Canadian Journal of Law and Technology

Volume 18 | Number 2 Article 3

11-2020

Forecasting Crime? Algorithmic Prediction and the Doctrine of Police Entrapment

Mathew Zaia
University of Ottawa, Ottawa Law Review

Forecasting Crime? Algorithmic Prediction and the Doctrine of Police Entrapment

Mathew Zaia[*]

> *It should be understood at the outset, that the object to be attained is the prevention of crime. To this great end every effort of the police is to be directed. The security of person and property . . . will thus be better effected than by the detection and punishment of the offender after he has succeeded in committing the crime.*
>
> - Commissioners of the Police, Scotland Yard, 1829[1]

1. INTRODUCTION

As the Commissioners of Police in mid-19th century England illustrate above, the prevention of crime is an inherent function of public policing. To carry out their function of detecting and combating crime, police frequently endeavour to locate and use new tools enabling them to pre-empt criminal activity.[2] Many conceptual policing models that drive law enforcement's focus have been highlighted in scholarly literature: community, problem-oriented, CompStat-driven (short for computer statistics), harm-focused, and order maintenance policing. Developments in modern technology provide additional tools, allowing police forces to delve deeper into suspects' behaviour and uncover previously unknown patterns of information. Such developments have facilitated paradigmatic shifts in public and private policing practices. As a result, police may be more likely to overstep their legal and constitutional boundaries.

One example of such an overstep is police entrapment. The doctrine of entrapment has been defined by judges, lawyers, and legal scholars as the inducement of criminal activity that, without the interference of police, would not have occurred.[3] Entrapment cases may involve undercover police officers encouraging vulnerable and marginalized persons to participate in criminal activity. These covert practices risk inducing otherwise law-abiding citizens into committing an offence. While concerns over entrapment are prevalent in Canada

---

[*] B.A. (Hons.), M.A., J.D. Candidate, Editor-in-Chief (English) of the Ottawa Law Review. I wish to thank Professor Carissima Mathen for her incredibly helpful supervision and mentorship; Professor Craig Forcese for his important comments and feedback; and the late Professor Ian Kerr for inspiring me to explore artificial intelligence and its place in law. The opinions expressed herein are those of the author and should not be attributed to the Ottawa Law Review.

[1] Jerry Ratcliffe, *Intelligence-Led Policing*, 2nd ed (New York: Routledge, 2016), Chapter 2.

[2] *Ibid*, see generally Chapter 1.

[3] See Brendon Murphy & John Anderson, "After the Serpent Beguiled Me: Entrapment and Sentencing in Australia and Canada" (2014) 39:2 Queen's LJ 621.

and the United States (US) as illustrated by the case of *R. v. Nuttall*,[4] they also exist in the United Kingdom (UK) and Australia.[5] However, this paper primarily focuses on entrapment in Canadian law.

The Supreme Court of Canada has said that police investigatory powers that encourage or facilitate criminal behaviour are permissible only if law enforcement has a reasonable suspicion that an individual is engaging in criminal activity, or pursues an investigation in line with a *bona fide* inquiry.[6] Such investigations are frequently predicated on anonymous tips received through Crime Stoppers,[7] advisory letters from the Canadian Security Intelligence Service (CSIS),[8] or other data that jumpstarts an investigation.[9] In the *Nuttall* case, a disclosure letter from CSIS helped advance the Royal Canadian Mounted Police (RCMP) investigation.[10] Today, new models such as predictive policing[11] (gathering data for generalized, *geographic* suspicion centered on probability-based thinking) and intelligence-led policing[12] (engaging *individuals* with heightened levels of risk) are becoming more commonplace. For such models to establish a reasonable suspicion or to constitute a *bona fide* inquiry, a significant amount of reliable data is required.

This paper explores whether and to what extent developments in the area of AI can legitimately inform the creation of reasonable suspicions and *bona fide* inquiries in the Canadian entrapment context. The paper aims to fill a gap in Canadian entrapment scholarship, which has not focused on the possible impacts that predictive technologies may have on the contours of the doctrine.[13] It argues that due to a number of factors, including their lack of transparency, predictive

---

4 2018 BCCA 479, 2018 CarswellBC 3405 (B.C. C.A.) [*Nuttall*].

5 See *R. v. Ahmad*, 2020 SCC 11, 2020 CarswellOnt 7387, 2020 CarswellOnt 7388 (S.C.C.) [*Ahmad*] at paras 150-153 (dissenting).

6 *Ibid*; *R. v. Mack*, 1988 CarswellBC 701, 1988 CarswellBC 767, [1988] 2 S.C.R. 903 (S.C.C.) [*Mack*].

7 See *R. v. Le*, 2016 BCCA 155, 2016 CarswellBC 947 (B.C. C.A.), leave to appeal refused 2016 CarswellBC 3004, 2016 CarswellBC 3005 (S.C.C.). For an explanation of and further research on Crime Stoppers, see Randy K Lippert and Kevin Walby, "Funnelling Through Foundations and Crime Stoppers: How Public Police Create and Span Inter-Organisational Boundaries" (2017) 27:6 Policing < char style = '"amp" > Society 602.

8 Craig Forcese & Kent Roach, *False Security: The Radicalization of Canadian Anti-Terrorism* (Toronto: Irwin Law, 2015) at 116.

9 *Ibid* at 118.

10 See *Nuttall*, *supra* note 4 at para 20.

11 For a detailed description of predictive policing, see generally Andrew Guthrie Ferguson, "Predictive Policing and Reasonable Suspicion" (2012) 62 Emory LJ 259.

12 For a detailed description of intelligence-led policing, see generally United States of America, US Department of Justice, *Intelligence-Led Policing: The New Intelligence Architecture*, NCJ 210681 (Washington: International Association of Chiefs of Police, 2005).

13 However, one article in the US examined the impact of predictive policing on reasonable suspicions to strictly *stop and search*: Ferguson, *supra* note 11.

technologies present difficult challenges for officers of the court and weaken the accused's ability to argue entrapment. The paper suggests that if predictive technologies become more prevalent, the doctrine of entrapment must be revisited.

Exploring how predictability affects the doctrine of entrapment in Canada is important because police entrapment often occurs in respect of serious offences including but not limited to terrorism and drug trafficking.[14] The jeopardy for accused persons is typically high in entrapment cases. The reliability of predictive technologies bears directly on individuals' liberty; any inaccuracy could lead to an abuse of process given that individuals' decision-making would be influenced by inaccurate data or predictions. If predictive technologies are adopted more commonly in Canada, exploring their impacts on entrapment would allow legislatures and courts to prepare themselves for responding to emerging cases dealing with entrapment.

Section two of this paper discusses the Canadian doctrine of entrapment. Section three lists and describes contemporary predictive policing technologies. It additionally considers different policing models that deal with prediction. Section four addresses the reliability of predictive technology and the issues that come with using certain data. In the fifth section, the relationship between predictive technologies and entrapment law is explored. The paper concludes with observations on the challenges and opportunities of such technologies for entrapment cases. Although predictive technologies can be useful, their place in entrapment law complicates things for the existing entrapment framework and many associated stakeholders. As such, the paper's conclusion also offers general recommendations for how Canadian courts might grapple with the AI-entrapment relationship in legal matters before them.

2. A BRIEF OVERVIEW OF ENTRAPMENT

Courts can expand or inhibit police investigatory powers. The Supreme Court of Canada is seen as the guardian of police powers, as it has both enabled and limited their development.[15] Beginning in the 1980s in *R. v. Amato*,[16] the Supreme Court developed the pre-existing[17] doctrine of police entrapment with a

---

[14] For example, a terrorism-related conviction may include a maximum sentence of life imprisonment: *Criminal Code*, RSC 1985, c C-46, s. 83.22(1); those merely *accused* of terrorist activity (without being convicted) may also be subject to terrorism peace bonds with restrictive conditions pursuant to section 810.011 of the *Code*.

[15] Richard Jochelson & Mark Doerkson, "The Supreme Court of Canada Presents: The Surveillant Charter and the Judicial Creation of Police Powers in Canada" in Randy K Lippert et al, eds, *National Security, Surveillance and Terror: Canada and Australia in Comparative Perspective* (Cham: Palgrave Macmillan, 2016) 75.

[16] 1982 CarswellBC 661, 1982 CarswellBC 739, [1982] 2 S.C.R. 418 (S.C.C.); in the 1970s, scholars suggested that entrapment was not defined in Canada other than comments in *obiter*: see Joel Shafer & William J Sheridan, "The Defence of Entrapment" (1970) 8:2 Osgoode Hall LJ 277.

view to revolutionizing its treatment. As an extension of the abuse of process doctrine in the common law, entrapment is used in Canada to ensure that public police officers do not "transgress the very laws that they are entrusted to enforce."[18] In other words, the courts employ the doctrine to limit the state's power in police investigations and "protect against overreaching and discriminatory policing."[19]

When police entrap an individual, they induce the individual into committing an offence they otherwise would not have committed.[20] Defence counsel can present entrapment after the Crown has proven the offence beyond a reasonable doubt,[21] and the burden of proof lies with the accused on a balance of probabilities.[22] Thereafter, the trial judge (juries play no role in Canada) must assess the claim. If the offender is found to have been entrapped by law enforcement, a stay of proceedings is issued on the basis of abuse of process. Entrapment thus differentiates itself from traditional defences for two reasons: it does not negate any element of the offence, and the entrapped individual is not acquitted.[23]

Despite police stings[24] and entrapment being featured more in the US than in Canada, the Supreme Court of Canada in the late 20th century took its own path regarding the law of entrapment and proceeded in a different legal direction. Writing for the majority in *Mack*, Justice Lamer (as he then was) carved out an assessment of the doctrine focusing on state action. There are two ways entrapment can be established in Canada:

> (a) the authorities provide a person with an opportunity to commit an offence without acting [i] on a reasonable suspicion that this

---

[17] It existed in the English common law but was not "developed as a defence in its own right": *ibid* at 278. As such, the doctrine is pre-existing insofar as it was inherited from English common law. See also Steven Penney, "Entrapment Minimalism: Shedding the 'No Reasonable Suspicion or Bona Fide Inquiry' Test" (2019) 44:2 Queen's LJ 356.

[18] Allan Hutchinson & Neil R Withington, Comments, "Criminal Law — Evidence — Defence of Entrapment — Discretion to Exclude Evidence" (1980) 58 Can Bar Rev 376 at 376.

[19] David M Tanovich, "Rethinking the Bona Fides of Entrapment" (2011) 43:2 UBC L Rev 417 at 418.

[20] See Murphy & Anderson, *supra* note 3.

