402 F Supp 3d 767; *Brown et al v Google LLC et al*, U.S. District Court No 20-03664.

60 *Spencer*, *supra* note 2 at paras 60–66; *Personal Information Protection and Electronic Documents Act*, RSC 2000, c 5, s 7(3)(c.1).

circumstances where a REP cannot be maintained. In addition to this, a REP may be abandoned or diminished in relation to the stratified REP level that applies in the investigative context. Privacy expectations are often diminished in relation to computer use and information accessed via the internet but continue to provide meaningful protection against digital state surveillance. While it is clear that a REP can maintain valid protection for individuals who make use of ISP offerings, the law also allows police to access private information normally protected by s. 8 by securing prior judicial authorization in the form of a warrant. From this foundation, the following section considers whether APT use can fall within the scope of currently authorized police powers or if they alternatively constitute a breach of s. 8 *Charter* protections.

B. APT's Relationship to Section 8 Rights

APTs engage the private information of individuals in several stages to generate sufficient output information. First, APTs collect private information from databases to generate pattern formulae. This information is consolidated and processed to generate inferential outputs. Results may be shared between law enforcement agencies, other governmental bodies, or with private sector actors under contract. These outputs are applied to real-time police decision-making to optimize resource allocation and the overall performance of duties. In addition to using APT outputs in frontline enforcement decisions, government reports indicate an interest in applying algorithmic technologies to augment decision-making in broader criminal justice processes, such as granting bail, generating sentence recommendations, establishing an accused's risk to re-offend, and determining parole eligibility.[61] The following outlines the various stages where APT is applied in Canadian justice and its potential to infringe on the privacy rights enshrined in s. 8 of the *Charter*.

1. Data Collection, Accuracy Concerns and Data Processing

A key question raised in *Jones* is whether the pre-emptive collection of data to forecast potential crime or gather disparate personal information generally is either necessary or proportionate to its infringement on s. 8

---

61 "The Rise and Fall of AI and Algorithms in American Criminal Justice: Lessons for Canada" (October 2020) at 3–9, online (pdf): *Law Commission of Ontario* <www.lco-cdo.org/wp-content/uploads/2020/10/Criminal-AI-Paper-Executive-Summary-Final-Oct-28-2020.pdf> [perma.cc/9FVQ-MJWD].

privacy rights.[62] *Hunter v Southam* generally requires that, whenever state agents intrude on protected spheres of privacy, they must have reasonable grounds to believe the collected information will reveal evidence of a crime. Related to internet use, the *Spencer* jurisprudence explains that some degree of anonymity is a known feature of internet activity, which forms a key priority that grounds the requirement for police to secure a warrant before obtaining access to IP subscriber information from ISPs.[63] Individuals often have limited knowledge about the scope of their electronic footprint and may be even less aware of the ways their anonymity can be defeated through technological means.[64] APTs often rely on the collection, collation, and analysis of massive data sets that include personal information, communications, biometrics, geolocations and, social media information. Enforcement agencies also routinely collect information from online and 'real' environments that are considered public, or not protected by privacy law. While these claims are technically valid in Canada, Robertson and colleagues note that these assertions are somewhat baseless because there is no technology-specific law that either permits or prevents this type of data collection by police.[65]

In opposition to the claims of Canadian police regarding APT, Robertson and colleagues highlight a series of SCC statements regarding informational privacy. In the context of investigative requests for access to historical information retained by corporate third parties, the SCC explained that:

> The right to retain protection for information that has already been shared with third parties for limited purposes flows from the fact that "all information about a person is in a fundamental way [their] own, for [them] to communicate or retain for [themselves] as [they see] fit.[66]

The majority later confirmed this perspective, concluding that:

> While individuals do inevitably lose some degree of control over their personal information when it is shared with others, they may reasonably expect that the information will not be divulged further to (or collected by) law enforcement."[67]

---

62 *Jones*, *supra* note 51 at para 74.
63 *Spencer*, *supra* note 2 at para 48.
64 Robertson, Khoo & Song, *supra* note 1 at 77.
65 *Ibid* at 75–77.
66 *Spencer*, *supra* note 2 at para 40.
67 *R v Cole*, 2012 SCC 3; *R v Marakah*, 2017 SCC 59; *Jones*, *supra* note 51.

The SCC also specifically raised concerns about using surveillance technologies to fish for prospective criminals: "[l]aw enforcement usage of sophisticated surveillance technologies "for forward-looking 'fishing expedition[s],' in the hope of uncovering evidence of crime… is untenable."[68] These statements underscore the SCC's understanding of the threats present by digital surveillance technologies in relation to s. 8 privacy rights and the principles the section is intended to protect. Unfortunately, the SCC has yet to formally consider the use of APT as part of the digital surveillance array and its potential to refine the "forward-looking fishing expeditions" that will undoubtedly form an expanding basis of future investigations.

The concerns highlighted here do not include criticisms of mass data collection, collation, and analysis by APTs. While currently unconsidered in the Canadian common law, Robertson and colleagues raise particular concern about expressed intentions from APT proponents to expand database access to include social media information sourced from corporate leaders like Facebook and Google. While a nominal impact at the individual level, systematic collection of personal information at a macro-scale paired with algorithmic analysis to detect behavioural patterns holds significant privacy implications.[69] Robertson and colleagues articulated this concern aptly:

> The aggregation and algorithmic analysis of data can potentially reveal a detailed picture about individuals that they may not expect to exist, let alone expect to be in the possession of the government. Indeed, it is the creation of this more detailed portrait of an individual's private life that provides the reason for algorithmic surveillance-based tools – they collect and reveal information that is otherwise unavailable to law enforcement.[70]

Canadian users of PFAPTs have expressed interest in expanding their access to private social media data to support Social Network Analysis functions. APT software can systemically mine social media accounts for personal information and apply it to inform future police interventions or deployments of police resources. The RCMP has indicated an interest in using online social media surveillance because this information, in their

---

68 *Jones*, *supra* note 51 at para 74.

