Osgoode Hall Law Journal

Volume 60, Issue 2 (Spring 2023) Article 2

7-10-2023

Oversight of Police Intelligence: A Complex Web, but Is It Enough?

Lyria Bennett Moses
Faculty of Law and Justice, UNSW

Citation Information

Bennett Moses, Lyria. "Oversight of Police Intelligence: A Complex Web, but Is It Enough?." *Osgoode Hall Law Journal* 60.2 (2023) : 289-336.
DOI: https://doi.org/10.60082/2817-5069.3892
https://digitalcommons.osgoode.yorku.ca/ohlj/vol60/iss2/2

Oversight of Police Intelligence: A Complex Web, but Is It Enough?

Abstract

This article analyzes the jurisdiction, function, powers, and expertise of oversight mechanisms with reference to capacity to oversee the legality of emerging police intelligence practices such as facial recognition, social media analytics, and predictive policing. It argues that oversight of such practices raises distinct issues ranging from the general oversight of policing, given the secrecy associated with police intelligence generally, to the use of complex software in particular. It combines doctrinal analysis with analysis of interviews with policing intelligence analysts, intelligence managers, lawyers, and IT professionals in three jurisdictions: Canada, Australia, and New Zealand. It brings together the roles of a variety of entities involved directly or indirectly in oversight; in particular, professional standards units, independent police and public sector oversight bodies, intelligence oversight, privacy and human rights regulators, courts, political bodies, contracting parties, and ad hoc bodies. Understanding the web of oversight as a whole, and comparing across jurisdictions, it concludes with specific proposals for reform.

Oversight of Police Intelligence: A Complex Web, but Is It Enough?

LYRIA BENNETT MOSES*

This article analyzes the jurisdiction, function, powers, and expertise of oversight mechanisms with reference to capacity to oversee the legality of emerging police intelligence practices such as facial recognition, social media analytics, and predictive policing. It argues that oversight of such practices raises distinct issues ranging from the general oversight of policing, given the secrecy associated with police intelligence generally, to the use of complex software in particular. It combines doctrinal analysis with analysis of interviews with policing intelligence analysts, intelligence managers, lawyers, and IT professionals in three jurisdictions: Canada, Australia, and New Zealand. It brings together the roles of a variety of entities involved directly or indirectly in oversight; in particular, professional standards units, independent police and public sector oversight bodies, intelligence oversight, privacy and human rights regulators, courts, political bodies, contracting parties, and ad hoc bodies. Understanding the web of oversight as a whole, and comparing across jurisdictions, it concludes with specific proposals for reform.

* UNSW Allens Hub for Technology, Law and Innovation, Faculty of Law and Justice, UNSW Sydney. This project was funded by a SSHRC partnership development grant. "Conceptions of Intelligence: Building a Cross National Comparative Analysis of Practices and Frameworks of Policing," 890-2016-0067. The author is grateful to the broader project team led by Carrie Sanders and including Janet Chan, Simon Mackenzie, James Sheptycki, Trevor Bradley, Crystal Weston, and Holly Blackmore, as well as to research assistants Lara Tessaro and Lauren Parnaby for their input and support. She also appreciates the feedback from the anonymous peer reviewers and editorial board.

INTELLIGENCE-LED POLICING has been defined as "a business model and managerial philosophy where data analysis and crime intelligence are pivotal to an objective, decision-making framework that facilitates crime and problem reduction, disruption and prevention through both strategic management and effective enforcement strategies that target prolific and serious offenders."[1] Intelligence-led policing is associated with a shift to strategic, future-oriented, proactive, and targeted approaches, particularly those that focus on risk and threat assessment and crime prevention across a wide area rather than responding to a single historic event.[2] This approach has been an important aspect of policing in Canada, Australia, and New Zealand since the early 2000s.[3] Whether or not intelligence-led policing is adopted wholeheartedly or effectively, police departments in those jurisdictions now include crime or intelligence analysts who analyze flows of data to generate actionable intelligence used in the prediction and management of crime.[4]

1. Jerry Ratcliffe, *Intelligence-led Policing* (Routledge, 2008) at 89.
2. *Ibid* at 8.
3. *Ibid* at 40.
4. See Carrie Sanders & Camie Condon, "Crime Analysis and Cognitive Effects: The Practice of Policing Through Flows of Data" (2017) 18 Global Crime 237 at 237, 241; Carrie B Sanders, Crystal Weston & Nicole Schott, "Police Innovations, 'Secret Squirrels' and Accountability: Empirically Studying Intelligence-led Policing in Canada" (2015) 55 Brit J Crim 711 at 712.

While the idea of intelligence-led policing is not new, the practices and technologies associated with it are evolving.[5] CompStat, started by the New York City Police Department in the 1990s, is the best-known early example of intelligence-led policing. CompStat analyzed crime data, with maps and statistical summaries used as a basis for analyzing the performance of commanders at regular meetings where commanders were held accountable for patterns of crime in their precincts.[6] While traditional methods, such as statistics, mapping, and simple visualisations remain important, intelligence-led policing now includes newer techniques associated with artificial intelligence. For example, police might use social media analytics to profile activists[7] or Clearview AI for facial recognition (both to identify specific suspects and to facilitate broader surveillance).[8] Some police departments use predictive policing software or methods to identify "risky" neighbourhood blocks or individuals.[9]

Accountability in the use of such tools is important because of the potential for harm.[10] Groups can be stigmatized, often along racial lines, when neighbourhoods are singled out for police surveillance.[11] There are also individual harms for those

5. See Michael T Rossler, "The Impact of Police Technology Adoption on Social Control, Police Accountability, and Police Legitimacy" in Cara E Rabe-Hemp & Nancy S Lind, eds, *Political Authority, Social Control and Public Policy* (Emerald, 2019) 209.
6. See Eli B Silverman, *NYPD Battles Crime: Innovative Strategies in Policing* (Northeastern University Press, 2001).
7. See Jim Bronskill, "Mounties Defend Social Profiling After Assembling Portrait of Activist," *CBC News* (2 January 2020), online: <www.cbc.ca/news/politics/rcmp-defends-social-media-profiling-1.5413580> [perma.cc/F84X-V8ZG].
8. See Mackenzie Smith, "Police Searched for Suspects in Unapproved Trial of Facial Recognition Tech, Clearview AI," *RNZ News* (15 May 2020), online: <www.rnz.co.nz/news/national/416697/police-searched-for-suspects-in-unapproved-trial-of-facial-recognition-tech-clearview-ai> [perma.cc/37LD-WRJG]; The Detail, "Blurred Lines - the Police and Facial Recognition Technology," *RNZ News* (17 September 2020), online: <www.rnz.co.nz/programmes/the-detail/story/2018764397/blurred-lines-the-police-and-facial-recognition-technology> [perma.cc/3BGS-QWLH].
9. Janet Chan & Lyria Bennett Moses, "Can Big Data Analytics Predict Policing Practice" in Stacey Hannem et al, eds, *Security and Risk Technologies in Criminal Justice* (Canadian Scholars Press, 2019); Shawn Singh, "Algorithmic Policing Technologies in Canada" (2021) 44 Man LJ 246 at 288.
10. See *e.g.* Kate Robertson, Cynthia Khoo & Yolanda Song, *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada* (Citizen Lab & International Human Rights Program, University of Toronto, 2020).
11. See generally Bernard E Harcourt, *Against Prediction: Profiling, Policing and Punishing in an Actuarial Age* (University of Chicago Press, 2013).

who are falsely classified as (potential) criminals or members of a gang.[12] The probabilistic nature of statistical reasoning and its focus on correlation rather than on an understanding of cause or motive means that, *by design*, it targets people without the need to articulate any grounds of suspicion. Privacy rights are also implicated, which is particularly important in the context of the *Canadian Charter of Rights and Freedoms*.[13] Reliance on faulty predictions may also lead to unreasonable searches and seizures.[14]

While there are concerns about *all* police intelligence practices, there is increasing apprehension about new techniques involving algorithmic prediction and more intense surveillance.[15] The use of social media as a data source for social network analysis or social media analytics places large groups under surveillance without a specific law enforcement justification.[16] Clearview AI is often used without authorization (or even awareness) of senior leadership, and its usage may indirectly implicate the police in breaches of copyright law.[17] More broadly, some uses of algorithmic surveillance technologies, which automate the systematic collection and processing of data, might fall outside of police powers or infringe human rights protections.[18] The use of predictive policing software can have a discriminatory impact on racialized neighbourhoods, and in Australia, the Suspect Targeted Management Program was found to subject young indigenous Australians to inappropriate forms of over-policing with insufficient transparency