[21] See Matthew Asma & Matthew Gourlay, *Charter Remedies in Criminal Cases: A Practitioner's Handbook* (Emond, 2018).

[22] See *R. v. Swan*, 2009 BCCA 142, 2009 CarswellBC 798 (B.C. C.A.).

[23] See Asma & Gourlay, *supra* note 21.

[24] In exploring terrorism-related allegations of entrapment in several countries, Norris found that only four Canadian police stings (.11 per capita) were undertaken, while 156 US police stings (.48 per capita) were undertaken: see Jesse J Norris, "Another Form of American Exceptionalism? A Comparative Analysis of Terrorism Sting Operations in the US and Abroad" (2019) Terrorism & Political Violence, DOI: https:/doi.org/10.1080/09546553.2019.1613984.

person is already engaged in criminal activity or [ii] pursuant to a *bona fide* inquiry;

(b) although having such a reasonable suspicion or acting in the course of a *bona fide* inquiry, they go beyond providing an opportunity and induce the commission of an offence.[25]

Unlike the US's subjective, culpability-based model that assesses whether the accused was already predisposed to commit an offence,[26] the Supreme Court's objective method is confined to strictly considering the state's conduct.[27] As exhibited above, authorities' actions are central to an objective assessment. However, the accused's predisposition is not completely irrelevant to Canadian courts. To the contrary, an accused's predisposition and previous conduct becomes germane in judicial assessments of reasonable suspicions discussed below. As this paper will elaborate, the relationship between predisposition and reasonable suspicions is crucial in the realm of algorithmic predictions; it may facilitate predispositions forming part of the equation for reasonable suspicions.

The technicalities of inducing the commission of an offence (part b of the entrapment test) extend beyond the scope of this paper. Nevertheless, it is worth mentioning that without a reasonable suspicion or a *bona fide* inquiry, officers are still able to engage in "extensive discussions" with an individual "so long as they do not provide the suspect a formal opportunity to commit an offence."[28] In such cases, they are not said to be inducing the commission of an offence. With that in mind, reasonable suspicions and *bona fide* inquiries are discussed in turn.

2.1 Reasonable Suspicions

When undertaking actions that would ordinarily infringe the rights of individuals, such as detaining, arresting, or searching them, police must meet certain legal thresholds. Originating in English law,[29] reasonable suspicions are on the lower end of the investigative threshold spectrum; they are more demanding than mere suspicions but less so than beliefs based on reasonable and probable grounds.[30] In *R. v. Chehil*, the Supreme Court of Canada stated that

---

[25] *R v. Seymour*, 2016 MBCA 118 at para 6 at para 130. In *Ahmad*, *supra* note 5, the Supreme Court affirmed both prongs of the test introduced in *Mack*.

[26] The subjective approach used in the US requires counsel to prove two elements, namely that the accused was predisposed to committing the given offence and law enforcement ultimately induced the commission of the offence: see *Mack*, *supra* note 6 at para 42.

[27] *Mack*, *supra* note 6 at para 110.

[28] Kent Roach, "Be Careful what you Wish for? Terrorism Prosecutions in Post-9/11 Canada" (2014) 40:1 Queen's LJ 99 at 121, referring to a case where the offender was not granted the entrapment defence despite an extensive police sting operation absent reasonable suspicion: *R. v. Hersi*, 2014 ONSC 4143, 2014 CarswellOnt 10303 (Ont. S.C.J.).

[29] See Terry Skolnik, "The Suspicious Distinction Between Reasonable Suspicion and Reasonable Grounds to Believe" (2016) 47:1 Ottawa L Rev 223.

reasonable suspicions engage *possibility*-type assessments, whereas beliefs based on reasonable and probable grounds involve *probability*-type measurements.[31] What enables a mere suspicion to become *reasonable* is its grounding in "objectively discernible facts"[32] rather than subjective beliefs or hunches.[33] These must include "concrete and specific information supporting [police's] belief that the search will uncover evidence of criminal activity."[34]

The reasonable suspicion threshold avoids what courts call random virtue-testing, a police scheme that risks "attracting innocent and otherwise law-abiding individuals into the commission of a criminal offence."[35] Random virtue-testing often occurs in cases concerning different types of trafficking[36] or child-luring[37] offences. In simple terms, random virtue-testing involves officers attempting to incriminate an individual on mere subjective hunches rather than grounds of reasonable suspicion. Thus, to circumvent a charge of entrapment reasonable suspicions must be developed *ex ante* by police.[38]

The significance of reasonable suspicions with respect to entrapment is illustrated in numerous cases. In *R. v. Abdelhaleem*, the accused — associated with the "Toronto 18"[39] — was convicted for sections 83.18(1) and 83.2 *Criminal Code* terrorism offences. Thereafter, he claimed that he was entrapped by CSIS

---

30 See *R. v. Kang-Brown*, 2008 CarswellAlta 523, 2008 CarswellAlta 524, 2008 SCC 18, [2008] 1 S.C.R. 456 (S.C.C.) at para 75 [*Kang-Brown*].

31 See *R. v. Chehil*, 2013 CarswellNS 693, 2013 CarswellNS 694, 2013 SCC 49, [2013] 3 S.C.R. 220 (S.C.C.) at para 27 [*Chehil*]; but see generally Skolnik, *supra* note 29 where the author argues that probability logically cannot be overlooked when thinking of reasonable suspicions; possibility is inherently probabilistic.

32 *R. v. Mann*, 2004 CarswellMan 303, 2004 CarswellMan 304, [2004] 3 S.C.R. 59 (S.C.C.) at para 27 [*Mann*]; see also Simon Stern, "Textual Privacy and Mobile Information", (2018) 13:17 Osgoode Hall LJ 1; however, "less reliable information could justify reasonable suspicion, though not reasonable grounds to believe": Skolnik, *supra* note 29 at 235.

33 See *Kang-Brown*, *supra* note 30.

34 See also Steven Penney, "Unreasonable Search and Seizure and Section 8 of the Charter: Cost-Benefit Analysis in Constitutional Interpretation" in Errol Mendes & Stéphane Beaulac, eds, *Canadian Charter of Rights and Freedoms*, 5th ed (Toronto: Lexis, 2013) at 42.

35 *Mack*, *supra* note 6 at para 115.

36 See generally *Supra*, note 25 for entrapment in a weapons trafficking case.

37 See Brent Kettles, "The Entrapment Defence in Internet Child Luring Cases" (2011) 16:1 Can Crim L Rev 89.

38 See Asma & Gourlay, *supra* note 21.

39 The Toronto 18 involved a "group of 18 individuals who were planning a series of attacks in the province of Ontario and were subsequently arrested in June 2006. [. . .] Today, with the release of court records, and a number of successful prosecutions, what is clear is that some group members had the ambition, the will, and arguably the capacity to carry out a spectacular bomb attack in Canada's most populous metropolitan area": John McCoy & W Andy Knight, "Homegrown Terrorism in Canada: Local Patterns, Global Trends" (2015) 38:4 Studies in Conflict & Terrorism 253 at 262—263.

and the RCMP. The Ontario Superior Court of Justice rejected his argument and held that law enforcement had *reasonable grounds to suspect* that Mr. Abdelhaleem was engaged in terrorist activity.[40]

2.2 Bona Fide Inquiries

Reasonable suspicions are generally focused on particular individuals thought to be engaging in criminal activity. Police investigations can also be undertaken pursuant to a *bona fide* inquiry, where officers become aware of criminal activity occurring in a certain location. For example, if criminal activity exists in a particular area, officers can present opportunities to individuals in the area to commit an offence. One can observe and liken these investigations to be grounded in reasonable suspicions of crime likely occurring in a given area.[41]

Investigations pursuant to a *bona fide* inquiry do not raise concerns about random virtue-testing. Areas said to be home to criminal activity expose any individual in said area to possible police investigation. Chief Justice Lamer, writing for the majority in *R. v. Barnes*, commented on this police power:

> When such a location is defined with sufficient precision, the police may present any person associated with the area with the opportunity to commit the particular offence. . . Such randomness is permissible within the scope of a *bona fide* inquiry.[42]

The rise of technology complicates these sorts of investigations. In *Ahmad*, the accused was subject to a "dial-a-dope" investigation where the Toronto Police Service received credible information regarding an individual selling drugs by way of telephone.[43] The pertinent question was whether *bona fide* inquiries applied beyond physical areas to virtual things like phone numbers. The Supreme Court affirmed that the test in *Mack* applied to virtual spaces. The majority (5-4) of the Court emphasized that "police must have reasonable suspicion over an individual or a well-defined virtual space, like a phone number, before providing an opportunity to commit a crime."[44] Writing for four dissenting judges, Justice Moldaver concluded that the *bona fide* inquiry prong of the *Mack* test required revision so as "to preserve the fundamental balance struck in *Mack* and *Barnes* between protecting individual liberties and fostering effective law enforcement while also bringing the doctrine in line with the realities of the digital age."[45]

---

[40] See *R. v. Abdelhaleem*, 2010 CarswellOnt 9938, [2010] O.J. No. 5693 (Ont. S.C.J.).

[41] See *R. v. Barnes*, 1991 CarswellBC 915, 1991 CarswellBC 11, [1991] 1 S.C.R. 449 (S.C.C.) [*Barnes*]. In *Barnes*, one of the questions put to the Court was whether the police had a reasonable suspicion about criminal activity occurring in a given area so as to present the accused with an opportunity to commit a crime. The Court found that the investigating officer's suspicion was instead based on a hunch.

[42] *Ibid* at 463 [emphasis in original].

[43] *Ahmad*, *supra* note 5.

[44] *Ibid* at para 40 [emphasis added]. In essence, the Court held that *bona fide* inquiries are not limited to physical spaces and extend into the digital world.

To summarize, in *Mack*, the Supreme Court provided two ways — in addition to inducement — whereby police can avoid entrapment: establishing reasonable grounds to suspect or investigating pursuant to a *bona fide* inquiry. Employed to avoid practices like random virtue-testing, maintain the function of the criminal justice system, and limit state power, these precursors to permissible police investigations have been stagnant for many years. Regarding the expansion of *bona fide* inquiries, *Ahmad* presents new challenges to the law of entrapment due to the use of technology, but it affirms the test provided in *Mack*. Indeed, the Supreme Court's split decision demonstrates such challenges. It sheds light on how expanding entrapment into the digital sphere may present issues with which courts may have to grapple.