69 *R v Rogers Communications*, 2016 ONSC 70 at para 19 [*Rogers*].

70 UN Human Rights Council, *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*, UNHRC, UN Doc A/HRC/27/37 (2014) at para 19, online: <undocs.org/A/HRC/27/37>; Robertson, Khoo & Song, *supra* note 1 at 76.

view, is sourced from an open or public source.[71] SPPAL also expressed interest in expanding APT access to local social media accounts.[72] Opposed to this perspective, Robertson and colleagues cite *Spencer* to highlight that individuals do not expect that their personal information will be systemically collected by law enforcement when consenting to use social media platforms.[73] In addition, the collected information reveals detailed information about a user's personal life, relationships, and daily activities, which surely do not qualify as a reasonable search under the *Patrick* criteria. Individuals may be aware that social media profiles are public, but it would not be reasonable to expect individuals to know that police are systematically watching every online act.

The use of APT in this fashion is already concerning but presents a heightened risk when considering data accuracy concerns. As described above, historical enforcement information is likely ripe with enforcement biases inherent to police reporting. While inaccurate in its own right, the expansion of APT access to social media accounts is especially concerning because of the nature of information users post and share. As the home of "fake news," the information sourced on social media platforms is well known for its inaccuracy, as well as user misrepresentations to 'present well' to a quasi-public audience.[74] To this end, the Saskatchewan Information and Privacy Commissioner (SIPC) concluded that social media information should not be applied by APTs, or by public bodies generally, because they are notorious sources of inaccurate information.

Algorithms cannot distinguish the contextual considerations involved with social media information, which may inadvertently trigger police

---

71 Nathan Munn, "Canadian Cops Will Scan Social Media to Predict Who Could Go Missing", *VICE* (17 April 2019), online: <www.vice.com> [perma.cc/9G45-WR8V]; Bryan Carney, "'Project Wide Awake': How the RCMP Watches You on Social Media", *The Tyee* (25 March 2019), online: <thetyee.ca/News/2019/03/25/Project-Wide-Awake/> [perma.cc/42QN-N2JK]; Catherine Tunny, "RCMP launches review of its social media monitoring operation", *CBC News* (5 November 2019), online: <www.cbc.ca> [perma.cc/HQ5U-9EC7].

72 Robertson, Khoo & Wong, *supra* note 1 at 51.

73 *Spencer*, *supra* note 2 at paras 38–50; *R v Wise*, [1992] 1 SCR 527, 11 CR (4th) 253; Robertson, Khoo & Wong, *supra* note 1 at 77.

74 Kai Shu et al, "Fake News Detection on Social Media: A Data Mining Perspective" (September 2017), online: *Association of Computing Machinery Digital Library* <dl.acm.org/doi/10.1145/3137597.3137600> [perma.cc/LHE6-Q3H2]; Harry T. Dyer, *Designing the Social: Unpacking Social Media Design and Identity*, 1st ed (Norwich, UK: Springer Nature, 2020).

intervention.[75] Private vendors are generally obliged to take reasonable steps to ensure the accuracy of personal information that is provided to the police.[76] While that is the case, some Canadian provinces exempt data accuracy obligations for the collection of personal data for law enforcement purposes.[77] Data accuracy concerns related to surveillance technologies have yet to be formally considered by the SCC, but the Ontario Court of Justice explained that reliance on inaccurate information risks constitutional inconsistency: an "arrest based on a source, the reliability of which in the end is unknown, cannot be said to be objectively reasonable."[78] Robertson and colleagues share the concerns of the SIPC: "Law enforcement agencies' reliance on error-tainted algorithmic forecasts would risk unjustifiable interferences with *Charter*-protected interests such as privacy or liberty, if law enforcement authorities act on those algorithmic predictions."[79] The SCC confirms these statements, concluding that state actors are expected to take all reasonable steps to ensure that data retained about offenders is up to date, accurate, and as complete as possible.[80] Be that as it may, government databases regularly fall short of this standard, meaning that further action is required.

Concerns related to APT data collection are alarming, but the most serious threat to *Charter* rights held in the generation of output data that is used to supplement investigative decision-making regarding officer interference with individual liberties. The fragmented information collected about individuals, as well as general trends about their identities, movements, and beliefs, are all examined as part of APT data analytics. Outputs generated from these data are used to draw inferences about a target's private life. APT data analysis takes this a step further by including metadata as part of its examination. Metadata consists of information about the information captured in the data log, like time, location, date, as well as

---

75 *Community Mobilization Prince Albert (Re)*, 2014 CanLII 81867 at para 32–38 (SK IPC); Jordan Pearson, "Researchers Claim AI Can Identify Gang Members on Twitter", *VICE* (1 November 2016), online: <www.vice.com/en_us/article/mg7kgx/researchers-claim-ai-can-identify-gang-members-on-twitter> [perma.cc/8VJ7-XXCH].

76 *Privacy Act*, RSC 1985, c P-21, s 6(1); *Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25, s 35.

77 *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F 31, s 40(3); *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c M 56, s 30(3).

78 *R v White*, 2006 ONCJ 147 at para 27–28.

79 Robertson, Khoo & Song, *supra* note 1 at 87.

80 *Ewert v Canada*, 2018 SCC 30 at 3.

the identity of the sender or the recipient.[81] In essence, it appears that algorithmic collection of information sourced from third parties can extend investigative powers beyond the limits that prevent police from collecting such data directly.[82]

In cautioning readers against APT's prospectively serious breaches of privacy rights, Robertson and colleagues take this a step further to argue that APT data processing and its application in the field amounts to a breach of the right to equality before the law, as captured in s. 15 of the *Charter*.[83] While outside the scope of our discussion here, Robertson and colleagues argue that the use of macro-scale data collection, aggregation, and analysis to detect patterns based on protected characteristics like race, religious belief, age, gender, and sexual orientation hold serious deleterious potential for the equality rights of Canadians. Generating recommendation outputs based on granular information about individuals suggests that a system of constitutionally questionable generalizations is being employed to police these populations, even if target recommendations are issued on a case-by-case basis. While these considerations are outside the scope of this discussion, it is important to note the broader risks that may be associated with APTs.