12. See Hannah Bloch-Wehba, "Visible Policing: Technology, Transparency and Democratic Control" (2021) 109 Cal L Rev 917. See also Vicki Sentas & Camilla Pandolfini, *Policing Young People in NSW: A Study of the Suspect Targeting Management Plan* (Youth Justice Coalition, 2017).
13. Part I of the *Constitution Act*, *1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Canadian Charter*]. See Robertson, Khoo & Song, *supra* note 10.
14. See Singh, *supra* note 9.
15. *Ibid*.
16. In Australia, see Lyria Bennett Moses et al, *Using "Open Source" Data and Information for Defence, National Security and Law Enforcement: Legal Report (Report A)* (Data to Decisions CRC & University of New South Wales Sydney, 2018). In Canada, see Robertson, Khoo & Song, *supra* note 10 at 77, citing *R v Spencer*, 2014 SCC 43 at paras 38-50.
17. See Jake Goldenfein, "Australian Police are Using the Clearview AI Facial Recognition System with No Accountability," *The Conversation* (3 March 2020), online: <theconversation.com/australian-police-are-using-the-clearview-ai-facial-recognition-system-with-no-accountability-132667> [perma.cc/5QH2-QHYD]; Monique Mann & Marcus Smith, "Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight" (2017) 40 UNSWLJ 121; Teresa Scassa, "How Clearview AI Could Violate Copyright Law" (10 March 2020), online: *Centre for International Governance Innovation* <www.cigionline.org/articles/how-clearview-ai-could-violate-copyright-law> [perma.cc/EGM8-CQPB].
18. See generally Robertson, Khoo & Song, *supra* note 10.

and oversight.[19] Police increasingly act as "knowledge brokers," sharing information with private security firms and insurance companies,[20] sometimes in ways that circumvent the chain of command and secrecy laws.[21]

As is evident from the nature of these concerns, many involve apprehension that police intelligence practices fail to comply with the law.[22] This includes privacy or data protection laws, but also limits on police powers and warrant requirements. General critiques of intelligence practices, while important, often lack access to sufficient detail to make a full assessment of the legality of particular activities.[23] For example, it is difficult to say whether the surveillance being conducted is always done within legal constraints due to secrecy around methods and practices. It is therefore essential that, like other police activities, oversight mechanisms exist to assure that intelligence practices (including methods for identifying suspects, assessing risk associated with people and places, and monitoring communities) operate within legal parameters.[24] Such oversight mechanisms need to capture both maverick and systemic non-compliance.

Oversight of police intelligence practices raises distinct issues from oversight of policing more generally. Whereas police violence may be experienced directly by individuals who can, in a well-designed system, engage with complaint processes, harms related to non-compliant intelligence practices are often invisible. People are often unaware that their social media feeds are being analyzed,[25] that they are appearing in virtual face recognition lineups,[26] that an image of them at a protest has been captured and analyzed, or that their encounters with police are the result of data-driven predictive models. Surveillance regimes, both general and

19. See Sentas & Pandolfini, *supra* note 12.
20. Richard V Ericson & Kevin D Haggerty, *Policing the Risk Society* (University of Toronto Press, 1997) at 200, 424.
21. See Mia Hartmann, "Grey Zone Creativity" in Nicolas Fyfe, Helene Gundhus & Kira Vrist Rønn, eds, *Moral Issues in Intelligence-Led Policing* (Routledge, 2018) 161 at 163.
22. Legality is an essential component of security. See Peter Gill, "Not Just Joining the Dots But Crossing the Borders and Bridging the Voids: Constructing Security Networks after 11 September 2001" (2005) 16 Policing & Society 27 at 4142.
23. See Robertson, Khoo & Song, *supra* note 10; Sentas & Pandolfini, *supra* note 12.
24. For the purposes of this article, oversight includes review. In Canada, review describes assessment of the activities of an organization against standards such as lawfulness and propriety, whereas oversight implies a more direct role in management. See Canada, Commission of Inquiry in the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Minister of Public Works and Government Services Canada, 2006) at 499-500 [Arar Report: Policy Report].
25. See Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (New York University Press, 2017) at 114.
26. *Ibid* at 89.

particular, often remain undisclosed.[27] Because of secrecy around police tactics, operations, and strategy, oversight of intelligence needs to go beyond reactive, complaints-based approaches that assume sufficient awareness among members of the public.[28] Further, holistic approaches that go beyond single incidents and bad cops to explore systemic issues in governance and policy are essential.[29] Only oversight that includes independent investigations in the absence of public complaints can provide assurance that police intelligence practices are lawful.[30] Further, such oversight must come with access to otherwise secret information about police intelligence practices and expertise, to sufficiently understand them and assess their legality.

In the three countries examined (Australia, Canada, and New Zealand), the oversight of law enforcement intelligence is spread among a variety of entities, including professional standards units, independent police and public sector oversight bodies, intelligence oversight (at the federal level in Canada and Australia), and privacy regulators. Other bodies also play an important role in the legal accountability of police intelligence, including courts (as issuers of warrants, arbiters of admissibility of evidence, and adjudicators of civil and criminal cases against police officers), political entities (such as parliamentary committees, responsible ministers, and police review boards), and other organizations with whom law enforcement interact. In addition, on an ad hoc basis, police may be called on to provide accounts of intelligence practices to inquiries, royal commissions, project-based bodies, and human rights commissions. Each of these oversight mechanisms has important limitations, so the volume of oversight alone does not of itself indicate comprehensiveness.[31] Indeed, the complexity of oversight arrangements can itself be a problem if entities collectively lack sufficient

---

27. See *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*, UNGAOR, 27th Sess, UN Doc A/HRC/27/37 (2014) [UNHCR, *The Right to Privacy in the Digital Age*].
28. See Garth den Heyer & Alan Beckley, "Police Independent Oversight in Australia and New Zealand" (2013) 14 Police Practice & Research 130.
29. See Andrew Goldsmith, "The Pursuit of Police Integrity: Leadership and Governance Dimensions" (2001) 13 CICJ 185 at 197 [Goldsmith, "Police Integrity"]. See also Janet Chan, *Changing Police Culture* (Cambridge University Press, 1997). *Contra* Frank Harris, "Holding Police Accountability Theory to Account" (2012) 6 Policing 240.
30. See generally Lyria Bennett Moses & Louis De Koker, "Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data by National Security and Law Enforcement Agencies" (2017) 41 Melbourne UL Rev 561.
31. See Janet Chan, "Governing Police Practice: Limits of the New Accountability" (1999) 50 British J Sociology 251 at 259 [Chan, "Governing Police Practice"].

expertise, power, and access to oversee all relevant activities,[32] or where complexity leads to contradictory interpretations of requirements and, hence, competing demands.[33] It thus remains important to analyze whether these arrangements *can* collectively assure the legality of law enforcement intelligence practice.

There is literature in the United States that points to a potential gap in oversight for police intelligence. In 2013, Samuel J. Rascoff observed that there was a "formal governance vacuum" in the oversight of local law enforcement agencies' increasing involvement in "true" intelligence work.[34] This echoes a similar complaint about the regulation and oversight of US crime intelligence systems in 1976, which led to the recommendation for the appointment of a privacy auditor and for the involvement of the courts through criminal and civil penalties for breach.[35] The oversight gap has been said to be caused by the expanded intelligence role that local police agencies took on after 11 September 2001, despite not falling within federal-level intelligence oversight regimes.[36] More recent literature points to a lack of transparency, made more acute due to newer surveillance techniques, as a source of a potential reduction in democratic, public, and political accountability.[37] There is no similar analysis in Canada, Australia, or New Zealand.