3. POLICING AND VIRTUAL PREDICTIONS

The police have a number of tools enabling their reactive practices including apprehending suspects, questioning appropriate witnesses, and collecting relevant evidence. For many years, the concept of reaction served as the nucleus to police action; everything done by police served a reactive purpose.[46] Viewed in this light, law enforcement had three functions: "routine patrol, immediate response to calls, and follow-up investigations."[47] The use of analytical tools at law enforcement's disposal shifts conventional policing toward a preventative, proactive approach. Two models have dominated discourse surrounding these expanding proactive police practices: intelligence-led and predictive policing.

This section outlines those two models. After providing a brief overview of both intelligence-led and predictive policing (3.1), the section refers to specific programs that use AI to aid their predictions (3.2). It does not seek to catalogue a comprehensive list of current policing models and programs. Instead, it intends to shed light on predictive technologies with a view to assessing how reasonable suspicions and *bona fide* inquiries in the entrapment doctrine are affected. To address predictive technologies, one must highlight the concept of data.

3.1 Monitoring, Collecting, and Analyzing Data

As consumers, our everyday lives are loaded with smart technology and data: devices that feature biometric capabilities;[48] fitness trackers that measure health conditions; and social media platforms such as Facebook and Twitter that use AI to predict individual likes and dislikes.[49] The growth in technology usage

---

[45] *Ibid* at para 186 (dissenting).

[46] See Jan Scott, "'Performance Culture': The Return of Reactive Policing" (1998) 8:3 Policing & Society 269.

[47] Department of Justice, "Police Discretion with Young Offenders", *Government of Canada* (7 January 2015), online: < www.justice.gc.ca > .

[48] See Shoshana Magnet, *When Biometrics Fail: Gender, Race, and the Technology of Identity* (Duke University Press, 2011).

produces a vast supply of data about billions of individuals. Some liken data to the "new oil" given the extent to which it features in sophisticated commercial transactions.[50] Indeed, the benefits of technology enable consistent data movement and transactions.[51]

There has also been a growth of surveillance by governments, private corporations, and individuals alike, all of which correspond to decreasing levels of personal privacy. Governments use technology to oversee and understand populations; private corporations like Amazon surveil and create products that enable citizens to surveil one another.[52] As a result, "[l]ess and less escapes the surveillant eye."[53]

Mass surveillance practices allow the collection of data that is useful for AI and algorithms for a variety of purposes, including administrative decision-making.[54] A key example is the criminal justice system. In the US, a program called COMPAS uses historical data to assess levels of risk that individuals pose for recidivism. In the UK, some police forces use a "Harm Assessment Risk Tool" (Hart) to forecast individual propensity to commit offences.[55] A similar tool is used in Australia, where police employ a "Suspect Targeting Management Plan" (STMP) to measure whether children as young as 11-years old are likely to offend. There are many other examples of predictive analytics in the justice system.[56]

Data-monitoring tools are in a constant state of flux. After complementing traditional surveillance practices, such as the population census, for many years, contemporary surveillance techniques now transcend them. Mark Andrejevic notes that "[a]t no previous time in human history has so much information been captured, stored, and sorted."[57] The vast quantity of data that is captured by and makes its way through "surveillance assemblages"[58] is often referred to as "big

---

[49] See Raghav Bharadwaj, "AI for Social Media Censorship — How it Works at Facebook, YouTube, and Twitter" *Emerj* (10 February 2019), online: < www.emerj.com > .

[50] Ramona Pringle, "'Data is the New Oil': Your Personal Information is Now the World's Most Valuable Commodity", *CBC* (25 August 2017), online: < www.cbc.ca > .

[51] See Bernard Harcourt, *Exposed: Desire and Disobedience in the Digital Age* (Harvard University Press, 2015).

[52] See Mathew Zaia, "Exploring Consciousness: The Online Community's Understanding of Mobile Technology Surveillance" (2019) 17:3/4 Surveillance & Society 533.

[53] David Lyon, *The Culture of Surveillance* (Cambridge: Polity Press, 2018) at 35.

[54] See Jesse Beatson, "AI-Supported Adjudicators: Should Artificial Intelligence Have a Role in Tribunal Adjudication?" (2018) 31 Can J Admin L & Prac 307.

[55] Sarah Marsh, "UK Police use of Computer Programs to Predict Crime Sparks Discrimination Warning", *The Guardian* (3 February 2019), online: < www.theguardian.com/uk > .

[56] For example, the Law Commission of Ontario suggests that automated decision-making is being used "in areas as diverse as immigration and refugee proceedings, police profiling, and to determine sentencing, bail and parole conditions": Law Commission of Ontario, "Automated Decision-Making in the Criminal Justice System" (22 March 2019), online: < www.lco-cdo.org > .

data."[59] These bodies of data are recognized by virtue of their volume, velocity, and variety,[60] as they enable storage and analysis through "datafication."[61] Used for various purposes, big data often carries data about data[62] and is regularly bought and sold.

Big data is compiled — often by consent to terms and conditions — from users or consumers of technology; this includes smartphone applications for social media, or food delivery and travel applications.[63] Some suggest that data are given willingly due to consumer trust in companies,[64] while others argue that the convenience and capacities of technology override individual protection of personal data.[65] Other data-gathering technologies include those to which consumers do not necessarily voluntarily subject themselves, some of which

---

[57] Mark Andrejevic, "Automating Surveillance" (2019) 17:1/2 Surveillance & Society 7 at 7.

[58] See Kevin D Haggerty & Richard V Ericson, "The Surveillant Assemblage" (2000) 51:4 Brit J Soc 605.

[59] For an introduction to big data, see Mark Andrejevic & Kelly Gates, "Big Data Surveillance: An Introduction" (2014) 12:2 Surveillance & Society 185.

[60] See Edd Dumbill, "Volume, Velocity, Variety: What You Need to Know About Big Data", *Forbes* (19 January 2012), online: < www.forbes.com > .

[61] See Jose van Dijck, "Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology" (2014) 12:2 Surveillance & Society 197.

[62] This is otherwise known as "metadata." The former Privacy Commissioner of Ontario defined metadata as "information generated by our communications devices and our communications service providers, as we use technologies like landline telephones, mobile phones, desktop computers, laptops, tablets or other computing devices": see Craig Forcese, "One Warrant to Rule Them All: Reconsidering the Judicialisation of Extraterritorial Intelligence Collection" in Randy K Lippert et al, eds, *National Security, Surveillance and Terror: Canada and Australia in Comparative Perspective* (Cham: Palgrave Macmillan, 2016) 27 at 34, citing Ann Cavoukian, "A Primer on Metadata: Separating Fact from Fiction" (2013) Ontario: Information and Privacy Commissioner, July. According to Justice Simon Noël of the Federal Court, "[m]etadata, on its own and processed through aggregation and analysis, can provide intimate insights into the lifestyle and personal choices of individuals; it is not an innocuous kernel of information": see John Paul Tasker, "What You Need to Know About the CSIS Metadata Ruling," *CBC News* (4 November 2016), online: < www.cbc.ca > .

[63] The legal scholar Bernard Harcourt calls the current surveillance society — one where consumers willingly expose themselves — the "expository society." For a theoretical discussion about the expository society, see generally Bernard Harcourt, "Digital Security in the Expository Society: Spectacle, Surveillance, and Exhibition in the Neoliberal Age of Big Data" (2014) Columbia Public Law Research Paper No 14-404.

[64] Fen Osler Hampson & Eric Jardine, *Look Who's Watching: Surveillance, Treachery and Trust Online* (Waterloo: CIGI Press, 2016).

[65] For example, see Emily West, "Amazon: Surveillance as a Service" (2019) 12:1/2 Surveillance & Society 27 for a discussion about how Amazon's surveillance suggests that North American populations have normalized surveillance for individual, beneficial purposes.

include automated license-plate readers,[66] police body cameras,[67] and airport biometric surveillance.[68]

The prevalence of these data requires ever-more efficient ways to analyze them. At the forefront of the analysis is AI, which not only provides enhanced capabilities, but in many cases learns new ways to undertake such functions.[69] Technologies with AI capabilities — such as robots — are being introduced in a number of industries. Indeed, AI is now permeating the confines of homes by way of machines such as Google Home and Amazon Alexa.[70] However, AI is inoperable without constant data input for processing and analysis.

Police forces are now using AI and algorithmic technologies to carry out their law enforcement functions.[71] These technologies draw data from a number of sources, including conventional crime reports containing suspect, offender, victim, and geographic data. As administrative decision-making tools, they must be consistent with principles of legality, transparency, justice, and fairness. Contemporary policing technologies also aid these algorithms. For example, police body cameras often carry biometric data, and "Stingrays" are able to collect data from network-connected devices in a given geographic area. Scholars note that "intelligence gathering has become one of the most strategic processes of surveillance."[72] These data are essential to modern policing functions, especially where prediction is at play.

The more common these policing tools become, the more challenges they present. COMPAS, for example, relies on controversial factors such as parental criminality, which can be distorted by previous bias and discrimination in policing.[73] And yet, the algorithm is used by the judiciary to determine sentencing options for convicted persons.[74] The Australian Youth Justice

---

66 See Ian Warren et al, "When the Profile Becomes the Population: Examining Privacy Governance and Road Traffic Surveillance in Canada and Australia" (2013) 25:2 Current Issues in Criminal Justice 565.

67 See Barak Ariel, "Police Body Cameras in Large Police Departments" (2016) 106:4 J Crim L & Criminology 729.

68 See Magnet, *supra* note 48.

69 See Harry Surden, "Artificial Intelligence and Law: An Overview" (2019) 35:4 Ga St U L Rev 1305; this is frequently referred to as machine learning.

70 For a review of household robots with respect to privacy, see Margot E Kaminski, "Robots in the Home: What Will We Have Agreed To?" (2015) 51 Idaho L Rev 661.

71 For the discussion that follows, the author cautions the reader not to merely assume a *Minority Report* style of policing that, like Big Brother, morphs the nation into an Orwellian-type dystopia. Law enforcement instead uses these data-guided tools carefully with an eye to undertake appropriate police functions and avoid discriminatory and other negative practices.

72 Kevin Walby, Randy K Lippert & James Gacek, "Securitising 'National Interests': Canadian Federal Government Departments, Corporate Security Creep, and Security Regimes" in Randy K Lippert et al, eds, *National Security, Surveillance and Terror: Canada and Australia in Comparative Perspective* (Cham: Palgrave Macmillan, 2016) 155 at 160.

Coalition suggests that those who are flagged by the STMP "experience a pattern of constant harassment by police".[75] It states that the STMP can have an adverse discriminatory effect on Indigenous Australians.