The risks of applying this potentially tainted data in the field are compounded by flaws that are inherent to the equipment used to collect environmental information in real time. Technologies like facial recognition software (FRT) can rapidly compare templated snapshots of individuals in public against databased information to determine if intervention is required. New inputs may become tainted by the flaws inherent to the template formation process.[84] Recent FRT research explains that these technologies are unreliable, particularly in the case of racialized individuals and women.[85] FRTs are more likely to misidentify these groups,

---

81 *Spencer*, *supra* note 2.

82 *R v Reeves*, 2018 SCC 56 [*Reeves*].

83 *Constitution Act*, *supra* note 44, s 15.

84 Iliana V. Voynichka & Dalila B. Megherbi, "Analysis of the Effects of Image Transformation, Template Selection, and Partial Information on Face Recognition with Time-Varying Expressions for Homeland Security Applications" (April 2014), online: *Homeland Security Affairs* <www.hsaj.org/articles/256> [perma.cc/H7GQ-MK4F].

85 Danielle Groen, "How We Made AI as Racist and Sexist as Humans" (12 November 2019), online: *The Walrus* <thewalrus.ca> [perma.cc/S8X2-QAVC]; Steve Lohr, "Facial

with highly varied rates in poor environmental conditions. The misidentification rates can be shocking: a 2018 report notes that FRT products from NEC Corporation produced inaccurate matches in 91–98% of cases studied by the UK Metropolitan Police and South Wales Police.[86] Notably, NEC Corporation is the choice APT hardware provider for police services in Calgary and Toronto.[87]

Considering the serious implications of APT at the data collection and analysis phases, along with the constitutional risks of applying its outputs in the field, the following section analyzes APT's relationship to the right against arbitrary detention, as stipulated in s. 9 of the *Charter*.

C. Section 9 Protections

S. 9 of the *Charter* protects Canadians from arbitrary detention by police.[88] Be that as it may, police have become empowered to engage in investigative detentions under SCC jurisprudence. The SCC established a jurisprudential test to craft investigative powers under the framework described in the UK.[89] In *R v Dedman*, the accused refused to participate in a breathalyzer test at a sobriety check stop. In considering whether the police were acting within their powers in detaining Dedman, the majority failed to find legislative authorization for the conduct of the police. Regardless, they proceeded to authorize investigative detentions related to an officer's execution of their duty to control traffic. This decision received the ancillary powers doctrine into the Canadian common law and has since been applied to authorize several investigative powers that remain without governing legislation. Notable examples include powers to use sniffer dogs in certain

---

Recognition Is Accurate, if You're a White Guy", *The New York Times* (9 February 2018), online: <www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html> [perma.cc/ANS2-LFVR].

86 "Face Off: The lawless growth of facial recognition in UK policing" (May 2018) at 3–4, 6, online (pdf): *Big Brother Watch* <bigbrotherwatch.org>.

87 Robertson, Khoo & Song, *supra* note 1 at 62; Kate Allen & Wendy Gillis, "Toronto police have been using facial recognition technology for more than a year", *Toronto Star* (28 May 2019), online: <www.thestar.com/news/gta/2019/05/28/toronto-police-chief-releases-report-on-use-of-facial-recognition-technology.html?rf> [perma.cc/5UGP-6MT2].

88 *Constitution Act*, *supra* note 44, s 9.

89 *Dedman v the Queen*, [1985] 2 SCR 2 at paras 35–36, 20 DLR (4th) 321 [*Dedman*].

contexts,[90] as well as to enter a private residence when an officer perceives a safety risk to investigators or the public.[91]

Formal common law powers of investigative detention were established using the imported ancillary powers doctrine from the *Dedman* decision. Using this doctrine, the SCC first defined powers of investigative detention in *R v Simpson*.[92] In that case, the arresting officer directed the accused to pull over after leaving a known drug den on suspicion of criminal activity. The officer conducted a safety search of the accused during what is now known as investigative detention and proceeded to recover drug evidence. While finding the detention unlawful, the SCC applied the *Waterfield* test to consider whether the detention was authorized by law, as an extension of 'unknown' police powers that exist while officers execute their duties. Thus, the framework of investigative detention was established in Canadian common law. Shortly thereafter, this framework was successfully applied in *R v Mann*.[93]

The SCC later noted that investigative detention requires an officer to hold a 'reasonable suspicion' that criminal activity may take place in order to engage an investigative detention in *R v Chehil*.[94] The majority defined the standard to engage an investigative detention as an officer's subjectively held belief that detecting criminal activity is possible, not the probability of actually uncovering it. In Chehil's case, the accused exhibited common behaviours associated with drug traffickers at the Vancouver International Airport, which piqued the arresting investigator's suspicion of criminal activity. Sniffer dogs confirmed that narcotics were in his bags before he received them. The accused was arrested once he collected his bags. The SCC rejected the accused's challenge to the constitutionality of the search and alternatively confirmed that a latent investigative power existed for police to use sniffer dogs to supplement their search capabilities. This conclusion was reached with consideration of the current jurisprudence, the constellation of facts in Chehil's case, and totality of the circumstances.[95]

Although continuing to authorize investigative detentions under the ancillary powers doctrine, the SCC has taken judicial notice of how this

---

90 *KB*, *supra* note 4 at paras 80–97.

91 *R v MacDonald*, 2014 SCC 3 at paras 37–41 [*MacDonald*].

92 *R v Simpson*, [1993] OJ No 308, 12 OR (3d) 182 [*Simpson*].

93 *R v Mann*, 2004 SCC 52 at para 28–40 [*Mann*].

94 *R v Chehil*, 2013 SCC 49 [*Chehil*].