This article analyzes the jurisdiction, function, powers, and expertise of oversight mechanisms with reference to *capacity* to oversee the legality of police intelligence practices in Canada, Australia, and New Zealand.[38] It is *not* a study of effectiveness, for which reference would need to be made to, *inter alia*, political

---

32. In the United Kingdom, see generally Kiron Reid, "Current Developments in Police Accountability" (2002) 66 J Crim L 172.
33. See generally Tobias T Gibson, "Multiple Principals and the (Lack of) Intelligence Oversight" (2017) 5 National Security LJ 239; Patrick Cronin & Stephen Reicher, "Accountability Processes and Group Dynamics: A SIDE Perspective on the Policing of an Anti-Capitalist Riot" (2009) 39 European J Soc Psychology 237.
34. See "The Law of Homegrown (Counter) Terrorism" (2010) 88 Tex L Rev 1715 at 1740-42. See also Samuel J Rascoff, "Domesticating Intelligence" (2010) 83 S Cal L Rev 575 at 583, 586.
35. See Howard L Draper, "Privacy and Police Intelligence Data Banks: A Proposal to Create a State Organized Crime Intelligence System and to Regulate the Use of Criminal Intelligence Information" (1976) 14 Harv J on Legis 1 at 72-73, 107.
36. See generally Benjamin S Mishkin, "Filling the Oversight Gap: The Case for Local Intelligence Oversight" (2013) 88 NYU L Rev 1414.
37. See Bloch-Wehba, *supra* note 12.
38. See also Philip C Stenning, "Evaluating Police Complaints Legislation: A Suggested Framework" [Stenning, "Evaluating Police Complaints Legislation"] in Andrew Goldsmith & Colleeen Lewis, eds, *Civilian Oversight of Policing* (Hart Publishing, 2000) 147.

support and funding,[39] adoption rate of recommendations,[40] susceptibility to capture,[41] responsiveness and timeliness, and membership.[42] Rather, this article asks about whether existing oversight institutions in Canada, Australia, and New Zealand *can* (if operating well) oversee police intelligence practices and analyzes how they might learn from each other to improve institutional arrangements.

I. METHODOLOGY AND OUTLINE

The article uses a mixed methods approach, linking doctrinal study of the arrangements for police intelligence oversight in each country, including examples from states, territories, and provinces in Australia and Canada, with an empirical examination of the understanding of oversight arrangements from the perspective of police in each country. For the latter, it draws on a broader qualitative empirical study using interview data from policing intelligence analysts, intelligence managers, lawyers, and information technology (IT) professionals. The broader study was carried out in three stages. In stage one, we conducted a systematic literature review of international literature on police intelligence practices. This review included 264 peer-reviewed articles examining police intelligence practices from 1979–2019. In stage two, we conducted a document and policy analysis of organizational and government documents from all three countries (documents ranged from 2009–2019). This included review of legal statutes, case law, policy statements, official reports, and internal police documents. This material was updated subsequently as new legislation was passed and new events occurred, but the systematic review was not repeated. No updates were made after 25 November 2022. Finally, stage three consisted of in-depth interviews (n=60) with police intelligence practitioners in Australia, Canada, and New Zealand. Interviews with practitioners in Australia (n=22) were conducted from November 2018 to October 2019 and included nine

39. See Colleen Lewis, "The Politics of Civilian Oversight: Serious Commitment or Lip Service?" in Goldsmith & Lewis, eds, *supra* note 38, 19 at 30-35.
40. See Louise E Porter, "Beyond 'Oversight': A Problem-Oriented Approach to Police Reform" (2013) 14 Police Practice & Research 169; Arar Report: Policy Report, *supra* note 24 at 543-45, 555-56.
41. See Tim Prenzler, "Civilian Oversight of Police" (2000) 40 Brit J Crim 659 [Prenzler, "Civilian Oversight"].
42. See Stephen P Savage, "Seeking 'Civilianness': Police Complaints and the Civilian Control Model of Oversight" (2013) 53 Brit J Crim 886; Barbara Attard, "Oversight of Law Enforcement is Beneficial and Needed - Both and Out" (2010) 30 Pace L Rev 1548; Lewis, *supra* note 39.

crime/intelligence analysts and thirteen managers/administrators from five police departments. Interviews with Canadian practitioners (n=18) were conducted from July 2018 to December 2018 and included six crime/intelligence analysts, five intelligence supervisors/managers, four police managers/administrators, two intelligence officers, and one in-house lawyer from seven police departments. Interviews with practitioners in New Zealand (n=20) were conducted from December 2018 to April 2019 and included ten crime/intelligence analysts/support staff, seven managers/administrators, and three field intelligence officers from one police department (as there is only one nationalized public policing body in New Zealand).

Interview guides were collaboratively constructed based on our systematic literature review and document and policy analysis. From these, we identified a number of key areas requiring further exploration based on existing knowledge, including how police practitioners define and understand intelligence, the implementation and use of technology for intelligence work, and the oversight of police intelligence. University Research Ethics Board approval was secured in all three countries prior to data collection. Interview data was digitally recorded and transcribed verbatim with all identifying material anonymized. Data was catalogued and coded in the NVivo qualitative data analysis software program. During initial coding, all data was coded thematically into thirty-eight large bucket codes derived from the key areas of interest identified in the systematic literature review, which informed the interview questions. For this component of the study, the bucket codes used were ethics, quality assurance, feedback and review, governance/accountability/oversight, measuring success, open source, policy/legal, risk, and role of managers/supervisors. This process is in line with constructivist grounded theory analysis, during which existing conceptual frames are used to inform the categorization and interpretation of data for further analysis.[43] One research assistant completed initial coding for all three countries in order to ensure consistency. After initial coding into large thematic buckets, the coded NVivo data set was shared with the entire team for review. Regular team meetings were held to discuss coding and to validate findings through investigator triangulation.[44] From here, members of the research team divided responsibilities for closer inquiry based on their respective areas of academic specialization. This

43. See Virginia Braun & Victoria Clarke, "Using Thematic Analysis in Psychology" (2006) 3 Qualitative Research in Psychology 77; Kathy Charmaz, *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis* (SAGE Publications, 2006).
44. See generally Norman Denzin, *The Research Act: A Theoretical Introduction to Sociological Methods*, 3rd ed (Prentice Hall, 1989).

author focused on oversight. This inquiry looked at three dimensions—oversight bodies (mirroring the structure of this article), perceptions of oversight (first-hand and second-hand), and impact of oversight on practice, creating more specific and focused coding to capture themes emerging from the analysis. Regular team meetings continued throughout the focused coding and analysis process, during which research team members could review their emerging findings with the team to ensure inter-coder reliability.[45]

Interviewees are labelled throughout with a country code (AU for Australia, NZ for New Zealand, CA for Canada, and their assigned number; for example, AU01). While this project does not include interviews with those working in oversight agencies or with the general public (in relation to their perceptions of oversight), it does yield some important comparative insights that can be explored in future work.

The goal of examining three countries simultaneously is to enable cross-jurisdictional learning; for example, as to whether New Zealand should bring law enforcement under intelligence oversight as is the case in Canada and Australia. The choice of jurisdictions is based on similarities in the range of oversight mechanisms deployed, which is useful when seeking policy insights.[46] All jurisdictions have civilian oversight of police, either specifically or as an aspect of a broader regime. All jurisdictions have privacy laws that are overseen by a privacy commissioner or similar. Canada's and Australia's oversight of intelligence includes law enforcement agencies. All have responsible government, with government ministers responsible to parliament and reliance on parliamentary committees for oversight. Canada and Australia were both described in 1994 as the only jurisdictions with truly independent police oversight.[47] In none of the jurisdictions considered is there an agency whose mission focuses exclusively on oversight of police intelligence. Indeed, the intelligence function may not even be mentioned explicitly in lists of functions and powers of police. This gap is particularly evident in the New Zealand Police's *Code of Conduct*, which does

45. See Carrie B Sanders & Carl J Cuneo, "Social Reliability in Qualitative Team Research" (2010) 44 Sociology 325.
46. See Lars Westfelt & Felipe Estrada, "International Crime Trends: Sources of Comparative Crime Data and Post-War Trends in Western Europe" in James Sheptycki & Ali Wardak, eds, *Transnational and Comparative Criminology* (GlassHouse Press, 2005) 19 at 19-20.
47. See David Landa, "Foreword" in David Moore & Roger Wettenhall, eds, *Keeping the Peace: Police Accountability and Oversight* (University of Canberra & Royal Institute of Public Administration Australia, 1994) vii.

not mention intelligence work, although it does discuss information handling.[48] However, it is also important to recognize differences. Only Australia and Canada have a federal system. Thus, New Zealand has a national police force; Australia has federal, state, and territory police forces; and Canada has provincial and municipal police as well as the federal Royal Canadian Mounted Police (RCMP). The relationships between the police and political authorities have some commonalities, but also important differences.[49] All of the agencies studied have the power to conduct intelligence; in South Australia this must be linked to an investigation.[50]

After describing the meaning of oversight and its relationship to accountability (Part II), the article launches into a comparative study of the various entities involved. Entities that have a statutory role in overseeing police intelligence activities are discussed in Part III, whereas those whose oversight role is less direct are discussed in Part IV. Part V looks at the role of transparency as an enabler of oversight and the particular role of the media in bringing awareness to intelligence practices. Part VI concludes with recommendations for reform of oversight arrangements for police intelligence in Canada, Australia, and New Zealand.