Beyond algorithmic prediction's minor presence in contemporary Canadian policing, it is likely that Canadian police services will predominantly base future investigations on some combination of algorithmic predictions using AI.[76] If so, a "reasonable" suspicion in the context of entrapment may turn out to be "virtual", informed by predictive technologies. If sufficiently widespread, such virtual suspicions could permit police to circumvent the strictures of current entrapment law.

3.2 Intelligence-Led and Predictive Policing

For approximately two decades, intelligence-led and predictive methods have dominated policing discourse. Intelligence-led policing began being used in the late 20th and early 21st centuries. In Canada, the RCMP adopted intelligence-led policing so as to advance beyond community policing models.[77] Despite AI not being as popular in early 21st century policing, intelligence itself was devised by individual officers from everyday police-gathered information. This intelligence was used, along with other problem-solving tools, to "target groups and individuals involved in serious organized crime or terrorism."[78]

Public Safety Canada defines intelligence-led policing as a way for "police to identify individuals at high risk and geographic areas of high risk. With this knowledge, police resources are utilized more effectively and efficiently to proactively respond to criminal activity."[79] Intelligence-led policing was formulated to redirect policing toward proactive measures.[80] Engaging both quantitative and qualitative analysis, intelligence-led policing:

---

[73] AI Now, *Litigating Algorithms: Challenging Government Use of Algorithmic Decision Systems* (An AI Now Institute Report, 2018) at 13.

[74] *Ibid.*

[75] Vicki Sentas & Camilla Pandolfini, *Policing Young People in NSW: A Study of the Suspect Targeting Management Plan* (A Report of the Youth Justice Coalition NSW) at 20.

[76] See Office of the Privacy Commissioner of Canada, "The Age of Predictive Analytics: From Patterns to Predictions" (August 2012), online: < https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/pa_201208/ > ; Ontario Human Rights Commission, "Policy on Eliminating Racial Profiling in Law Enforcement" (August 2019), online: < http://www.ohrc.on.ca/en/policy-eliminating-racial-profiling-law-enforcement#_ednref255 > .

[77] See John Edward Deukmedjian & Willem de Lint, "Community into Intelligence: Resolving Information Uptake in the RCMP" (2007) 17:3 Policing & Society 239.

[78] See Adrian James, "Book Review: Intelligence Led Policing (2nd ed)" (2017) 28:1 Policing & Society 120 at 121.

[79] Public Safety Canada, "Intelligence-Led Policing (Details)", Government of Canada (1 August 2013), online: < www.publicsafety.gc.ca > .

[80] See Ratcliffe, *supra* note 1, Chapter 2.

> is designed to be a model for the business of policing; aims to achieve crime and harm reduction, prevention and disruption; focuses on [. . .] prolific offenders, repeat victims and active criminal groups; employs a top-down management approach; merges crime analysis and criminal intelligence; [and] aids police resource prioritization.[81]

Some observe that the model now uses "biometric and drone technologies" while also amassing "data generated through the use of social media."[82] Most recently, scholars have noted that the model requires accumulating information from many sources, "including surveillance, informants and other agencies, to target habitual offenders and gain crime reduction efficiencies."[83] In Canada, the enactment of the *Anti-terrorism Act, 2001* broadened and facilitated such intelligence-led policing powers.[84]

Predictive policing has similar premises but is "[r]egarded as a refinement of 'intelligence-led policing'."[85] It has been described as:

> [T]he use of historical data to create a forecast of areas of criminality or crime hot spots, or high-risk offender characteristic profiles that will be one component of police resource allocation decisions. The resources will be allocated with the expectation that, with targeted deployment, criminal activity can be prevented, reduced, or disrupted.[86]

Predictive policing models currently utilize advanced analytics by way of machine learning and other AI to predict areas that are or will be fraught with criminal activity.[87] The non-profit RAND Corporation suggests that predictive policing is also attentive to particular individuals and their propensity to commit crime.[88]

In addition to data-mining methods, the model uses historical criminal data to pre-empt crime.[89] These methods include "algorithms to estimate a probability of future criminality at places or among high-risk people."[90]

---

81 *Ibid.*

82 Adrian James, "Intelligence-led Policing: Comparing National Approaches to its Regulation and Control" in Monica den Boer, ed, *Comparative Policing from a Legal Perspective* (Cheltenham: Edward Elgar, 2018) 134 at 136.

83 Jeremy G Carter & Bryanna Fox, "Community Policing and Intelligence-led Policing: An Examination of Convergent or Discriminant Validity" (2019) 42:1 Policing: An Intl J 43 at 44.

84 *Ibid.*

85 Privacy SOS, "What's Predictive Policing?", online: < www.privacysos.org > .

86 Jerry Ratcliffe, "Predictive Policing" in David Weisburd & Anthony A Braga, eds, *Police Innovation: Contrasting Perspectives* (Cambridge: Cambridge University Press, 2019) at 347 at 349.

87 See Albert Meijer & Martijn Wessels, "Predictive Policing: Review of Benefits and Drawbacks" (2019) 42:12 Int'l J Public Admin 1031.

88 See Walter L Perry et al, "Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations" (2013) RAND Corporation.

89 *Ibid.*

Recent developments in predictive policing highlight the model's ability to use "all kinds of societal data and variables"[91] to help facilitate more accurate results.

Predictive policing inherently consists of intelligence-led policing qualities, and the inverse is also apparent. It would be difficult for law enforcement to use raw data alone to fashion predictions. Data must be analyzed (by humans or machines) to produce intelligence which can inform police predictions. By definition, this policing strategy is *intelligence-led*.[92] Similarly, intelligence-led policing engages proactive policing by means of prediction using intelligence, ultimately allowing law enforcement to anticipate which areas and people require attention rather than remain reactive. Therefore, in the rest of the paper reference to both models will be made using the term "predictive policing" to capture the notion of police attempts to predict and prevent criminal activity using artificial intelligence and algorithms. The technicalities of the two terms for the purposes of this paper are not as important as highlighting law enforcement's predictive capabilities and how that influences the doctrine of entrapment.

Indeed, AI allows predictive policing to function more efficiently. The vast amount of data available to police departments[93] necessitates the use of machine analysis, as analysis by humans would be too cumbersome. Using AI helps locate "behavioural patterns and create a method for the sharing of data in the fight against crime."[94] Algorithms facilitate an easier approach to prediction than methods such as hands-on traditional geographic mapping.[95] These systems already exist in a number of police departments, as the following examples demonstrate.

> **PredPol** (short for predictive policing) is used by 50 US police forces. One of the most popular predictive programs, PredPol uses similar "models that predict earthquake aftershocks"[96] to predict criminality. The company running and distributing the program suggests that its

---

90 Ratcliffe, *supra* note 86 at 347.

91 Simon Egbert, "Predictive Policing and the Platformization of Police Work" (2019) 17:1/2 Surveillance & Society 83 at 84.

92 One author echoes this sentiment by submitting that predictive policing "borrows from the principles of [. . .] intelligence-led policing": see Beth Pearsall, "Predictive Policing: The Future of Law Enforcement?" (2010) Nat'l Inst Just J No 266.

93 But see Andrew Ferguson, "Big Data and Predictive Reasonable Suspicion" (2015) 163:2 U Pa L Rev 327, as he suggests that despite this amount of data available to police, much of it may not even be used.

94 John Wulff, "Artificial Intelligence and Law Enforcement" (2017) GIAC (GCFA) Gold Certification.

95 This refers to the traditional method of using pins to predict which sites would be most susceptible to crime.

96 Maha Ahmen, "Aided by Palantir, the LAPD Uses Predictive Policing to Monitor Specific People and Neighbourhoods", *The Intercept* (11 May 2018), online: < www.theintercept.com > .

algorithms can improve crime detection by up to 50 percent. The program relies on historic criminal data, including locations of crime, timing of crime, and type of crime, combined with "other socio-economic data."[97] Its creators claim that PredPol can discern criminal hot spots over a range of up to 150 square-meters.[98]

LASER (also known as "operation LASER"), used in the US, is a bit more dated, originating in 2011. LASER program is assisted by a private corporation, Palantir, which provides technology that enables law enforcement to score individuals. A higher number of points forces individuals onto a "Chronic Offender Bulletin" on which police focus much of their efforts.[99]

HunchLab is a more limited program that focuses its efforts on particular kinds of crime, as it predicts "genuinely *new* risk patterns for certain areas."[100] This program is unique insofar as it uses "data about [social] infrastructure" in addition to "imaginative rationales of big data mining in policing" to manufacture predictions. Indeed, it is reasonable to assume that the implementation of smart cities would therefore develop HunchLab's capabilities and performativity.

National Data Analytics Solution (NDAS) is a software that has made headlines in recent months. Based in the UK, NDAS is currently being developed by the West Midlands Police following a year of previous testing.[101] This program seeks to discern "where crime will be committed and by whom."[102] However, current reports suggest that NDAS leads are ensuring that the project is subject to independent review for ethical purposes.

Visual Analytics for Sense-making in Criminal Intelligence Analysis (VALCRI) is another project based in the UK that seeks to use machine learning to predict timeslots and areas with higher crime trends and patrol needs.[103] The program is said to use "anonymous criminal records, whilst also pulling in data *from a range of other*

---

[97] Mark Smith, "Can we Predict When and Where a Crime will Take Place?", *BBC* (30 October 2018), online: < www.bbc.com > .

[98] Ahmen, *supra* note 96.

[99] Issie Lapowsky, "How the LAPD Uses Data to Predict Crime", *Wired* (22 May 2018), online: < www.wired.com > .

[100] Egbert, *supra* note 91 at 85 [emphasis in original].

[101] Conor Reynolds, "Home Office to Invest $5 Million Into Police National Data Analytics Solution", *Computer Business Review* (18 July 2019), online: < www.cbronline.com > .

[102] Nafeez Ahmed, "Are we Sleepwalking into an AI Police State?", *Raconteur* (27 March 2019), online: < www.raconteur.net > .

[103] See Thomas Marquenie, "Data Analytics in a Police Context: Addressing Legal Issues in VALCRI", *KuLeuven Centre for IT & IP Law* (14 March 2017), online: < www.law.kuleuven.be > .