95 *Ibid* at paras 28–41.

investigative tool is routinely abused by police, with particular focus on people of colour. In *R v Grant*, the SCC considered the role of racial bias in forming the 'reasonable suspicion' used by officers to justify intervention with a young black man walking down the sidewalk. Two plain-clothes officers identified the youth as 'suspicious' and worthy of intervention. They directed a nearby uniformed officer to intercept the young man. While doing so, the plain-clothes officers enclosed Grant on the sidewalk. On identification as officers, the youth disclosed that he had a small sample of weed and a firearm. In considering Grant's case, the SCC reframed the jurisprudential test for determining if an investigative detention occurred, whether physical or psychological.

Psychological detention is established either where (1) the individual has a legal obligation to comply with a restrictive request or demand from an authority or (2) a reasonable person would conclude, on the basis of presented state conduct, that they were obliged to comply. Three factors are considered when determining whether a reasonable person would conclude they were detained: the circumstances of the encounter, the nature of police conduct, and the particular characteristics or circumstances of the individual where relevant, including age, physical stature, minority status, or level of sophistication.[96] While using the language of minority status, this test focused on the role of race in law enforcement practices. The Court affirmed that Grant was detained and attending officers failed to provide him with his entitlement to retain legal counsel, as defined in s. 10(b) of the *Charter*. While finding numerous breaches in Grant's case, the SCC proceeded to define a new test for admission of evidence under s. 24(2) of the *Charter*, which was applied to maintain partial conviction for the accused.

While the amendments stipulated in *Grant* were intended to address the prevalent influence of racial bias towards engaging investigative detentions, the SCC was forced to further refine its *dicta* on this issue in *R v Le*. In that case, officers aggressively approached five suspects while they conversed in a member's townhouse yard.[97] On their aggressive entry to the property, officers immediately started questioning the group while another officer stepped over the fence to inform the primary accused to keep his hands in plain view. Le attempted to inform the officers that he did not have identification on his person, but an officer interrupted with demands

---

96 *Grant*, *supra* note 27 at para 44.

97 *Le*, *supra* note 27.

to see the contents of a bag in the yard. The accused fled after this request. Once arrested, he was found to have drugs, cash, and a firearm in the bag. Of note, the group in the yard included the Asian accused and four other Black males. The SCC confirmed the unconstitutionality of the search and the detention. In doing so, the majority explained the circumstances of the encounter must be considered from the subjective perspective of the accused, who does not possess the knowledge of officers at the time of detention. Importantly, they explained that characteristics of the accused are considered at the standard of a reasonable person of similar racial background, with particular consideration of the social and historical context of that community's relationship with the police. The Court confirmed that more frequent interactions with police do not amount to sophistication but should rather be a consideration of an accused's understanding overall.[98] Once detention has been established under these criteria, a trier of fact will then consider if the detention was reasonable under the remaining *Collins* criteria: Was the authorizing law reasonable? Was the manner of the detention reasonable?

Since the recognition of investigative detention powers under the common law, the SCC continues to revisit its boundaries because of ongoing enforcement practices that are rooted in racial prejudice. James Stribopoulos explains that, from the beginning, intuitive assessments based on age, sex, socio-economic status, or race act as a foundation for investigative detentions. Courts are not exposed to the realities of its use on the frontline, where detentions may be applied to justify interference with vulnerable individuals in marginalized social spaces.[99] Although the court has a limited understanding of the frequency and realities involved with frontline investigative detention, a broader recording of its use is likely a part of internal reporting protocols for police. The aforementioned indicates that race continues to permeate the investigative processes of police. The SCC continues to reshape the scope of these powers to minimize its use against marginalized populations, but the trend of the jurisprudence reviewed here demonstrates the operation of racial bias at a systemic level.

---

98 *Ibid* at paras 37, 63–78, 90, 96–97, 106–10.

99 James Stribopoulos, "A Failed Experiment? Investigative Detention: Ten Years Later" (2003) 41:2 Atla L Rev at 341–44; James Stribopoulos, "The Forgotten Right: Section 9 of the Charter, Its Purpose and Meaning" (2008) 40 SCLR (2d) at 211.

Canadian governments recognized the serious implications of cognitive bias and "tunnel vision" in law enforcement as part of several inquiry reports into wrongful convictions. Bruce MacFarlane is a leader in these areas, whose work continues to ground contemporary government research into the prevalence of cognitive bias in the decision-making of law enforcement officials.[100] He defines cognitive bias as a psychological process that causes an individual to unconsciously select the information that supports already-formed conclusions and to methodologically disregard alternatives.[101] Biases can become layered between investigators or transferred to prosecutors through information sharing.[102] Inquiry reports found that cognitive biases can often crystallize into "tunnel vision," which can drive entire investigative teams to focus on a particular theory of a case and dismisses contrary evidence. MacFarlane also explains that representatives of the Crown may fall subject to "noble cause corruption," where moral intentions to uphold the principle of law can lead criminal justice actors to engage in unethical activities to achieve their objectives.[103] Virtually every inquiry into wrongful convictions in Canada cites MacFarlane's work, with the most recent recognition from the Public Prosecution Service of Canada.[104] Considering the SCC's decisions in *Grant* and *Le*, it is clear that the concerns highlighted in federal and provincial reports related to cognitive bias and tunnel vision continue to influence the on-the-spot decision-making of police officers.

---

100 Bruce A. MacFarlane, *Wrongful Convictions: The Effect of Tunnel Vision and Predisposing Circumstances in the Criminal Justice System* (Ontario: Ministry of the Attorney General: 2008), online: <www.attorneygeneral.jus.gov> [perma.cc/WF8V-ASR5] [MacFarlane, *Tunnel Vision*]; Bruce A. Macfarlane, "Wrongful Convictions: Determining Culpability When the Sand Keeps Shifting" (2014) 47:2 UBC L Rev 597 at 597 [MacFarlane, "Shifting Sands"]; Bruce A. MacFarlane, "Convicting the Innocent: A Triple Failure of the Justice System" (2006) 31:3 Man LJ 403 at 403.