II. WHAT IS OVERSIGHT?

Oversight is closely linked to the concept of accountability. Accountability refers to "the right of the account-holder to investigate and scrutinise the actions of the agent by seeking information and explanations and the right to impose remedies and sanctions."[51] In this case, the agent can be an entire organization, such as a police agency.[52] Accountability mechanisms are separate from the laws that define agencies' powers or regulate their conduct, although many accountability

48. See New Zealand Police, *Code of Conduct* (2022) at 7, in force under *Policing Act 2008* (NZ), 2008/72, s 20.
49. See Philip Stenning, "The Idea of Political 'Independence' of the Police: International Interpretations and Experiences" [Stenning, "Political Independence"] in Margaret E Beare & Tonita Murray, eds, Police *and Government Relations: Who's Calling the Shots?* (University of Toronto Press, 2007) 183 at 183.
50. See Police Act 1998 (SA), 1998/55 [Police Act 1998]; AU09.
51. See Richard Mulgan, *Holding Power to Account: Accountability in Modern Democracies* (Palgrave Macmillan, 2003) at 10. This is similar to the definition that Chan offers in the specific context of policing. "Governing Police Practice, " *supra* note 31 at 253.
52. *Contra* Jean-Paul Brodeur, "Accountability: The Search for a Theoretical Framework" [Brodeur, "Accountability"] in Errol P Mendes et al, eds, *Democratic Policing and Accountability: Global Perspectives* (Ashgate, 1999) 125 at 152, 157 (suggesting that organizational agents are the primary focus of accountability).

mechanisms are formally established in law.[53] Accountability is not the same as pressure, such as that which might be exercised by organized interest groups.[54] Instead, it comprises mechanisms that make particular individuals or organizations answerable in particular ways to particular entities for particular purposes, including but not limited to legal compliance.[55] It is also not the same as control; an oversight agency may not have the power to ensure that the overseen agency acts, or refrains from acting, in particular ways.[56] There are different models of accountability (often grafted together), including "old" models that emphasize sanctions for breaches of rules and "new" models that emphasize managerial techniques (such as risk management, audit, and performance indicators).[57]

While taxonomies of accountability are contested, the focus here is on accountability that relates to *legal* compliance.[58] This is one strand of accountability that, in the context of policing, could also include operating efficiency, hiring, promotion and discipline policies, and fiscal management.[59] Ethics is also a separate issue from legality,[60] although judges and oversight agencies sometimes point out ethical failings. Some entities play a role in legal accountability, although this is not their primary objective. For example, while ministers and parliamentary committees ensure mostly *political* accountability, they can also play a role in interrogating the legality of actions of agencies for which they are responsible. Thus, while a variety of entities are considered (particularly in Part IV), the focus here is on the role they play in the assurance of the legality of police intelligence practices.

Accountability is particularly important for policing because the public delegates significant power to the police, including the power to keep secrets from the public, yet needs to ensure that police act within the law and in the

53. See Mulgan, *supra* note 51 at 20.
54. *Ibid*.
55. See Janina Boughey & Greg Weeks, "Government Accountability as a 'Constitutional Value'" in Rosalind Dixon, ed, *Australian Constitutional Values* (Hart Publishing, 2018) 99 at 102; Mulgan, *supra* note 51 at 22-23.
56. See Stenning, "Political Independence," *supra* note 49 at 185.
57. See Chan, "Governing Police Practice," *supra* note 31.
58. See Jerry L Mashaw, "Accountability and Institutional Design: Some Thoughts on the Grammar of Governance" in Michael Dowdle, ed, *Public Accountability: Designs, Dilemmas and Experiences* (Cambridge University Press, 2006) 115 at 120.
59. See Andrew Goldsmith, "Necessary but Not Sufficient: The Role of Public Complaints Procedures in Police Accountability" in Philip C Stenning, ed, *Accountability for Criminal Justice: Selected Essays* (University of Toronto Press, 1995) 110 at 112.
60. See Kira Vrist Rønn, "The Professional Ethics of Intelligence" in Fyfe, Gundhus & Vrist Rønn, eds, *supra* note 21, 121 at 126.

public interest, in line with the Peel Principles.[61] While people do not have a right to know operational secrets, and police have a legal obligation to withhold certain information,[62] the public does have a right to demand accountability, including through independent oversight.[63] Accountability is particularly important due to the range of powers, ability to impact personal and community freedoms, and extent of discretion held by the police.[64] The intelligence context adds to, rather than subtracts from, the need for accountability, as articulated by the 2017 Independent Intelligence Review in Australia:

> A critical element of this 'state of trust' is the understanding that agencies provide intelligence which contributes to safeguarding national interests and the lives of citizens and that, in doing so, those agencies act with propriety, legality and proportionality, are responsive to Ministerial direction and control, and are accountable for their activities.[65]

A similar view is expressed in the preamble to the *National Security Act, 2017* in Canada.[66] The United Nations High Commissioner for Human Rights has also emphasized the importance of independent oversight in ensuring accountability for intrusions on the right to privacy in the context of state surveillance.[67] New data and surveillance technologies enhance the importance of accountability.[68]

---

61. On the principal–agent problem, see generally Mulgan, *supra* note 51. On accountability, see Attard, *supra* note 42 at 1548; Petter Gottschalk, *Knowledge Management in Police Oversight: Law Enforcement Integrity and Accountability* (Brown Walker Press, 2009) at 14-15. See also United Nations Office on Drugs and Crime, *Handbook on Police Accountability, Oversight and Integrity* (UN, 2011) at 5.
62. See *e.g. Police Act 1998*, *supra* note 50, s 74A.
63. See Bennett Moses & De Koker, *supra* note 30. See also Tony Plaff & Jeffrey Tiel, "The Ethics of Espionage" (2004) 3 J Military Ethics 1 at 12.
64. See Mary Seneviratne, "Policing the Police in the United Kingdom" (2004) 14 Policing & Society 329 at 330.
65. Austl, Commonwealth, Department of Prime Minister & Cabinet, *2017 Independent Intelligence Review* (DPMC, 2017) at 111 [*2017 Independent Intelligence Review*].
66. SC 2019, c 13, Preamble ("Whereas enhanced accountability and transparency are vital to ensuring public trust and confidence in Government of Canada institutions that carry out national security or intelligence activities").
67. See UNHCR, *The Right to Privacy in the Digital Age*, *supra* note 27 at 37.
68. See Ferguson, *supra* note 25 ("[t]he architecture of surveillance also needs an architecture of accountability" at 201).

Accountability is a broader concept than oversight,[69] but independent oversight is a crucial component of accountability.[70] In particular, of the five dimensions of accountability (who, for what, to whom, how, and according to what criteria),[71] oversight directs attention on *to whom*, although other dimensions continue to play a role in understanding the nature of that oversight. While this article includes some discussion of internal processes for ensuring legality, oversight should be linked to independent, external institutions.[72] In particular, independent oversight is crucial to avoid real or perceived bias in favour of police.[73] Oversight can be both vertical (with a clear hierarchy) or horizontal (where agencies are accountable to each other).

A study of oversight is different from, but not completely independent of, a study of the *rules* that govern police intelligence practice. While police powers are often articulated broadly, intelligence analysts are constrained (depending on jurisdiction) by constitutional law; human rights requirements; procedural requirements; rules about access to and disclosure of information; the scope of a policing organization's functions, purposes, and jurisdiction; and rules regarding behaviour and conduct of officers. Investigative processes may also take account of rules of evidence where intelligence relates to a specific investigation. Rules governing police intelligence are often complex, requiring police to navigate a range of legislation.[74] This complexity, alongside open-ended and sometimes unclear rules that can be worked around, may have an impact on compliance and the ability (and interest) of oversight bodies to hold police to account, including through allocation of responsibility and imposition of sanctions.[75] A comparison of oversight mechanisms thus requires awareness of the rules as a

69. See Gottschalk, *supra* note 61 at 15; Samuel Walker, "Police Accountability: Current Issues and Research Needs" (Paper presented at Policing Research Workshop: Planning for the Future, National Institute of Justice, 28-29 November 2006) [unpublished].
70. See Goldsmith, "Police Integrity," *supra* note 29 at 199; David H Bayley, "Preface" in Andrew Goldsmith, ed, *Complaints against the Police: The Trend to External Review* (Clarendon Press, 1991) v at ix-xi.
71. See Mashaw, *supra* note 58 at 117-18.
72. See Stenning, "Evaluating Police Complaints Legislation," *supra* note 38 at 158.
73. See Tim Prenzler, "Scandal, Inquiry, and Reform: The Evolving Locus of Responsibility for Police Integrity" in Tim Prenzler & Garth den Heyer, eds, *Civilian Oversight of Police: Advancing Accountability in Law Enforcement* (CRC Press, 2016) 3 at 6; Prenzler, "Civilian Oversight," *supra* note 41; Andrew Goldsmith, "Better Policing, More Human Rights: Lessons from Civilian Oversight" in Mendes et al, eds, *supra* note 52, 33 at 35.
74. See Lyria Bennett Moses, "Who Owns Information? Law Enforcement Information Sharing as a Case Study in Conceptual Confusion" (2020) 43 UNSWLJ 615.
75. Chan, "Governing Police Practice," *supra* note 31 at 262-63.

crucial context for that oversight, but does not require a full comparative analysis of the rules themselves. While rules that bind police in different jurisdictions will vary, the importance of mechanisms that ensure compliance with those rules applies universally.