> *sources* to provide analysts with insight" regarding police detective work and possibly patterns in crime detection.[104]

Predictive policing practices have also entered Canada. In Vancouver, police have taken the next step: using spatial analytics and machine learning to predict crime over a 100-meter radius.[105] Alleged to be accurate over 80 percent of the time, the algorithms target locations for upcoming criminal activity within a one- to five-hour timespan.[106]

Most, but not all, predictive policing programs use data available exclusively to police. These data include crime reports and tips of alleged or possible criminal activity. For example, the Ottawa Police Strategic Operations Centre (OPSOC) gathers data from crime reports, floor plans in public buildings, and social media to "provide frontline officers with crime statistics and predictive analytics."[107] It is not clear, however, whether these are the only data inputted into algorithms. One researcher suggests that social media and other data (e.g. VALCRI program above) being used by police departments is imminent, as "this is already happening" in "places such as Vancouver and Toronto."[108] For example, there exists the possibility of fourth-party corporations being useful to state data collection[109] according to the following logic: user "1" submits data to entity "2", which then sells 1's data to corporation "3", who has contractual obligations to release such data to "4". If, for example, "4" is willing to provide this information to state agencies at a payable rate, some wonder whether law enforcement might be able to use such data as part of their predictive programs.

3.3 Smart Cities

In 2009, a federally funded US report suggested that city or neighbourhood planning (such as the design of spaces or police resource allocation) would be considered for future predictive policing.[110] Now, smart cities are increasingly featured in North America; that 66 percent of American cities are engaging with smart cities reveals their popularity.[111] Smart cities exhibit an interplay between

---

[104] ADI, "The Rise in Intelligence Led Policing", *The Horizons Tracker* (5 July 2017), online: < www.adigaskell.org > [emphasis added].

[105] See John Beck, "Vancouver Police Drive Down Crime with Machine Learning and Spatial Analytics", *ESRI* (21 February 2019), online: < www.esri.com > .

[106] *Ibid*; see also Matt Meuse, "Vancouver Police Now Using Machine Learning to Prevent Property Crime", *CBC News* (22 July 2017), online: < www.cbc.ca > .

[107] Nathan Munn, "Predictive Policing is Coming to Canada's Capital, and Privacy Advocates are Worried", *Vice* (13 February 2017), online: < www.vice.com > .

[108] Alex Ballingall, "Surveillance and Predictive Policing: Welcome to the 'Safety State' of Tomorrow", *Toronto Star* (10 May 2016), online: < www.thestar.com > .

[109] See Joshua L Simmons, "Buying You: The Government's Use of Fourth-Parties to Launder Data about 'the People'" (2009) 3 Colum Bus L Rev 950.

[110] Craig D Uchida, "A National Discussion on Predictive Policing: Defining Our Terms and Mapping Successful Implementation Strategies" (2009) NCJ 230404 Discussion Paper.

private and public sectors using communication technologies and data governance in a city's infrastructure.[112] Viewed from different perspectives, the advanced cities are and can be used for a number of underlying purposes, one of which involves:

> [P]ervasive and ubiquitous computing and digitally instrumented devices built into the very fabric of urban environments [. . .] that are used to monitor, manage and regulate city flows and processes, often in real-time, and mobile computing [. . .] used by many urban citizens to engage with and navigate the city which themselves produce data about their users.[113]

Monitoring, managing, and regulating are done through both pre-existing and novel urban technologies, including self-driving shuttle busses,[114] drones engaging in fast-food delivery,[115] and smart energy, infrastructure, and mobility.[116] The core of smart city technology is its ability to produce valuable data. Scholars have observed that ownership of this data is shared by a number of parties, including the municipality where the technologies are utilized.[117]

In 2017, the Government of Canada encouraged the implementation of smart cities by announcing its first Smart Cities Challenge.[118] The competition "empower[ed] communities to adopt a smart cities approach" for various purposes.[119] The process involved several municipalities submitting proposals for their own smart city visions. For example, the winner of the grand prize ($50 million CAD) detailed a list of elements that were central to its proposal, including engagement and mobilization efforts, collaborative governance, and an impact measurement approach.[120] Showing enthusiasm to smarten their cities, many other municipalities also submitted proposals.

---

[111] See Nick Ismail, "Smart City Technology: It's all About the Internet of Things", *Information Age* (14 August 2018), online: < www.information-age.com > .

[112] See Rob Kitchin, "The Real-Time City? Big Data and Smart Urbanism" (2014) 79:1 GeoJournal 1.

[113] *Ibid* at 2.

[114] See e.g. Charlotte Jee, "New York City's Self-Driving Shuttle Service Launches Today", *MIT Technology Review* (7 August 2019), online: < www.technologyreview.com > .

[115] See Charlotte Jee, "Uber says it will Start Delivering McDonald's by Drone this Summer", *MIT Technology Review* (13 June 2019), online: < www.technologyreview.-com > .

[116] See Teena Maddox, "Smart Cities: 6 Essential Technologies", *TechRepublic* (1 August 2016), online: < www.techrepublic.com > .

[117] See Teresa Scassa, "Who Owns all the Data Collected by 'Smart Cities'?", *The Toronto Star* (23 November 2017), online: < www.thestar.com > .

[118] See Infrastructure Canada, "Smart Cities Challenge", *Government of Canada* (Updated 14 May 2019), online: < www.infrastructure.gc.ca > .

[119] *Ibid*.

[120] Montreal Final Proposal, "Summary of the Proposal", *Smart Cities Challenge Canada* (Updated 14 May 2019), online: < www.infrastructure.gc.ca > .

Among Canada's proposed smart cities, the City of Toronto's partnership with Sidewalk Labs — a member of the tech giant Google family[121] — has made headlines. One panel of experts in Toronto recently questioned the ownership of the produced data.[122] The Ontario Information and Privacy Commissioner had suggested that plans to substantiate data privacy for the Sidewalk Labs project were problematic.[123] The Commissioner called for the provincial legislature to address gaps in privacy legislation before commencing the smart city project[124] which was ultimately cancelled.

As sensors and other gadgets permeate the walls of Canadian cities, they will necessarily extend law enforcement's predictive arm. Important questions that remain unanswered include but are not restricted to which public or private bodies will retain the data and for how long, how the data will be stored and protected, and how transparency will work with respect to processes and purposes of data collection.

If municipal, provincial, or federal police agencies are able to access and use smart city data, their algorithmic predictions will be polished, and their ability to cross-reference existing data will presumably be enriched. A simple example involves the possibility of ubiquitous wireless internet,[125] which could be complemented by, for example, Stingrays for cross-network data collection. Ultimately, using a Stingray would allow the agency operating the device to intercept network communications.[126] The ability to obtain data from a smart city filled with technology may therefore "be of potential value in a criminal investigation or to prevent crime from occurring in the first place."[127]

3.4 Data Reliability, Sufficiency, and Accuracy

As mentioned earlier in this paper, predictive tools are only as accurate as the data they are fed. What happens when this data has deliberately been corrupted?[128] When was the data created? How can users be sure that the data

---

[121] See Nick Summers, "Toronto is Reining in Sidewalk Labs' Smart City Dream", *Engadget* (31 October 2019), online: < www.engadget.com > .

[122] See David Ride & Jacob Lorinc, "Digital Panel Raises Big Concerns with Sidewalk Labs' Smart City Proposal", *The Star* (10 September 2019), online: < www.thestar.com > .

[123] See Donovan Vincent, "Sidewalk Labs' Urban Data Trust is 'Problematic,' Says Ontario Privacy Commissioner", *The Star* (26 September 2019), online: < www.thestar.com > .

[124] *Ibid.*

[125] See Nicholas Sokic, "Five Smart City Technologies that Sidewalk Labs is Pitching", *Financial Post* (28 June 2019), online: < www.business.financialpost.com > .

[126] See Torin Monahan, "Built to Lie: Investigating Technologies of Deception, Surveillance, and Control" (2016) 32:4 The Information Society 229.

[127] Elizabeth E Joh, "Policing the Smart City" (2019) 15 Int'l J L in Context 177 at 177.

[128] See Karen Hao, "Police Across the US are Training Crime-Predicting AIs on Falsified Data", *MIT Technology Review* (13 February 2019), online: < www.technologyreview.com > .

is free of bias? Will certain groups of people be unevenly affected by the data? These questions are among the many that scholars, governments, and private corporations continue to ponder in light of increasing algorithmic decision-making. The importance of such questions stems from the need to use reliable and sufficient data for fair and equitable practices.

While some predictive policing programs have been explored and tested, the majority have not been rigorously scrutinized to warrant their everyday, real-world use. The minimal testing and evaluation of predictive policing tools remain impediments to predictive policing's growth and evolution.[129] Many predictive tools are too novel for evaluative reports to exist.[130] Scholars characterize existing studies as inconclusive, ultimately suggesting it is simply "too early to say if [predictive policing] does lead to more effective policing."[131]

Predictive policing tools typically amass older, raw data to produce their algorithmic predictions. As these data often include previous crime data, they are "necessarily limited by what individuals choose to report and what law enforcement officers directly observe."[132] For example, some police departments may have a reporting record replete with certain minority groups, while other records may exhibit a history of inaccurate or insufficient reporting, broadly understood. Predictive tools will thus deliver varying kinds and types of predictions.

Absent any processes to confirm that data is not biased, flawed, or fragmented, predictive tools merely perpetuate pre-existing issues. In part, these issues are perpetuated because of how much more efficient AI and algorithms are than general human analysis. The more bad data, the more inherently biased, inaccurate, and unreliable results.[133] Consider the following illustration. Where a police department's predictive tools rely on data from over-policed geographic areas filled with minorities, algorithms will likely point to the same areas suggesting further police presence. The algorithm's predictions may even increase the likelihood of recidivism in the same areas.[134] In these instances, "predictive policing itself affects the data collected."[135] That is, the criminal activity officers

[129] See Andrew Guthrie Ferguson, "Policing Predictive Policing" (2017) 94:5 Washington University L Rev 1109.

[130] See Lindsey Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border" (2017) 41:327 NYU Review of Law & Social Change 327.

[131] Sylvia Thomson, "'Predictive Policing': Law Enforcement Revolution or Just New Spin on Old Biases? Depends on who you ask", *CBC* (24 September 2018), online: < www.cbc.ca > .

[132] Lyria Bennett Moses & Janet Chan, "Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability" (2018) 28:7 Policing & Society 806 at 809.

[133] See Ezekiel Edwards, "Predictive Policing Software is More Accurate at Predicting Policing than Predicting Crime", *Huffington Post* (31 August 2016), online: < www.huffpost.com > .

[134] See Rashida Richardson, Jason M Shultz & Kate Crawford, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice" (2019) 94:192 NYU L Rev 192.

are led to will be used as subsequent crime data fed into the algorithm.[136] The cycle then continues again and again.