101 MacFarlane, *Tunnel Vision*, *supra* note 99; MacFarlane, "Shifting Sands", *supra* note 99; Keith A. Findley, "Tunnel Vision" in Bryan Cutler, ed, *Conviction of the Innocent: Lessons from Psychological Research*, 2nd ed (Washington, DC: APA Press, 2010).

102 Keith A. Findley & Michael S. Scott, "The Multiple Dimensions of Tunnel Vision in Criminal Cases" (2006) Wis Law Rev 291 at 309.

103 MacFarlane, *Tunnel Vision*, *supra* note 99 at 20–26; "Lawyer defends use of informant in Sophonow inquiry", *CBC News* (8 May 2001), online: <www.cbc.ca> [perma.cc/TJD 5-7FPM].

104 *Innocence at Stake: The Need for Continued Vigilance to Prevent Wrongful Convictions in Canada* (Ottawa: Public Prosecution Service of Canada, 2019) at ch 2, online: <www.ppsc-sppc.gc.ca/eng/pub/is-ip/ch2.html> [perma.cc/D7BZ-V9PV].

This type of historical information is used to train APT. Once trained, the software generates formulas that are applied to new inputs to match targets against its database. Robertson and colleagues explain that the application of APT formula in the field is really an application of generalized inferences to determine whether police should intervene with an individual. The SCC previously explained that a reasonable suspicion could not rely on generalized suspicions in *R v Kang-Brown*.[105] Building on MacFarlane's description of cognitive bias, the use of APT to support the reasonable suspicion necessary to justify investigative detentions risks the amplification of already-existing biases and applying them at an exponential level in the field. Robertson and colleagues state:

> Relying on algorithmic policing technologies as grounds for suspicion may violate section 9 where the algorithmic prediction(s) are based on statistical trends, as opposed to being particularized to a specific individual. Officers may subconsciously rely on a risk prediction generated by an algorithm to form grounds for suspicion that they consider to be "reasonable", even if the suspect's actions have not changed. Rather than identifying meaningful interventions, APT outputs could instead be used to justify officer interventions that support already formed suspicions that may be unconstitutional. Algorithmic predictions may thus result in detentions that are rooted in generalized suspicions that are based on tools with questionable reliability in its output information.[106]

In a broader sense, APTs are highly susceptible to building unconscious biases into their outputs as a function of their training data, as well as the humans that develop the technology and the individuals that apply its recommendations in the field. By providing 'black-box' outputs that can be used to reinforce and justify pre-conceived decisions about an individual's 'suspicious' behaviour, APTs risk perpetuating these biases at an exponential level. Robertson and colleagues note that current research into the use of algorithmic technologies recognizes the tendency of humans to rely on the judgements of automated decisions as superior to their own, even when they have reason to believe the technology is flawed.[107] "Automation bias" may be an appropriate addition to Macfarlane's

---

105 *KB*, *supra* note 4 at paras 68–79.

106 Robertson, Khoo & Song, *supra* note 1 at 111–13; Andrew Guthrie Ferguson, "Predictive Policing and Reasonable Suspicion" (2013) 62:2 Emory LJ 259 at 259.

107 Robertson, Khoo & Song, *supra* note 1 at 124–25; Lindsey Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border" (2017) 41:3 NYU Rev L & Soc Change 327 at 342–43, online: *NYU Social Change* <https://socialchangenyu.com/wp-content/uploads/2017/09/barrett_digital_9-6-17.pdf> [perma.cc/H9EQ-7V4L].

characterization of cognitive bias in Canadian law enforcement. Robertson and colleagues confirm that reliance on algorithmic tools that generate predictions on the basis of immutable individual characteristics will result in biased decisions against particular groups.[108] The *Le* jurisprudence confirms that violations of the right against arbitrary detention are often significant and humiliating experiences that strike at the core of individual dignity.[109] In terms of race, being subjected to increased police scrutiny, higher-stop rates, and use of detention can compound the already-negative experiences of some racialized community members.

Considering the serious risks to *Charter* rights against arbitrary detention, Robertson and colleagues caution that stronger public education in digital literacy and targeted training for officers is essential to prevent cognitive biases from becoming justified detentions under the authorization of APT outputs:

> Without establishing effective training, technological literacy, cultural competence, and related best practices throughout all law enforcement agencies across the country, individuals remain at an elevated risk of having their section 9 rights violated by way of automation bias and other biases in algorithmic policing. Clear written policies, directives, and meaningful accountability mechanisms are recommended.[110]

V. Issues with Ancillary Expansion of Investigative Powers

It is clear from this discussion that police investigative powers hold serious potential to infringe *Charter* protected rights. Considering this, it is surprising that investigative powers continue to fall outside the scope of statutorily defined powers. Rather than legislating police powers to conduct investigations in line with the constitutional roles of the legislatures and the courts, investigative powers continue to proliferate under the SCC's ancillary powers doctrine. Richard Jochelson explains that, although the Court has engaged in this practice with increasing frequency since terror attacks against the United States on 9/11, expanding police powers continues to fall outside of the courts' traditional role as guardians of the constitution.[111] Our

---

108 *Chehil*, *supra* note 94 at para 43.

109 *Le*, *supra* note 27 at para 95

110 Robertson, Khoo & Song, *supra* note 1 at 125–26.

111 Jochelson, *supra* note 5 at 355–76.

Parliamentary democracy designates legislators with the responsibility to craft laws that limit the liberty of Canadians. Alternatively, it is the role of courts to determine whether government legislation is constitutionally consistent to ensure that enacted laws respect their natural boundaries.