III. OVERSIGHT UNITS AND AGENCIES

This Part focuses on institutions, or units within institutions, for whom oversight of police intelligence is part of an explicit mandate. It begins in Part III(A) with a discussion of internal oversight through professional standards units. Part III(B) explores the role of institutions with responsibility for oversight of police activities broadly in the specific context of police intelligence. Part III(C), conversely, considers institutions responsible for overseeing intelligence practices and the extent to which their jurisdiction extends to police, as opposed to security agencies. Part III(D) focuses on the role of privacy commissioners or regulators in overseeing compliance with that particular rule set, given its particular importance to police intelligence. Part III(E) provides some examples of ad hoc oversight, where a temporary body is established to look into a particular event or issue.

A. INTERNAL OVERSIGHT

In addition to supervision through the chain of command, most police agencies have a professional standards unit. Depending on the jurisdiction, this unit may respond to complaints, conduct audits, emphasize lawfulness as an aspect of culture (through training, guidance, et cetera), or engage in other compliance-focused activities.

Professional standards units and senior leaders have a role in developing an internal culture that values legal compliance. Mechanisms for this include providing advice,[76] anticipating problems,[77] and vetting officers.[78] Internal oversight is often overseen by or conducted in cooperation with independent external bodies, which engage in cross-referral and provision of information.[79] While internal oversight does not replace the need for external, independent oversight, it can be effective, particularly as police may be less likely to close ranks to hinder an internal process.

76. AU03.
77. CA04.
78. AU21.
79. AU08; AU16; AU21.

Auditing is an important element of internal oversight, particularly in Australia and New Zealand.[80] Numerous Australian and New Zealand participants described a system whereby all database access is tracked, with everyone responsible for keeping track of the reasons for each access (which they may be required to recount in random or targeted audits). Participants also gave examples of red flags placed on people who searched for themselves, their neighbours, famous people, or persons with the same name.[81] Auditing is sometimes used to ensure data deletion rules are complied with,[82] but may be incomplete with respect to intelligence work more broadly.[83] It is also possible that audits go nowhere; one interviewee stated, "I've been audited by external auditors before about my processes but never heard the outcome."[84] Interestingly, auditing was not mentioned by Canadian participants, except for one who referred to it quite loosely and one who identified it as a difference between the police agencies he had worked for in Canada and Australia:

> We do have general oversight of auditing of what people are doing within the police service.[85]

> I think there's even no auditing…[In Australia], once a year, you'd get an audit and there'd be this print-out, here's every single check you've done every car you've looked up, every address, every name, it's all there for a year. And we know it's you because when you log-in it's whatever and I'm like yep cool and they highlight 15 random and they say you explain why you looked up these criteria and so when you start like on your first day they say here's a notebook every time you go into [the police database, COPS] write down who you looked up and make some note that you can understand as to why you did that…[In Canada] I have not had any audit on any database I've used so like justify why did you look up this person.…I think would it be easy to slip a check on your neighbour? Absolutely.[86]

Other technological controls can also play a role alongside auditing to hard wire compliance, particularly with respect to rules relating to access and dissemination:

---

80. AU01; AU05; AU06; AU07; AU08; AU09; AU11; AU12; AU13; AU14; AU17; AU18; AU21; NZ01; NZ02; NZ06; NZ09; NZ10; NZ12; NZ15; NZ16; NZ17.
81. AU09; AU11; NZ17.
82. AU12.
83. AU03.
84. AU20.
85. CA15 (Patrol Analyst).
86. CA02 (Intelligence Analyst).

> [Y]ou can design out non-compliance where people forget to do something because you can wire the business process and the policy into the system.[87]
>
> [T]here's checks and balances even for most of our systems that you log into, warnings come up, talk[ing] about the disclosure could be a criminal offense outside of your work duties.[88]
>
> [W]e needed permission to put in a work request to get access to a database.[89]
>
> There's folders that are locked down, there's a lot of stuff that we lock down. So that only those who need to know, know. I can't just go willy-nilly one day and go look up every flatmate I've ever lived with and find out where they are now.[90]

While one can design systems to encourage compliance, this does not guarantee that there are no ways around the system or that compliance will be perfect. A Field Intelligence Officer stated, "The good thing is that it's actually locked-down, so you can't bring that up in a Business Objects search, it has been locked-down by IT. But there are ways to find them, if you know how."[91]

Internal mechanisms described above are useful in the "bad cop" scenario, but less useful where the illegality is institutional. Internal oversight mechanisms cannot be sufficient in the context of policing, and their success in making intelligence practices accountable is further contingent on how well they are done. For example, internal oversight relies on expertise on the rules around intelligence that may be lacking at senior levels.[92] Nevertheless, internal accountability processes, particularly tracking usage of databases combined with regular compliance audits, can identify some forms of misconduct. Canadian police agencies that are not already auditing the use of information systems could learn from the Australian and New Zealand approaches here.

B. OVERSIGHT OF POLICE AGENCIES AND OFFICERS

Police oversight is generally justified in terms of concerns about misconduct and corruption and has, historically, often originated in response to the revelations of inquiries and reviews.[93] In this Part, the focus is on independent bodies with oversight over the activities of a police agency but excludes police service boards,

87. AU03 (Manager).
88. AU21 (Manager).
89. CA09 (Intelligence Analyst).
90. NZ06 (Lead Intelligence Analyst).
91. NZ09.
92. NZ04; CA07.
93. See Tim Prenzler & Carol Ronken, "Models of Police Oversight: A Critique" (2001) 11 Policing & Society 151 at 152-56.

which are discussed together with political actors below. There are a variety of such bodies in the jurisdictions examined, sometimes with broader jurisdiction that covers the public service more broadly.

Due to the complexity and diversity of arrangements in different jurisdictions, it is not possible to provide a comprehensive picture. However, this Part will provide examples of arrangements that do and do not provide sufficient coverage of police intelligence oversight. The test is whether there is at least one oversight body with jurisdiction, power, and expertise to investigate the legality of intelligence practices (such as the use of facial recognition, social media analytics, or predictive policing). Such a body would need to have power over civilian employees as well as sworn officers, at least in jurisdictions where intelligence work is primarily done by civilians.

A purely complaints-based jurisdiction is not likely to be sufficient. This is for two reasons. First, while it is possible for a complaint to lead to a broader policy review, that would rarely be the primary objective of a complaints process.[94] Complaints processes are necessarily reactive.[95] This is particularly so where the complaints form focuses on a specific incident.[96] As a Commission of Inquiry in Canada noted, complaints-driven oversight does "not recognize that people may be harmed by conduct that stems, not from intentional or individual misconduct, but from inadequate systemic and organizational controls."[97] This is particularly so for police intelligence systems and processes that are generally invisible to those interacting with police. Second, intelligence operations are generally secret, so that not even those interacting with police are aware of the

94. See generally Graham Smith, "Rethinking Police Complaints" (2004) 44 Brit J Crim 15 [Smith, "Rethinking"].criminal conduct, tortious action and unacceptable policyand four functions are consideredmanagerial, liability, restorative and accountability. It is concluded that in order to effectively and efficiently deal with the various causes of complaint, a two-tier system is required to deal with complaints that allege unprofessional behaviour and criminal conduct, and a third, separate tier, is necessary to consider complaints regarding unacceptable police policy.","container-title":"The British Journal of Criminology","DOI":"10.1093/bjc/44.1.15","ISSN":"0007-0955","issue":"1","page":"15-33","title":"Rethinking Police Complaints","volume":"44","author":[{"family":"Smith","given":"Graham"}],"issued":{"date-parts":[["2004"]]}}],"schema":"https://github.com/citation-style-language/schema/raw/master/csl-citation.json"}

95. See David Brereton, "Evaluating the Performance of External Oversight Bodies" in Goldsmith & Lewis, eds, *supra* note 38, 105 at 118-19.