The more algorithmic predictions are used, the more data is needed. Scholars have explored the possibility of police data being "bad" for a number of reasons beyond common threats like racial bias. For example, bad data "includes flaws, fragmentation, and the internal and external pressures to collect vast amounts of data."[137] These data may involve human error as a product of officers incorrectly inputting information such as home addresses.[138] Another example is "dirty" data "derived from or influenced by corrupt, biased, and unlawful practices, including data that has been intentionally manipulated."[139] Such data is sometimes a result of work pressures facilitated by managers, as they seek certain analyses, crime report data, and outcomes.[140] These issues beg the question of whether police would in fact increase their surveillance efforts to gather, store, and analyze more data through their new predictive algorithms. Overreaching data-gathering efforts can be problematic because insufficient or unnecessary means may be used to acquire the data and satisfy required benchmarks.

Safeguards are needed to protect individuals from predictions based on subpar data. In some jurisdictions, protections against bad data in respect of algorithmic decision-making have already been administered.[141] The UK's General Data Protection Regulation (GDPR) provides that "a data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning individuals or similarly significantly affects them."[142] In the predictive policing context, this protection may enable officers to use their discretion rather than strictly follow what the predictive programs recommend. Canadian legislation

---

[135] Moses & Chan, *supra* note 132 at 810.

[136] *Ibid*. See also Richardson, *supra* note 134, where the authors suggest that situating officers in certain areas based on statistics leads to areas being both more policed and criminalized than usual.

[137] Ferguson, *supra* note 129 at 1145.

[138] *Ibid*. The author also emphasizes that proponents of PredPol would suggest that their predictive program is not subject to such deficiencies given that it primarily focuses on reported crime rather than things like arrest statistics.

[139] See Richardson, Shultz, & Crawford, *supra* note 134 at 195. Here, the authors show that the Los Angeles Police Department incorrectly recorded 14,000 serious assaults as minor offences from 2005 to 2012.

[140] See John A Eterno, Arvind Verma & Eli B Silverman, "Police Manipulations of Crime Reporting: Insiders' Revelations" (2016) 33:5 Justice Q 811 at 829.

[141] For example, legislatures in Washington have taken initial steps to develop protections in respect of algorithmic decision-making: State of Washington House Bill 1655 (66th Legislature, 2019 Regular Session), referred to Committee on Innovation, Technology & Economic Development.

[142] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679, Article 22.

protecting citizens from bad data may be warranted when predictive policing becomes heavily reliant on algorithmic decision-making.

In 2019, Canada adopted its Directive on Automated Decision-Making.[143] The Directive was formulated to ensure that state decisions made with algorithms are "compatible with core administrative law principles such as transparency, accountability, legality, and procedural fairness."[144] One of its core functions is to ensure emerging technologies are also captured by its guidelines. In brief, the Directive provides a number of requirements that must be met when using algorithms for decision-making. Requirements range from "providing a meaningful explanation to affected individuals of how and why the decision was made"[145] to issues concerning data quality, where "the automated decision system [must be] relevant, accurate, [and] up-to-date."[146] Other elements such as up-to-date information may conflict with some older data used for predictive policing. Given that both predictive policing and the Directive are in their infancy, their interplay has yet to be observed.

The reliability of predictive policing in respect of algorithmic decision-making will vary from one police department to the next depending on historic police practices. If a police department is already relying on flawed data to make conventional human-generated predictions, these practices will necessarily heighten existing flaws. Indeed, police departments are not in the business of creating additional issues for their already difficult work. When further considering algorithmic capabilities, one could argue that the efficiency tied to algorithms — and in this case with the ability to help prevent criminal activity — may outweigh the prejudicial implications attached. In addition, some indicate that using algorithms precludes individual human biases.[147] Nevertheless, safeguards are important in guaranteeing that individuals affected by algorithmic predictions, particularly in the criminal justice system, understand what goes on behind the scenes to establish such predictions.

4. ALGORITHMIC PREDICTIONS AND THE ENTRAPMENT DOCTRINE

Having explored the contours of entrapment law and complexities of predictive policing, the paper now turns to whether and how predictive policing fits into the Canadian entrapment doctrine. This section is separated in four parts. Part one discusses subjective predispositions and how these are affected by

---

[143] See Government of Canada, "Directive on Automated Decision-Making" (Updated 05 February 2019), online: < www.tbs-sct.gc.ca >.

[144] *Ibid*.

[145] *Ibid*, s. 6.2.3.

[146] *Ibid*, s. 6.3.3.

[147] See Thomson, *supra* note 131; but see Kari Paul, "'Disastrous' Lack of Diversity in AI Industry Perpetuates Bias, Study Finds", *The Guardian* (17 April 2019), online: < www.theguardian.com >.

predictive policing. Second, changes are recommended concerning judicial assessments of reasonable suspicions and *bona fide*. The third part touches on possible issues for suspected and accused persons, including with respect to the presumption of innocence. Finally, the section concludes with remarks on obstacles for both Crown and defence counsel, particularly regarding disclosure.

4.1 Doctrinal Modification: Subjective Predispositions

Subjective predispositions of the offender do not justify bringing entrapment allegations. Recall that unlike US entrapment law, predispositions in Canadian criminal law are not used to assess whether police officers have appropriate reasonable suspicions. Predispositions merely become factors that affect police's gathering of a reasonable suspicion and are ultimately not sufficient on their own.[148] As Chief Justice Lamer and Justice Major clarified in *R. v. Pearson*,[149] predisposition is not the focus of entrapment; instead, entrapment is concerned with whether "guilt was uncovered in a manner that shocks the conscience and offends the principle of decency and fair play."[150]

To prevent police from over-focusing on recidivists when establishing reasonable suspicions, courts should be more cautious when dealing with subjective predispositions. As noted in an earlier section, predictive policing can potentially enable cycling back to previous offenders. Subjective predispositions would therefore be crucial and significant when reaching the reasonable (virtual) suspicion threshold. In simple terms, predictions, if amounting to reasonable suspicions, will unfortunately heavily rely on past criminal records and individuals with a propensity to commit a criminal offence. They will rely on subjective predispositions. It is thus reasonable to suggest that predisposition dominates the reasonable suspicion equation when dealing with algorithmic predictions.

Given the inherent weight of predisposition that pulls technological predictions in certain directions, it is also reasonable to ask whether Canadian entrapment law would instead be following a subjective approach when rooted in predictive policing algorithms. Indeed, the subjective approach relies on individuals' predisposition to engage in criminal activity. Predictive policing's focus and basis on predisposition begs the question of whether an offender, upon alleging entrapment, bears the burden of proving a lack of predisposition to counter the given algorithm.[151] Taking it one step further, the offender would have one task: establishing proof — likely on a balance of probabilities given that the beyond a reasonable doubt threshold would be too high — that the data showing they were predisposed to commit a crime was incorrect or flawed. Once

---

[148] See Murphy & Anderson, *supra* note 3.

[149] 1998 CarswellQue 1079, 1998 CarswellQue 1080, [1998] 3 S.C.R. 620 (S.C.C.).

[150] *Ibid* at 628.

[151] See *Mack*, *supra* note 6 at para 110 where Justice Lamer discusses offenders having to prove wrongful police conduct.

the offender has proven lack of predisposition, the burden would likely shift to the Crown to prove — perhaps beyond a reasonable doubt similar to the US — that the offender was in fact predisposed. However, the Crown would be armed with predictive policing data — in addition to other resources — to meet this burden.

To avoid focusing purely on predisposition, decisions engaging in reasonable suspicion analysis should not be fully automated. That is, much like Article 22 of the GDPR noted earlier in this paper, police departments should be required to use their own judgment when acting on algorithmic predictions. A predictive policing algorithm should not be immediately resorted to and applied without further police inquiry. Although this would involve more work for police departments, it would be a small price to pay to ensure validity, legitimacy, and accuracy of their predictive tools.

Police officers must therefore maintain *some* discretion in their line of work. Assuming full-scale implementation of predictive policing technologies, questions will surely surface — among legal practitioners and scholars — regarding whether *all* algorithmic predictions should be responded to immediately, or whether some take priority over others.[152] That law enforcement should automatically respond to and investigate every algorithmic prediction would vitiate any discretion. The danger in removing police discretion completely is that:

> [d]iscretion is at the root of criminal justice practice. Police officers necessarily exercise discretion in deciding whether to [. . .] stop and search or arrest. Some people look less 'suspicious' than others, and possible offences have to be prioritized. [. . .] Similarly, when officers are able to be proactive (as compared to their usual reactive mode) they have to use discretion about the offences or offenders in which to invest scarce time.[153]

Officers ought to use their discretionary powers to embark on investigations and act on algorithms prior to presenting opportunities to commit crimes. Of course, it may be difficult for officers to strike a balance between deference to the algorithms and their own discretion. It is worth questioning why algorithms would be used in the first place if law enforcement would still have overruling authority. In using their discretion, officers should also be expected to provide clear reasons for prioritizing one prediction over the other or ignoring some altogether. Ultimately, police discretionary power should remain intact as an

---

[152] In and of itself, the prospect of departments prioritizing some algorithmic predictions over others may open the door to civil liability if certain predictions should have been (but were not) acted upon. Indeed, civil liability in this respect falls beyond the boundaries of this paper.

[153] Andrew Sanders & Richard Young, "From Suspect to Trial" in Mike Maguire, Rod Morgan, & Robert Reiner, eds, *The Oxford Handbook of Criminology*, 5th ed (Oxford: Oxford University Press, 2012) 838 at 842.

important policing tool, but law enforcement should be ready to provide grounds for its decision-making in respect of responding to predictions.[154]

Due to the issue of possibly inaccurate predictions, Parliament should require officers to embark on a reasonable risk minimization analysis before acting on a virtual prediction. Indeed, police have long since become risk and knowledge workers.[155] Law enforcement is expected to eliminate or diminish risk when investigating criminal activity, as risk management "is one of the most important components in law enforcement and public safety, both in the daily administrative mayhem and operational duties."[156] As such, requiring officers to minimize risk in the course of their investigations would be paramount. If police simply act on every prediction the algorithm provides, many people subject to the predictions may be incorrectly targeted. Enacting legislation to have officers engage in risk minimization analysis would be a start. Therefore, courts would ultimately need to be satisfied that police officers have engaged in risk minimization so as not to allow each and every prediction — heavily reliant on predisposition — to be acted upon.

4.2 Doctrinal Modification: Reasonable Suspicions and *Bona Fide* Inquiries

Provided police departments engage in minimizing the inherent risks in assessing predisposition, questions of reasonable suspicion and *bona fide* inquiries must be unpacked. This paper argues for the modification of the current entrapment doctrine and the minimization of risk. Modification is necessary to maintain police accountability in the investigative process. If police departments find predictive policing more accurate and efficient, then the police ought to be more accurate and precise in their investigations relying on predictive policing. Further accuracy and precision would ensure that as policing tools advance and develop, police accountability also follows. In other words, police precision and accuracy leads to more precise and accurate predictions as the algorithms develop.