Opposed to the *Waterfield* test described above, Jochelson explains that it is more appropriate for the court to apply the common law *Oakes* test to determine whether the government can justify breaches or encroachments of individual rights, rather than authorizing state infringements on the bench. The Crown bears the burden of demonstrating that a proposed law addresses social harms in a proportion greater than the content of the rights being infringed. If there is a failure to do so, the court is empowered to strike legislation down or permit the government to reshape the law, within a reasonable time, to conform with its constitutional limits. When considering the use of police investigative powers, the court continues to be faced with an absence of governing legislation for surveillance tools. Rather than demanding a legislative framework for constitutional validation, SCC jurisprudence continues to unilaterally authorize the use of surveillant technologies under the ancillary powers doctrine. Jochelson describes this test as an inversion of the logic defined in *Oakes*, where the court can instead authorize constitutionally questionable police conduct when finding a sufficient nexus with existing common law duties for police. He argues that the ancillary powers doctrine forms the basis of a security calculus that is intended to enforce national security objectives, which is being applied beyond the interpretive purpose of the court and into the role of the legislature.[112]

Jochelson compares the structure of the *Waterfield* test to the *Oakes* test to illustrate this inversion. In highlighting the resemblance of these tests, he explains that *Oakes* is a two-prong approach, where the second prong includes three supplementary considerations. The Crown must first demonstrate the impugned legislation's sufficiently pressing and substantial purpose to justify a restriction of liberty. The second stage considers whether the law's effect is rationally connected to its objective, whether its impairment of rights is minimal, and whether the law's effect is proportional in relation to its objective. This final stage accounts for the

---

112 *Ibid* at 357–58.

importance of the legislative objective, which is balanced against the impugned law's salutary benefits and deleterious effects.[113]

The *Waterfield* test follows a similar track, where the court identifies whether the impugned police conduct is reasonably related to a valid common law power, like controlling traffic or maintaining public safety. Based on the court's analysis, the trier of fact will determine whether the importance of the police conduct, in line with their common-law duties, can reasonably justify their execution of that power to meet the duties that arose in the case-at-bar. Jochelson finds the second prong of the *Waterfield* analysis to be consistent with the second stage of *Oakes*, where a trier of fact considers whether the impugned power is a sufficiently tailored response to the suspected activity in question. He notes that rational connection considerations are often met with descriptions of police responsiveness on a standard of reasonability. In addition, the court often considers the nature of the accused's conduct in determining whether investigative methods, including applications of force, are minimally intrusive to the rights of the accused. Finally, the court considers the totality of the circumstances, which Jochelson likens to the cost-benefit analysis of the *Oakes* test. The court applies a contextual consideration of the circumstances at the time of detaining the accused to determine whether the cost of rights infringement outweighs the benefits provided by upholding the law.[114] Jochelson notes the adamant opposition of dissenting SCC justices to expand investigative powers under the *Waterfield* test to demonstrate the inappropriate nature of this test. Dissenting judges went so far as to argue that the ancillary powers doctrine risks replacing *Oakes* for a watered-down test for *Charter* scrutiny that can allow expansive growth of police investigative powers.[115]

Considering the constitutional role of the judicature, I agree with Jochelson's assertion that the *Oakes* test is a more appropriate jurisprudential tool than the *Waterfield* criteria. *Oakes* is applied in response to the legislative acts of Parliament: when a right is infringed, the court determines whether the law's encroachment is justified under s. 1 of the *Charter*. Where *Waterfield* is applied, there is no legislative

---

113 *R v Oakes*, [1986] 1 SCR 103 at paras 40–49, 62–71, 53 OR (2d) 719 [*Oakes*]; Jochelson, *supra* note 5 at 365–67.

114 *Dedman*, *supra* note 89 at paras 22–23, 68–69; Jochelson, *supra* note 5 at 367–69.

115 *R v Orbanski*, 2005 SCC 37 at para 81; *KB*, *supra* note 4 at paras 50–57.

authority for the state to act. This is particularly troubling because the ancillary powers doctrine is not authorized by law but is instead a judicial usurpation of the legislative role of Parliament. Jochelson notes that using this test is a betrayal of the common law's traditional role of protecting liberties from the tyranny of majorities. Rather, the removal of liberties is the constitutional responsibility of Parliament.[116]

The SCC proceeded to expand investigative powers using the ancillary powers doctrine under the auspices of dialogue theory. They claim that law-making is a discursive process, where legislators and judges exchange perspectives on the status of the law through the passage of legislation and its constitutional verification in court. Jochelson acknowledges the role of dialogue theory but draws attention to its illogical application in the context of ancillary expansions of police powers. He explains that, rather than dialogue, the use of powers in this way amounts to a judicial monologue where the court can unilaterally invent common law powers and simultaneously declare them constitutional. In addition to undermining the structure of our democracy, the expansion of ancillary powers is exceptionally concerning when considering its implications for an unsuspecting accused. Unilateral expansion of police powers without governing legislation implies that an accused, due to issues with intelligibility and unpredictable discretionary choices of police, may never know the full extent of the investigative search and detention powers available to police until appearing in court.

Our discussion reviewed the use of the ancillary powers doctrine to authorize the use of surveillance technologies like heat scans and sniffer dogs. Considering the trend of this jurisprudence, Jochelson's concerns regarding the *Waterfield* test, and the extreme risk to individual liberties presented by the macro-scale implementation of APTs, the author demands strong legislative action to delineate the boundaries of police investigative powers. In particular, I recommend the enactment of a dedicated statutory framework that defines the use of surveillant technologies by police, with a particular focus on delineating the permissible scope of APT use. Robertson and colleague's research highlights the imperative nature of enacting APT-related legislation and provides a policy framework that can jump-start a governmental response to better protect the rights of individuals. In addition to upholding the constitutional limits of law-making in Canada,

---

[116] Jochelson, *supra* note 5 at 370–74.

the implementation of governing legislation can also allow the court to resume its traditional role of validating the constitutionality of Parliament's laws. The following section reviews government's current knowledge of APT use in Canada, their expressed intention to expand data access, and Robertson and colleague's recommendations to implement a Canadian governance regime for APTs.