96. An example of this narrow focus is the complaints form for the Independent Police Conduct Authority in New Zealand. See "Complaint to the Independent Police Conduct Authority," online (pdf): *IPCA* <www.ipca.govt.nz/includes/download.ashx?ID=155622> [perma.cc/3LQT-XEP4] ["Complaint to IPCA"].

97. Arar Report: Policy Report, *supra* note 24 at 486.

impact of intelligence programs such as predictive policing or social media monitoring on those interactions, so complaints *about intelligence practices* will be rare.[98] An example is the variability in suburb-by-suburb targets for search warrants in New South Wales (NSW), Australia—based on public information, it would be difficult for an individual to know whether the racial makeup of their suburb was a factor in the issuance of a search warrant against them.[99]

The Civilian Review and Complaints Commission (CRCC) in Canada has relatively comprehensive oversight over the relevant police service, the RCMP.[100] The CRCC has the power to initiate investigations without a complaint, including reviewing police programs beyond individual misconduct.[101] This has been used, for instance, where the CRCC investigated the RCMP's bias-free policing model.[102] There is also the possibility of joint investigations between federal and provincial oversight bodies,[103] which is particularly important given that the RCMP undertakes some municipal and provincial policing under contract.[104] While the CRCC's access to privileged information necessary to review the RCMP's national security activities is limited,[105] that would come under the purview of the National Security and Intelligence Review Agency (NSIRA), discussed in the following Part. An important limitation of the CRCC's oversight in the context of complaints is that it cannot be used to make conduct complaints about civilian staff.[106]

The arrangements in Canadian provinces are far more complex, and each province is different in terms of the structure of policing (potentially including the RCMP, provincial police, municipal police, and First Nations police). For example, Ontario previously had three relevant entities:[107] (1) The Office

98. *Ibid*.
99. See Angus Thompson & Pallavi Singhal, "Revealed: The Suburb-by-Suburb Targets NSW Police Use to Reach Crime Detection Goals," *The Sydney Morning Herald* (28 June 2020), online: <www.smh.com.au/national/nsw/revealed-the-suburb-by-suburb-targets-nsw-police-use-to-reach-crime-detection-goals-20200625-p5566a.html> [perma.cc/Z946-LKK8].
100. See *Royal Canadian Mounted Police Act*, RSC 1985, c R-10, ss 45.29-45.78 [*RCMP Act*].
101. *Ibid*, ss 45.34-45.35.
102. See Canada, Civilian Review and Complaints Commission for the RCMP, *Review of the RCMP's Bias-Free Policing Model* (30 March 2022), online: <www.crcc-ccetp.gc.ca/en/review-rcmps-bias-free-policing-model-report> [perma.cc/T75A-X5BH].
103. See *RCMP Act*, *supra* note 100, s 45.75.
104. See *e.g.* British Columbia, "Policing Agreements," online: <www2.gov.bc.ca/gov/content/justice/criminal-justice/policing-in-bc/publications-statistics-legislation/publications/policing-agreements> [perma.cc/E3BF-MERU].
105. See *RCMP Act*, *supra* note 100, s 45.4.
106. *Ibid*, ss 10, 45.53(1).
107. See Police Services Act, RSO 1990, c P15, ss 21-26.9 [Police Services Act, 1990].

of the Independent Police Review Director received, managed, and oversaw public complaints about police and had related review powers; (2) The Ontario Civilian Police Commission heard appeals, adjudicated applications, conducted investigations, and resolved disputes about oversight and provision of policing services; and (3) The Special Investigations Unit's jurisdiction was confined to incidents involving police officers where there has been death, serious injury, or allegations of sexual assault, so is not directly relevant to intelligence practices.[108]

While the Office of the Independent Police Review Director had the power to conduct systemic reviews beyond the immediate issues raised by a given complaint or fault of an individual, these reviews only came into play in the context of complaints received.[109] In particular, the statutory obligation to review issues of a systemic nature only arose where they "are the subject of" or "give rise to" complaints.[110] This overcomes the first concern about reliance on complaints (that the oversight agency will not look beyond specific circumstances for broader, systemic issues) but not the second (that lack of awareness will prevent complaints being filed). Thus, while complaints led to an investigation on procedures for voluntary collection of DNA which requires a physical interaction with the target population,[111] this route may not be invoked for facial recognition tools that do not require such interaction, at least while public awareness is limited.

These arrangements were later changed to: (1) replace the Office of the Independent Police Review with the Law Enforcement Complaints Agency; (2) create a new Inspector General of Policing with responsibility for, *inter alia*, overseeing police service boards, chiefs of police, and police services to ensure compliance with the *Comprehensive Ontario Police Services Act, 2019* and *Community Safety and Policing Act, 2019* and dealing with systemic concerns; and (3) narrow the jurisdiction of the Special Investigations Unit to criminal matters. [112] The reforms eliminate the earlier gap in oversight, with the Law

108. See *Special Investigations Unit Act, 2018*, SO 2018, c 3, Sched 4, as repealed by *Special Investigations Unit Act, 2019*, SO 2019, c 1, Sched 5 [*Special Investigations Act*, 2019].
109. See *e.g.* Office of the Independent Police Review Director, "Systemic Reviews," online: <www.oiprd.on.ca/news/systemic-reviews> [perma.cc/3SCS-GLHQ].
110. *Police Services Act, 1990*, *supra* note 107, s 57.
111. See Gerry McNeilly, *Casting the Net: A Review of Ontario Provincial Police Practices for DNA Canvasses* (Office of the Independent Police Review Director, July 2016).
112. Comprehensive Ontario Police Services Act, 2019, SO 2019, c 1, ss 79-101, 130-46 [Community Safety and Policing Act, 2019]; Special Investigations Unit Act, 2019, *supra* note 108.

Enforcement Complaints Agency having powers to conduct investigations in the absence of a complaint.[113]

The situation in most Canadian provinces is similar to the previous position in Ontario, although there are exceptions. Alberta's Law Enforcement Review Board and Quebec's Commissaire à la Déontologie Policière have the power to conduct inquiries but only at the request of the relevant minister.[114] In Prince Edward Island, the minister has broad power to launch an investigation or direct the Police Commissioner to do so.[115] Manitoba's Police Commissioner has the power to investigate the conduct of an *extra-provincial* police officer in the absence of a complaint.[116] New Brunswick grants its Police Commission "own motion" powers to investigate any matter relating to any aspect of policing in any area of the province,[117] making it the only Canadian jurisdiction with full "own motion" powers to launch an investigation. Further, throughout Canada, conduct complaints cannot generally be made against civilian employees.[118]

Australia combines two approaches to law enforcement oversight—anti-corruption bodies as well as oversight or handling of complaints. In NSW, these separate roles are combined in one body, the Law Enforcement Conduct Commission, with extensive investigatory powers including with respect to agency conduct that is illegal, unjust, or improperly discriminatory.[119] Thus, it was able to investigate the NSW Police's Suspect Target Management Plan, which has been shown to disproportionately target Indigenous youth.[120]

Anti-corruption and integrity bodies exist in many Australian jurisdictions. The Australian Commission for Law Enforcement Integrity has strong investigatory powers in relation to corruption in the Australian Federal Police

---

113. *Community Safety and Policing Act, 2019*, *supra* note 112, s 161.
114. See *Police Act*, RSA 2000, c P-17, s 17 [Alberta *Police Act*]; *Police Act*, CQLR 2000, c P-13.1, s 128 [Quebec *Police Act*].
115. See *Police Act*, RSPEI 1988, c P-11.1, ss 4(1), 18(1) [PEI *Police Act*].
116. See *The Law Enforcement Review Act*, CCSM, c L75, s 7.2(1).
117. See *Police Act*, SNB 1977, c P-9.2, s 22(4)(a) [NB *Police Act*].
118. See *e.g.* Alberta *Police Act*, *supra* note 114, s 42.1(1); Quebec *Police Act*, *supra* note 114, s 143; PEI *Police Act*, *supra* note 115, ss 20(b), 21(1); *The Law Enforcement Review Act*, *supra* note 116, s 6(1); NB *Police Act*, *supra* note 117, s 1 (definition of "conduct complaint"); *Police Act*, RSBC 1996, c 367, s 78(1); *Royal Newfoundland Constabulary Act, 1992*, SNL 1992, c R-17, s 22(1); *Police Act*, SNS 2004, c 3, s 70; *Police Act, 1990*, SS 1990-91, c P-15.01, s 45. *Cf Community Safety and Policing Act, 2019*, *supra* note 112, s 107.
119. See *Law Enforcement Conduct Commission Act 2016* (Austl), 2016/61, ss 11, 51-97.
120. See Law Enforcement Conduct Commission, *Law Enforcement Conduct Commission Annual Report 2018-2019* (Law Enforcement Conduct Commission, 2019). See also Sentas & Pandolfini, *supra* note 12.

and Australian Criminal Intelligence Commission and has power to commence investigations in the absence of a specific complaint.[121] The situation is similar in Victoria.[122] In Tasmania and Western Australia, the Integrity Commission and the Corruption and Crime Commission, respectively, have a slightly wider scope, covering "improper behaviour" in Tasmania and unlawful, unreasonable, unjust, oppressive, or improperly discriminatory behaviour in Western Australia.[123] Bodies with wide anti-corruption powers beyond police agencies, such as Queensland's Crime and Corruption Commission, are not limited to sworn officers.