In *Mack*,[157] Justice Lamer stated that if police had sufficient information to suggest that criminal activity was occurring in a given area, any individual in the area could be provided the opportunity to commit said criminal offence. He provided an example, saying that if police receive a number of complaints of theft at a bus terminal, causing them to investigate pursuant to a *bona fide*

---

[154] Officers providing such grounds would ensure that ultimately accurate algorithms are not avoided because of possible biased police decision-making. It is reasonable to assume that some algorithms will be quite accurate in their predictions, so avoiding these predictions requires justification so as to prevent discrimination or bias by officers.

[155] See Randy K Lippert & Kevin Walby, "Marketization, Knowledge Work and Visibility in 'Users Pay' Policing in Canada" (2014) 54:2 Brit J Crim 260, i.e. their work involves investigation, risk management, and sharing knowledge.

[156] Matthias Wicks, "Risk Management: A Key Component in Public Safety" (ND) online, *Police Chief Magazine*: < www.policechiefmagazine.org > .

[157] *Supra* note 6.

inquiry, they could place a handbag in the middle of the terminal. Upon seeing someone take the handbag, they could arrest the individual without engaging in entrapment. Despite law enforcement providing an opportunity to anyone in the area to commit a crime, they circumvent the strictures of entrapment because of the *bona fide* inquiry.

Where police use predictive policing in similar circumstances to the example provided in *Mack*, Justice Lamer would likely permit police presenting similar opportunities to anyone in the given area. Indeed, his ruling in the predictive policing context would be viewed in a similar light to ordinary police data producing a *bona fide* inquiry. The difference would be the efficiency predictive policing offers. As such, Justice Lamer would likely allow predictive policing in this context, but he would surely question whether the data used for prediction were sufficient, valid, and reliable, as well as how they are authenticated by police.

This paper proposes that police need to be sufficiently precise when investigating criminal activity and presenting opportunities to commit an offence. The concept of using predictive policing to develop a reasonable suspicion or investigate pursuant to a *bona fide* inquiry suggests that such technology must be more scrupulous for investigations. If the tool is more efficient and accurate, the general Canadian public would likely call for more accuracy and precision in police investigations reliant on predictive policing. Not only would more accuracy and precision be fruitful for community-police relations, but the use of more accurate technology warrants more exact investigations to justify the tools' use.

Not requiring greater precision would lead to an increase in police power without a similar increase in police accountability. In the bus terminal example in *Mack*, this would mean anyone in the vicinity would still be subject to the presentation of an opportunity to commit a crime, albeit without ensuring that predictive policing is not being abused. In other words, predictive policing being more accurate necessitates further precision when police engage certain individuals rather than merely being able to "test" anyone who is present in a given area.[158] Perhaps in a case more similar in its facts to *Barnes* where the Court opposed investigations being grounded in subjective hunches, a six-block radius would be too wide, ultimately requiring a narrower approach when using predictive policing tools. Therefore, both reasonable suspicions and investigations pursuant to *bona fide* inquiries would require police to be more precise when deciding how opportunities are presented and to whom.

If the notion that any persons present in an area may be subject to criminal opportunity is removed from the entrapment doctrine, random virtue-testing would be bypassed. Random virtue-testing refers to incriminating individuals

---

[158] This is important given that the Supreme Court has suggested that "[a] method of searching that captures an inordinate number of innocent individuals cannot be reasonable, due to the unnecessary infringement of privacy and personal dignity that an arrest would bring": *Chehil*, *supra* note 31 at para 51.

based on mere police hunches rather than being grounded in reasonable suspicions or *bona fide* inquiries.[159] In *Barnes*, the Supreme Court of Canada held that the police did not entrap the offender given the existing reasonable suspicion on which their investigation was based; any individual present in the area was subject to opportunities to commit a crime. Some have argued that the case of *Ahmad* involved some form of random virtue-testing. In that case, police operated on uncorroborated tips and ultimately called related phone numbers, arranged to meet the individuals, and purchased drugs from them prior to executing the arrests. Restricting the scope of a suspected area and the individuals with whom police may engage would guarantee that random virtue-testing is significantly diminished.

Avoiding random virtue-testing would do much to prevent discriminatory practices. As noted earlier, predictive policing may keep police investigations hovered over certain areas. These areas may predominantly be home to people from particular socio-demographic groups. If officers are constantly instructed — by virtual suspicions — to return to such areas, typical reasonable suspicions and investigations pursuant to *bona fide* inquiries would likely amount to greater chances of recidivism. That is, police officers recognizing previous offenders may alert them, when they arrive in a given area, to present said persons with criminal opportunities because of the individual's association with criminal conduct. As such, further precision and accuracy of the geographic area or individual persons being investigated would avoid these discriminatory practices.

In short, further precision of reasonable suspicions and investigations pursuant to *bona fide* inquiries circumvent random virtue-testing. Presumably, police departments would not fully implement predictive policing programs until ensuring some accuracy. If police considerably rely on predictive policing tools to meet their investigatory thresholds and also engage in risk minimization, there would be no need to worry about random-virtue testing. The police would have ultimately minimized risk, used more precise and accurate predictions, and ensured "[a] nexus [. . .] between the criminal conduct [. . .] and the investigative technique employed."[160] If each of the opportunities offered by police are grounded in these thresholds, law enforcement would necessarily avoid any random virtue-testing.

4.3 Implications for the Suspected, Accused, and Crown and Defence Counsel

Implementing a new, more efficient and accurate policing tool obviously increases the state's power to investigate. These tools support police's use of resources beyond the general public's reach. As a result, the data used and collected impacts the lives of Canadians. Ultimately, using these tools risks legal implications for suspects with whom predictive policing tools engage. Legal

---

[159] See *Barnes*, *supra* note 41.

[160] *Chehil*, *supra* note 31 at para 36.

implications also exist for suspects who become accused persons following arrest, demonstrating the interplay between predictive policing tools and the criminal justice process.

This section explores some arising ramifications for both suspects and accused persons when predictive policing technologies are adopted. The section does not purport to establish a comprehensive list of effects that suspects and accused persons may experience. However, it does offer some insight into questions that would be necessary to address in the predictive policing landscape. The highlighted issues range from being "selected" by an algorithm to alleging entrapment. Particularly, it explores the presumption of innocence and disclosure issues.

Offenders may run into a host of issues when alleging entrapment, one of which involves the presumption of innocence. For years, the presumption of innocence has been "a foundational principle of the modern criminal justice system."[161] The rule ensures that only those whose offences have been proven by the state to reach a legal threshold — beyond a reasonable doubt — are considered guilty. In the event that a judge or jury finds that the Crown has met its burden and secured a conviction, a punishment may be imposed.[162] Until then, the presumption of innocence is in full force, and its protection is crucial because of strong measures such as punishment; the fragility of fact-finding at trials; the maintenance of proper relationships between the state and citizens; and standards of proof.[163] However, the presumption is not limited to the trial context; it also applies to pre-trial circumstances when considering its "reputation-related aspect,"[164] its moral value,[165] and its protection against arbitrary state conduct.[166]

In the entrapment context, predictive policing could produce deleterious effects for the presumption of innocence. Given the surveillance practices rooted in predictive policing algorithms, these effects are engendered due to the possible shift of legal burden. Recall that beyond conventional policing records and statistics, emerging technologies — including in smart cities — can assist the substance of predictions. The use of these technologies in criminal proceedings

---

[161] Nicole Marie Myers, "Eroding the Presumption of Innocence: Pre-trial Detention and the use of Conditional Release on Bail" (2017) 57:3 Brit J Crim 664 at 664.

[162] *Ibid.*

[163] See Andrew Ashworth, "Four Threats to the Presumption of Innocence" (2006) 10 Int'l J of Evidence & Proof. 241.

[164] *Ibid* at 244. Here, the author is referring to the fact that the presumption involves disallowing public figures to "make statements imputing guilt to the defendant before trial and conviction"

[165] See Antonella Galette, "The Changing Nature of the Presumption of Innocence in Today's Surveillance Societies: Rewrite Human Rights or Regulate the Use of Surveillance Technologies?" (2013) 4:2 European J of L and Tech.

[166] See Hannah Stewart, "The Right to be Presumed Innocent" (2014) 8:2 Crim L and Philosophy 407.

can often redirect the burden of proof "from the claimant to the accused or suspected"[167] to challenge issues with the technologies. If burdens shift to the accused, there will be additional onuses on the accused to prove that they should not have been subject to algorithmic predictions.[168] In addition, predictive policing tools can help develop the police's belief that any individual may be perceived as the "bad man,"[169] thereby calling the presumption of innocence into question far before the court process. In other words, an algorithm's accurate prediction may result in individuals being treated as already guilty on moral (not legal) grounds.

On the other hand, predictive policing for entrapment purposes may be able to assist non-suspected and non-accused persons. If predictive policing algorithms are precise enough to determine who may be subject to reasonable suspicions, they will also guarantee that others should not be subject to similar suspicions. While some suggest smart technologies will create a culture of suspicion,[170] the same technology also "enables the innocent to be rapidly eliminated from enquiries."[171] When formulating reasonable suspicions about particular individuals, police will theoretically be able to distinguish certain individuals and avoid investigating others. The prospect of narrowing an investigation toward one individual — whether by way of reasonable suspicion or *bona fide* inquiry — will logically enable technologies to identify those who should not be subject to investigation.

Following conviction, however, offenders are responsible for proving entrapment. At its core, entrapment is a defence against conviction, but it differs from traditional defences in ways mentioned earlier in this paper. Offenders must nevertheless prove that one of the entrapment branches have been met, and in doing so they engage their *Charter* right to make full answer and defence. The right to make full answer and defence is a significantly complex right that encompasses sections 10 and 11 of the *Charter* and is also a principle of fundamental justice.[172] Beyond the possibility of accused persons having further burdens following predictive policing's implementation, it would become increasingly challenging to allege entrapment when reasonable suspicions or *bona fide* inquiries are based on algorithms.

The major obstacle offenders and their counsel face is that of disclosure, and Crown counsel may also struggle with the same concept. Governed by the

---

[167] Galette, *supra* note 165.

[168] This is further discussed below with respect to making full answer and defence.

[169] See Ian Kerr, "Prediction, Pre-Emption, Presumption: The Path of Law After the Computational Turn" in Mireille Hildebrandt & Katja de Vries, eds, *Privacy and Due Process After the Computational Turn* (London: Routledge, 2013) 91.