VI. APT Legislation is Required

The above sections of this essay described the implementation of APT in Canada and its potential to infringe *Charter* protected rights. The roll-out of these programs has been facilitated by regional police forces, provincial police services, as well as Canada's federal law enforcement agencies. All agencies operate as a function of government and some serve as a direct extension of provincial or federal Ministries of Justice. For example, SPPAL is a joint partnership between the Government of Saskatchewan, the Saskatoon Police Service, and the University of Saskatchewan. While connected to the development and application of APTs, Canadian governments have been reluctant to legislate, or even acknowledge, the implications of algorithmic decision-assistance on the *Charter* rights of Canadians. It is clear that government officials are comfortable with the expansion of these technologies in law enforcement, but action must be taken to balance the encroachments that are taking place with companion legislation to demarcate the acceptable boundaries of its use.

Although reluctant to legislate, the Government of Canada has recently expressed intention to expand public access to more detailed data that is already captured in historical law enforcement records. In 2020, the Justin Trudeau minority government declared, as part of their Speech from the Throne, an intention to 'redouble' their efforts to address systemic racism by "building a whole-of-federal-government approach around better collection of disaggregated data."[117] The federal government expressed this intention as part of its broader strategy to address systemic racism. While noble, consideration of APTs potential to infringe *Charter* protections against racial discrimination,

---

[117] Canada, Privy Council, *A Stronger and More Resilient Canada: Speech from the Throne to Open the Second Session of the Forty-Third Parliament of Canada*, 43–2 (23 September 2020), online: <www.canada.ca> [perma.cc/P36W-HFF7].

unreasonable search and seizure, and arbitrary detention by state actors rights and their progressive authorization under SCC jurisprudence indicates that expanded access to disaggregated data may alternatively act to exacerbate the effects of systemic racism, rather than mitigating its effects in law enforcement. This information may be used to better connect Canadians with social services, but research into the capabilities of APTs indicates that systems are already in place to algorithmically apply this information in law enforcement operations. It is worth noting that the Throne Speech includes other positive intentions to address systemic racism in Canada. Be that as it may, the constitutional risks inherent to the application of digital information as part of APT processes are much greater than the prospective benefits this information can provide.

These changes have yet to become authorized by Parliament but hold serious deleterious potential for the *Charter* rights of Canadians, particularly those who are Indigenous or Black. Our discussion reviewed the fallacious nature of historical enforcement information, as well as the risks of allowing disaggregated data collection related to specific character features like race. Canadian governments know about the use of APT in their jurisdictions, as well as the current flaws inherent to these technologies. It is also clear from the Government of Canada's Throne Speech that Parliamentary intention exists to expand access to granular data that can be input into APT systems and used by officers as part of APT outputs. Considering the serious implications this trajectory holds for Canadians, I assert that it is incumbent on Parliament and local legislators to comprehensively define the scope of APT use in law enforcement. This is more critical than ever because APTs are already in use and hold potential to affect s. 15 equality rights, as they relate to marginalized populations.

Further to this recommendation, I assert that it is most appropriate for Parliament to establish these rules in legislation, as opposed to regulations, in the criminal justice context. Some business-minded proponents argue that the Government of Canada should introduce regulations to govern the growth of algorithmic decision-making software in this jurisdiction.[118] While their arguments may have merit in the context of business enterprise, I disagree. A review of recent decisions by the OPCC shows that regulatory powers may not be enough to prevent majoritarian groups from influencing

---

[118] Aviv Gaon & Ian Stedman, "A Call to Action: Moving Forward with The Governance of Artificial Intelligence in Canada" (2019) 56:4 Alta L Rev at 1137–165.

the legislative will to strengthen privacy protections.[119] This is already the case: Moulton noted that consultative pressure was applied by industry leaders to restore the status quo after the OPCC attempted to take positive action in this regard. Instead, the Parliamentary executive confirmed their preference for allowing business as usual when it comes to sharing customer information with international third parties. [120] On this basis, I believe that regulatory flexibility is not appropriate in the context of criminal justice. The prospective risks of institutionalizing APT surveillance with too much flexibility may allow governments to quietly activate features like Palantir's Governance Entity to lower match thresholds or to grant even greater access to prejudicial data sets. Should this take place, majoritarian pressures may be strong enough to maintain course, even with minority opposition to such actions. Rather than regulations, we believe that legislation is the best avenue for authorizing the use of APTs. Further to this, legislation would allow the court to establish clear guidelines regarding the constitutionality of APT use and would require a majority will in Parliament to grant expanded access to data sets or their application in the field.

Most importantly, legislation must be introduced to govern the use of algorithmic decision-making in law enforcement because the Court has yet to validly test the constitutionality of its use in Canada. Surveillance technologies have thus far been authorized under common law police powers as a function of the ancillary powers doctrine. The SCC was reasonably able to apply the *Waterfield* test to expand powers in this way because legislation was absent. Should legislators implement a governing framework for APT use in Canada, or the broader use of surveillance technologies by law enforcement generally, the SCC will finally have an opportunity to apply the *Oakes* test to verify APT's constitutionality in relation to *Charter*-protected rights. As discussed in sections IV and V of this essay, the ancillary expansions may have been appropriate in the past to permit an investigative collection of fragmented pieces of personal data, but this method is not appropriate when its application may systemically breach the *Charter*-protected right of equality before the law.

To jump-start the legislative process, Robertson and colleagues provide a comprehensive suite of recommendations that includes

---

119 PPC, *supra* note 56; Mouton, *supra* note 57.

120 Moulton, *supra* note 57.

overall government priorities, as well as discreet points that can help to resolve APT's prospective risk to *Charter*-protected rights.[121] I agree with several of these recommendations, including commissioning a judicial inquiry into the repurposing of historical police data sets for use in APTs; establishing standards of equipment reliability, necessity, and proportionality in criminal justice; implementing a dedicated oversight organization for APT use at the regional and national levels; mandating algorithmic impact assessments[122] before any APT can be used within the relevant jurisdiction; restricting APT data collection in public spaces; and establishing mechanisms for ongoing expert consultation to retool APT limits as the technology grows and improves. I hope that elected officials are cognizant of the risks that APT poses to the rights of Canadians and that action will be taken before marginalized Canadians start slipping through these cracks at an exponential level.