The ombudsman-based model of handing complaints against the police was long dominant in Australia.[124] Ombudsmen still have a role in handling complaints against police in the Commonwealth,[125] Northern Territory,[126] Tasmania,[127] and Western Australia (although in some jurisdictions this excludes operational matters).[128] In some jurisdictions, ombudsmen have "own motion" powers to initiate an investigation in the absence of a complaint and significant investigatory powers in the course of an investigation, including powers to enter premises, require a person to provide information, and examine witnesses.[129] Because ombudsmen have jurisdiction over the public service generally, they can handle complaints against civilians working in police agencies. In South Australia, the Office for Public Integrity oversees complaints against police, but does not have powers in relation to complaints against civilian employees of police agencies.[130] However, the primary challenge faced by ombudsmen in Australia is not jurisdiction, but rather a lack of resources.[131]

---

121. See *Law Enforcement Integrity Commissioner Act 2006* (Cth), 2006/85.
122. See *Independent Broad-based Anti-corruption Commission Act 2011* (Vic), 2011/66.
123. See *Integrity Commission Act 2009* (Tas), 2009/67, s 4 (definition of "misconduct"); *Corruption, Crime and Misconduct Act 2003* (WA), 2003/48, s 3 (definition of "reviewable police action").
124. See Matthew Goode, "Complaints Against the Police in Australia: Where We are Now and What We Might Learn About the Process of Law Reform, with Some Comments About the Process of Legal Change" in Goldsmith, ed, *supra* note 70, 115 at 147.
125. See "Australian Federal Police," online: *Commonwealth Ombudsman* <www.ombudsman.gov.au/How-we-can-help/australian-federal-police> [perma.cc/2EBY-RS5N].
126. See *Ombudsman Act 2009* (NT), 2009/5 [*Ombudsman Act* (NT)].
127. See *Ombudsman Act 1978* (Tas), 1978/82 [*Ombudsman Act* (Tas)].
128. See *Parliamentary Commissioner Act 1971* (WA), 1971/64.
129. See *e.g. Ombudsman Act 1976* (Cth), 1976/181, ss 8-9, 13-14; *Ombudsman Act* (NT), *supra* note 126, ss 14, 31-36; *Ombudsman Act* (Tas), *supra* note 127, ss 13, 23A-27.
130. See *Police Complaints and Discipline Act 2016* (SA), 2016/60.
131. See Louise Porter & Tim Prenzler, *Police Integrity Management in Australia: Global Lessons for Combating Police Misconduct* (CRC Press, 2012) at 160.

In New Zealand, the Independent Police Conduct Authority has oversight over NZ Police. While its website claims "We are the only NZ Police oversight body,"[132] this is only true in the sense that it is the only oversight body focused on policing (for example, the privacy commissioner has a broader jurisdiction). The Independent Police Conduct Authority has the power to hear complaints about "any practice, policy, or procedure" that affects the complainant.[133] There is no power to act on an "own motion" basis[134] except in the context of death or serious injury.[135] While a complaint can lead to examination of the broader policy, this is not well captured by the complaints form (which focuses on a specific incident).[136] New Zealand also has an ombudsman, but with no oversight functions in relation to police except with respect to access to information.[137]

Particularly in jurisdictions where there is reliance on complaints, intelligence practice is rarely a focus for police oversight. For example, in Alberta, a document published by the Law Enforcement Review Board lists "Categories of Police Misconduct," none of which directly relate to intelligence (although the document does include generally applicable categories like breach of confidence, neglect of duty, and unlawful or unnecessary exercise of power).[138] A similar sense that oversight was about other aspects of policing could be seen in some interviews:

> [Provincial police unit] is more around shootings and deaths in custody and stuff here but they also do like corruption and those types of things as well.[139]
>
> We are governed by legislation and the IPCA [Independent Police Conduct Authority] I guess? I don't know if police intelligence even comes up in IPCA, I've never seen intelligence come up in it.[140]

---

132. "About us" (2017), online: *Independent Police Conduct Committee* <www.ipca.govt.nz/Site/about-us> [perma.cc/P3LL-B3VK].
133. *Independent Police Conduct Authority Act 1988* (NZ), 1988/2, s 12(1)(a)(ii).
134. *Ibid*, s 12(2).
135. *Ibid*, s 13.
136. See "Complaint to IPCA," *supra* note 96.
137. This is evident on the NZ Ombudsman's website. See "Get help (for the public)," online: *NZ Ombudsman* <ombudsman.parliament/nz/get-help-public> [perma.cc/4HZD-M3ZK]. Using the tool on this site, choose "I want to *make a complaint* about *the police*." The site indicates that the Ombudsman can help with an *Official Information Act* request but that complaints should be directed to the Independent Police Conduct Authority.
138. See Law Enforcement Review Board, "Categories of Police Misconduct," online (pdf): *Government of Alberta* <www.alberta.ca/assets/documents/lerb-categories-police-misconduct.pdf> [perma.cc/7PTP-K9F3].
139. CA03 (Staff Sergeant).
140. NZ01 (Intelligence Analyst).

What comes from this analysis, though, are three potential barriers to police or public sector oversight of police intelligence, each a concern in some of the jurisdictions analyzed. The first barrier is a dependence on complaints as the only or the primary source of jurisdiction—here, secrecy and lack of public awareness mean that misconduct, where it occurs, is unlikely to result in a formal complaint. The second is jurisdictional limits that focus on specific harms or illegalities (either generally or in the context of reviews that do not require a complaint), such as corruption or physical harm. The third is jurisdictional limits that prevent complaints about the conduct of civilian employees, which is more of an issue in contexts where police intelligence is civilianized.[141]

C. OVERSIGHT OF INTELLIGENCE AGENCIES AND FUNCTIONS

The oversight described in the previous Part was tied closely to police agencies, either specifically or as an aspect of the public service. A different approach that facilitates oversight over broader security networks is oversight of *intelligence*.[142] Examples of intelligence oversight include Canada's NSIRA and Australia's and New Zealand's Inspector-General of Intelligence and Security (IGIS). Intelligence oversight traditionally focused on national security agencies (such as the Canadian Security Intelligence Service and Communications Security Establishment), but, in Canada, now applies to "any activity…that relates to national security or intelligence" undertaken by the RCMP.[143] IGIS's role in Australia has also expanded recently.

In Canada, the *National Security and Intelligence Review Agency Act* established the NSIRA,[144] which replaced the Security Intelligence Review Committee and the Office of the Communications Security Establishment Commissioner. While those former agencies had jurisdiction over the Canadian Security Intelligence Service and Communications Security Establishment, respectively, the new agency's mandate includes reviewing "any activity carried out by a department [including the RCMP] that relates to national security or intelligence" and investigating complaints against the RCMP concerning national security.[145] The Review Agency can cooperate and share some information with other oversight bodies, in particular the CRCC (see Part III(B), above) and the Privacy

141. See *e.g.* Sanders & Condon, *supra* note 4 at 241.
142. See Gill, *supra* note 22 at 45.
143. *National Security and Intelligence Committee of Parliamentarians Act*, SC 2017, c 15, s 8(1)(b).
144. See SC 2019, c 13, s 3 [*NSIRAA*].
145. *Ibid*, ss 8(1)(b), 8(1)(d)(ii); *RCMP Act*, *supra* note 100, ss 45.53(4.1), 45.67(2.1). See also *ibid*, s 2 (definition of "department").

Commissioner (see Part III(D), below).[146] It can also seek an opinion or comment from the Canadian Human Rights Commission.[147] For police, these reforms are focused on "high policing" by the RCMP,[148] the federal police agency.