[170] See Katerina Hadjimatheou, "Surveillance Technologies, Wrongful Criminalisation, and the Presumption of Innocence" (2016) 30:1 Philosophy & Tech 39.

[171] *Ibid* at 39.

[172] See *R. v. Rose*, 1998 CarswellOnt 4392, 1998 CarswellOnt 4393, [1998] 3 S.C.R. 262 (S.C.C.).

ordinary rules of evidence at trial, entrapment hearings follow similar statutory and common law principles in respect of evidence. The Canadian common law disclosure rule holds that, upon prosecuting an individual, the Crown has a duty to disclose all information that is likely relevant to the case at bar.[173] Here, the Crown can "resist disclosure by establishing clear irrelevance."[174] Disclosure, which must occur prior to the accused's election of trial,[175] is an ongoing Crown duty and a defendant's right "whether or not it is favourable to the accused person."[176]

For disclosure purposes, the Supreme Court of Canada has established that police departments are separate from the Crown. The Crown is faced with disclosure obligations while the police are not held to the same standards. However, the separation does not preclude police from withholding certain information. In *R. v. McNeil*,[177] Justice Charron, writing for the majority, insisted that it is common knowledge "that the police have a corollary duty to disclose to the prosecuting Crown all material pertaining to the investigation of an accused."[178] The Court reminds us that the Crown has a duty to inquire further if it becomes aware of relevant information.[179]

With a focus on entrapment, algorithms informing reasonable suspicions or *bona fide* inquiries present a difficult puzzle to solve for the Crown, and this can affect the defence's ability to make full answer and defence. Evidently, predictive policing algorithms are part of the police investigation and are relevant to cases relying on them. As part of their corollary duty, the police are therefore required to disclose the information. The duty then rests on the Crown to disclose this relevant information to defence counsel.

A question then remains unanswered: exactly what information must the Crown disclose? Is the Crown required to share the inner workings of the algorithm? The data on which the algorithm's prediction is based? To further complicate things, third-party companies usually own and maintain the technology itself, and the inner workings of the technology and how it works is proprietary for, *inter alia*, intellectual property purposes.[180] Given that

---

[173] See *R. v. Stinchcombe*, 1991 CarswellAlta 559, 1991 CarswellAlta 192, [1991] 3 S.C.R. 326 (S.C.C.). If the information is sought by the defendant, and the defendant has a reasonable expectation of privacy in that information, the *O'Connor* and *Mills* regimes govern production: see David M Paciocco, "Filling the Seam Between *Stinchcombe* and *O'Connor*: The "*McNeil*" Disclosure Application" (2007) 53 Crim LQ 161.

[174] Paciocco, *ibid* at 163.

[175] See Máximo Langer & Kent Roach, "Rights in the Criminal Process: A Case Study of Convergence and Disclosure Rights" in Mark Tushnet, Thomas Fleiner & Cheryl Saunders, eds, *Routledge Handbook of Constitutional Law* (Routledge, 2013).

[176] Brian Manarin, "Assessing the Expert: A Call for Reciprocal Disclosure in Canada" (1999) 39:1 Med Sci L 17 at 17.

[177] 2009 SCC 3, 2009 CarswellOnt 116, 2009 CarswellOnt 117 (S.C.C.).

[178] *Ibid* at para 52.

[179] *Ibid*.

companies "are frequently unwilling to disclose the formula [. . .] on which their tools are based,"[181] it is reasonable to question the precise nature of the Crown's duty in such circumstances.

Determining what information is required in order for defence counsel to offer a full answer and defence becomes difficult. Algorithms are highly sophisticated in nature and are not very well understood by non-experts. Such complications and minimal understanding of the technology may even present problems for other legal actors given that:

> [I]f a police officer, magistrate judge, or the public does not have access to how the predictions are made, there is no check on the legitimacy of the factors used. Nor is there a way to ascertain whether further decisions that relies on those circumstances [. . .] were legally reached.[182]

In the event that the algorithms remain observed through technological jargon, defence counsel's ability to argue entrapment — and the other officers of the court's understanding of the matter — is surely hindered.

At first glance, the next reasonable step would be to disclose the algorithm's workings using ordinary language. Conveying the information so as to make it accessible would enable parties of the court to better understand the algorithms. However, access to the mechanics of the algorithm would likely threaten law enforcement's work. Suppose an algorithm gathered a reasonable suspicion on a particular individual who was in the midst of terrorist activity. If the way in which the algorithm predicted such activity was disclosed to the public, police investigations would be vulnerable. To prevent such disclosure, police may have to argue that the information is privileged and therefore should not be disclosed.

Complications with disclosure in these circumstances extends to those who are subject to predictive policing algorithms. Recall that Canada's Directive regarding automated decision-making requires that individuals are informed of how decisions were made with some sort of transparency. The Directive allows Canadians to understand the reasons for which they are subject to algorithmic decision-making in line with administrative principles. Beyond a court of law, then, individuals have the right to request such information. Therefore, access to this information — for our purposes, information governing the algorithm — is of utmost importance when an individual is prosecuted by the state.

A final issue involves whether the predictive policing programs should simply be accepted as authoritative and valid. In other words, defence counsel may benefit from being able to use the data on which the charge was based and call experts to test validity, methodology, and more. If permitted, defence counsel

---

[180] See Mara Hvistendahl, "Crime Forecasters: Police are Turning to Big Data to Stop Crime Before it Happens" (2016) 353:6307 ScienceMag 1484.

[181] Robert Muggah, "Does Predictive Policing Work?" (4 December 2016), online *Igarapé Institute*: < www.igarape.org.br > .

[182] Barrett, *supra* note 130 at 344.

may even be able to consult with experts to build their own analysis based off the data and measure whether the expert's model(s) is more accurate and valid than the predictive policing's algorithm.

How the Crown provides this information to offenders is one concern that, if approached satisfactorily, can make the process fairer and more transparent. A government-mandated independent oversight body for predictive policing tools is a start. Predictive policing will surely evolve with new ways of informing predictions, and one way to maintain accountability is through an oversight body to ensure data is being used objectively, is valid, and is up to date. An oversight body would assist offenders in understanding the algorithm's legitimacy, but it would also enable law enforcement to conduct their investigations without fear of repercussions for insufficient or problematic data. Presumably, such an entity would consist of experts in artificial intelligence and algorithms. Although it would not fully address disclosure issues, an oversight body is a first step for all officers of the court and provides transparency for judges to "determine whether or not an officer's reliance on that information was reasonable."[183] Perhaps the implantation of such a body would help maintain automated data analysis' "promises to make [. . .] institutional decision-making more objective, consistent, and rigorous."[184]

5. CONCLUSION

The landscape of technology in North America is constantly evolving and continues to present new challenges to existing legal doctrines and principles. Gone are the days where technological apparatuses were restricted to common functions (e.g. simple mathematical calculations) that simply expedited human processes and practices. AI and algorithms instead offer new ways to analyze data, perform tasks, and undertake processes of which humans are incapable.[185] They have taken on a number of human practices and functions to promote expeditious and nuanced analyses, while also performing other operations. Indeed, artificial intelligence and algorithms are able to do something humans have desired and questioned for many years: predict phenomena. Coupled with the ability to predict, however, are the rights and freedoms of individuals that ought to be addressed.

A number of Canadian judicial decisions accept the maxim that as technology continues to evolve, so too must the law. Most pertinent to this belief are cases that involve communications between different technologies[186] or police retrieving certain information by searching and seizing such

---

[183] Barrett, *supra* note 130 at 343.

[184] Aaron Shapiro, "Predictive Policing or Reform? Indeterminacy and Intervention in Big Data Policing" (2019) 17:3/4 Surveillance & Society 456 at 456.

[185] For the use of AI and algorithms and questions posed therefrom, see generally Patrick Lin, Keith Abney & George A Bekey, eds, *Robot Ethics: The Ethical and Social Implications of Robotics* (Cambridge: MIT Press, 2014).

technologies.[187] Although the law is developing in these areas, a number of legal issues have not yet been considered in light of sophisticated technology. This paper suggests that the entrapment doctrine ought to be modified in light of predictive policing's growth in the criminal justice system. Given predictive policing's ability to previse criminal activity using historic and current data, the entrapment doctrine developed in *Mack* should be revisited.

A few qualifications are needed to avoid negative repercussions for a number of stakeholders in the entrapment context. These provisos are mere suggestions as to how Canadian courts can tackle questions of entrapment when they are based on predictive policing. First, police should follow the Government of Canada's Directive on Automated Decision-Making strictly and ensure that decisions are not made *purely* by predictive policing tools. In order to fulfil this task, police must maintain their discretion when responding to predictive policing's directions regarding investigatory steps.

Second, when predictive policing is used to develop reasonable suspicions or investigate pursuant to *bona fide* inquiries, precision and accuracy are key elements to maintaining police accountability. These are also important in the digital world as illustrated in *Ahmad*, where the Supreme Court — referring to the use of technology in entrapment generally — held that "the virtual space in question must be defined with sufficient precision in order to ground reasonable suspicion."[188] Police departments using more accurate tools (i.e. predictive policing) to discern locations or individuals in respect of criminal activity should be held to a higher standard when making their determinations. The more accurate and precise the investigating police officers are, the less likely a court will be to find that random virtue-testing occurred.

Finally, implications for the suspected, accused, or counsel for both sides must be addressed by the courts. Here, questions arise regarding the presumption of innocence and whether the legal burden shifts onto the accused, as well as whether officers begin to presume those who are subject to predictive policing algorithms as guilty. Nevertheless, the more accurate a prediction, the more precise and believable the circumvention of other, non-accused and non-suspected persons. Difficulties also arise for defence and Crown counsel. As for defence counsel, issues with respect to disclosure and how the algorithmic information is conveyed may be one concern. With defence counsel requiring such specific information to make full answer and defence for an accused, Crown counsel is obliged to disclose this relevant information. The difficulties that come with Crown (and even police to Crown counsel) disclosure arise for two reasons. First, the technology that is used for predictive policing is typically proprietary, and its inner workings ought not to be disclosed for competition purposes.

---

[186] See generally *R. v. Marakah*, 2017 SCC 59, 2017 CarswellOnt 19341, 2017 CarswellOnt 19342 (S.C.C.).

[187] See generally *R. v. Cole*, 2012 SCC 53, 2012 CarswellOnt 12684, 2012 CarswellOnt 12685 (S.C.C.).

[188] *Ahmad*, *supra* note 5 at para 41.

Second, disclosing how police sift through these covert technological investigations would threaten police powers and their ability to conduct law enforcement duties effectively.