While the development and implementation of APTs continue to be ignored by legislators and other government actors outright, recent legislative action from the Government of Canada indicates an understanding of the risks inherent to the information available through internet services and the historical information retained by ISPs. The Trudeau minority government recently proposed *Canada's Digital Charter* under Bill C-11, which intends to demarcate digital 'safe spaces' in order to protect personal information currently retained by private sector proponents.[123] This legislation focuses on increasing an individual's control

---

121 Robertson, Khoo & Song, *supra* note 1 at 150–69.

122 Dillon Reisman et al, "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability" (April 2018) at 5, online (pdf): *AI Now* <ainowinstitute.org> [perma.cc/D8SK-EQYD]; Algorithmic Impact Assessment" (29 March 2019), online: *Government of Canada* <open.canada.ca/aia-eia-js/?lang=en> [perma.cc/AMZ9-2E8V]; Privacy Commissioner of Canada, *Guide to the Privacy Impact Assessment Process* (Ottawa: PPC, 2020), online: <www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/#toc4-1> [perma.cc/245F-JLLH].

123 Bill C-11, *Digital Charter Implementation Act*, 2nd Sess, 43rd Parliament, 2020 (second reading 24 November 2020), online: <parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading> [perma.cc/5HGD-92Y3]; "Canada's Digital Charter: Trust in a Digital World" (12 January 2021), online: *Innovation, Science and Economic Development Canada* <www.ic.gc.ca> [perma.cc/56GZ-AZUF]; "Canada's Digital Charter in Action: A Plan by Canadians, For Canadians" (23 October 2019), online: *Innovation, Science and Economic Development Canada* <www.ic.gc.ca> [perma.cc/58WR-TENG]; Gillian Stacey et al, "New Privacy Law For Canada: Government Tables the *Digital Charter Implementation Act, 2020*" (20 November 2020), online: *Davies Ward Phillips and Vineberg LLP* <www.dwpv.com> [perma.cc/4MZM-GG56].

over information handled by private companies, institutionalizing the right for individuals to move their information from one organization to another, and ensuring that individuals can meaningfully demand the deletion of their information or for its automatic expiry when records become unnecessary. The Minister of Innovation, Science and Economic Development contends that Bill C-11 will drastically improve digital enforcement measures and will impose the strongest fines amongst Canada's partner nations for breaching privacy laws. Fines may approach the greater of 5% of a company's revenue or $25 million. This bill is encouraging but has yet to receive royal assent and entry into force.[124] At the time of writing, it is too early to evaluate the motivations of such legislation or to understand the scope of its impact related to the development and implementation of APTs in Canada.

VII. Conclusion

Our discussion reviewed the reality of APTs in Canada and the risks these technologies present to the *Charter*-protected rights of Canadians. Research indicates that Canadian governments and law enforcement agencies have already started to acquire, train, and apply APTs at the regional, provincial, and federal levels. Algorithmic technologies collate and analyze disparate information from public and private databases to identify patterns, which form the basis of formulae used to 'predict' future trends of criminal and anti-social behaviour. The results generated from these 'black-box' calculations may appear like an objective science, but, like all recorded information, they remain subject to the observational biases and operational flaws that ground the enforcement practices that influence APT outputs. Robertson and colleague's prospective research into APT implementation and development resoundingly concludes that APT

---

124 Canada, Department of Justice, *Bill C-11; An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make related and consequential amendments to other Acts*, (4 December 2020), online: <www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c11.html> [perma.cc/72BR-4FSM]; Miles Kenyon, "Bill C-11 Explained" (23 April 2021), online: *Citizen Lab* <citizenlab.ca/2021/04/bill-c-11-explained/> [perma.cc/3EDS-TYRZ]; Caroline Deschênes et al, "Canada: Digital Charter Implementation Act, 2020 (Bill C-11) – Overview of Changes to the Applicable Regime" (9 December 2020), online: *Mondaq* <www.mondaq.com/canada/privacy-protection/1014324/digital-charter-implementation-act-2020-bill-c-11-overview-of-changes-to-the-applicable-regime> [perma.cc/68BF-SM37].

deployment holds serious deleterious potential for the *Charter* rights of Canadians, with particularly malicious consequences for people of colour.

In line with Robertson and colleague's observations, this discussion highlighted how the development and implementation of APT in Canada risk macro- and micro-level encroachments of rights enshrined in ss. 8 and 9 of the *Charter*. Every stage of APT processes holds the potential to systemically infringe, if not breach outright, constitutional protections against unreasonable search and seizure, as well as arbitrary detention. While already concerning, the most pernicious consequence of applying APT in the field can be found in the use of general formulae to issue on-the-spot intervention reports to officers. These recommendations are intended to encourage officers to intervene with identified targets, often on the basis of systematically biased and inaccurate information. SCC jurisprudence indicates that police interference with individual liberties cannot be based on generalized suspicions but must instead amount to a reasonable suspicion that criminal activity may be taking place.

Legislators and governmental decision-makers understand the invasive scope of APTs and the risks inherent to their application on a macro-scale. While that is the case, lawmakers maintain their statutory ignorance of investigative digital surveillance and the proliferation of new internet-based tools like APT. Rather than demarcating their permissible uses for law enforcement purposes, these surveillance technologies continue to be authorized under the ancillary powers jurisprudence of the SCC. Jochelson explained the inappropriate nature of this approach to argue that the traditional role of courts calls for application of the *Oakes* test to determine if state action falls within its constitutional limits. Considering APTs serious implications for the rights of Canadians, Robertson and colleague's comprehensive research and recommendations, as well as the legislative intentions expressed by Parliamentarians, this paper calls on legislators to implement dedicated legislation to govern the use of surveillant technologies by law enforcement agencies, with a particular focus on regulating their use of APTs. Considering Parliament's intent to expand public access to disaggregated police data, this paper asserts that the time to implement legislation in this area is now. Failure to do so risks the exponential application of APTs against Canada's most vulnerable populations, including Black and Indigenous communities.