In Australia, IGIS's role was recently expanded to include oversight over the intelligence functions of the Australian Criminal Intelligence Commission and the Australian Federal Police.[149] This aligns with a recommendation of the 2017 Independent Intelligence Review,[150] but is contrary to the recommendation of the subsequent Comprehensive Review of the Legal Framework of the National Intelligence Community.[151] IGIS has power to decline to consider a complaint where the complaint could more effectively or conveniently be considered by another integrity body, and there are mechanisms to transfer complaints.[152] State and territory police remain outside IGIS's jurisdiction.

The state of South Australia has established oversight over the circumstances in which information is classified as "criminal intelligence" by its state police commissioner.[153] Criminal intelligence is defined in different Acts in similar ways, for example as

> information relating to actual or suspected criminal activity (whether in South Australia or elsewhere) the disclosure of which could reasonably be expected to prejudice criminal investigations, to enable the discovery of the existence or identity

146. *NSIRAA*, *supra* note 144, ss 13-15.1. See also *Privacy Act*, RSC 1985, c P-21, ss 37(5), 64(2) [*Privacy Act* Canada].
147. See *NSIRAA*, *supra* note 144, s 26.
148. This term comes from Jean-Paul Brodeur. High policing is characterized by the absorption of intelligence beyond any narrow domain or function, conflation of separation of powers, a focus on protecting national security, and reliance on informants. See John-Paul Brodeur, "High and Low Policing: Remarks about The Policing of Political Activities" (1983) 30 Soc Problems at 507, 513-14. For clarification, see John-Paul Brodeur, "High and Low Policing in Post-9/11 Times" (2007) 1 Policing 25 at 26-28.
149. *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth) cl 56, amending *Inspector-General of Intelligence and Security Act 1986* (Cth), 1986/101 (inserting s 8(3A)).
150. See *supra* note 65 at 21 (Recommendation 21).
151. See Austl, Attorney-General's Department, *Comprehensive Review of the Legal Framework of the National Intelligence Community* by Dennis Richardson AC (Commonwealth of Australia, December 2020), vol 1 at 80, online (pdf): <www.ag.gov.au/system/files/2020-12/volume-1-recommendations-and-executive-summary-foundations-and-principles-control-coordination-and-cooperation.PDF> [perma.cc/GY5Z-ME7P]. See especially *ibid*, vol 3 at paras 40.93-40.104.
152. See *e.g. Inspector-General of Intelligence and Security Act 1986*, *supra* note 149, s 11(4A); *Law Enforcement Integrity Commissioner Act 2006*, *supra* note 121, s 23A.
153. *Police Act 1998*, *supra* note 50, s 74A.

> of a confidential source of information relevant to law enforcement or to endanger a person's life or physical safety.[154]

The government appoints a retired judicial officer (which, in Australia, lends an air of importance and prestige without falling foul of separation of powers) to oversee criminal intelligence.[155] The most recent review (tabled in Parliament on 18 October 2022 with respect to the period between 1 July 2021–30 June 2022) stated that there was no instance of criminal intelligence used over the relevant period, due to the narrow definition.[156] This oversight is thus very specific and does not capture the kinds of intelligence activities with which this article is primarily concerned.

The type of oversight that had been enacted at the federal level in Australia and Canada is significantly broader. There is nothing similar in New Zealand. Comments from some NZ participants expressed concern about the lack of intelligence oversight for NZ Police and the desirability of adopting something similar to Canada and Australia. For example, an Intelligence Officer stated, "Hopefully it comes back a step and we actually look [at] oversight of intelligence across the board."[157] Bringing police intelligence under *intelligence* oversight would be particularly useful given the extensive information sharing and collaboration between NZ Police and the Security Intelligence Service.[158] However, other participants expressed skepticism that intelligence oversight was appropriate for police either due to the relatively narrow agenda of intelligence in New Zealand compared to Australia,[159] or because of the existing multi-layered oversight networks including the judiciary (as described in this article).[160]

While intelligence oversight operates within the narrow domain of federal agencies in those jurisdictions where it exists at all, the approach offers some advantages. The existence of review powers outside of the context of a complaint allows for oversight of policies and programs. The focus on intelligence activities allows for both specific expertise and oversight over broader networks. While unlikely to conflict with the very different role of the judiciary (discussed in Part

---

154. *Firearms Act 2015* (SA), 2015/46, s 4(1).
155. See *Police Act 1998*, *supra* note 50, s 74A(4).
156. See Austl, SA, *Review under section 74A(4) of the Police Act 1998 for the period of 1 July 2021-30 June 2022* by the Honourable Michael David (2 August 2022).
157. NZ04.
158. See Rebecca Kitteridge, "Speech: Understanding Intelligence Remark" (Address to the Institute of Public Administration New Zealand, 18 September 2019), online: <www.nzsis.govt.nz/news/speech-understanding-intelligence> [perma.cc/62ZR-LTLJ].
159. NZ16.
160. NZ19.

IV(A), below), overlap with oversight agencies focused on police in general needs to be carefully managed.

D. OVERSIGHT OF COMPLIANCE WITH PRIVACY LAW

Privacy oversight is particularly relevant to police intelligence, which frequently draws on personal and sensitive information.[161] For example, mass surveillance using social media analytics risks breaching limits on the collection of personal and sensitive information where it is not reasonably necessary for or directly related to an agency function (in Australia),[162] where it does not directly relate to an operating program or activity of the agency (in Canada),[163] and where the collection of the information is not necessary for an agency purpose (in New Zealand) (or similarly for state, territorial, and provincial legislation).[164] Information sharing with other public and private sector bodies is also affected as there are restrictions on when information can be disclosed to law enforcement and, for information held by police agencies, when it can be disclosed to other agencies.[165] Privacy law is also one means through which individuals can find out about information held *about them*, although such rights are generally limited.[166] While police have more degrees of freedom under privacy laws than most public sector agencies, and may use privacy law as a pretext to conceal information, there are still constraints. It is thus still important to consider oversight and accountability for compliance with those rules.

In Canada, the Privacy Commissioner has played an active role in overseeing police data practices. The Privacy Commissioner has audit powers to examine questions such as "whether the RCMP had appropriate controls in place to ensure its collection of subscriber information from companies without a warrant

161. See Gottschalk, *supra* note 61 at 17.
162. See Bennett Moses et al, *supra* note 16.
163. See *Privacy Act* Canada, *supra* note 146, s 4.
164. See *Privacy Act 2020* (NZ), 2020/31, s 22(1(1)(b)).
165. See *Privacy Act* Canada, *supra* note 146, s 8(2)(e).
166. See *e.g. ibid*, s 18(1), 22(1); *Exempt Personal Information Bank Order, No. 13 (RCMP)*, SOR/90-149 (designation of exempt banks); *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165, s 27(3)(a) [BC *Freedom of Information Act*]; *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31, s 39(3) [Ontario *Freedom of Information Act*]; *Municipal Freedom of Information and Protection of Privacy Act,* RSO 1990, c M.56, s 29(3)(a). For other provisions that law enforcement can use to prevent disclosure, see *e.g. Privacy Act* Canada, *supra* note 146, s 5(3).

was in compliance with the *Privacy Act*."[167] There have been a number of relevant audits, including of the RCMP's exempt data banks, the use of data brokers, the National Integrated Information Initiative (N-III) electronic records-sharing program, and selected RCMP databases in 2011.[168] The Privacy Commissioner can also make more general recommendations in response to specific complaints. One Privacy Commissioner investigation concerned the RCMP's uploading to the Canadian Police Information Centre (CPIC) information concerning a complainant's attempted suicide, thus making the information available to US Customs and Border Protection.[169] The Privacy Commissioner made broad recommendations, including a change in the default state of the CPIC database to suppress the sharing of certain data with US border officials and to create greater clarity in CPIC policies. More recently, the Privacy Commissioner investigated the RCMP's use of Clearview AI, finding that it contravened the *Privacy Act* because it collected information through a contract with a private company that was itself collecting information unlawfully and thus acted outside of its legal authority.[170] A significant challenge for the Commissioner is limited power to demand information. For example, the Commissioner noted in relation to an audit of the collection of subscriber information that it was "unable to assess whether such controls were in place" and thus it was "impossible to determine how often the RCMP collected subscriber data without a warrant."[171]

---

167. Office of the Privacy Commissioner of Canada, *Privacy Act Annual Report to Parliament 2013-14: Transparency and Privacy in the Digital Age*, by Daniel Therrien, Catalogue No IP50-2014E-PDF (October 2014) at 3, online: <www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201314/201314_pa> [perma.cc/U9DZ-JBGD] [*Privacy Act Annual Report 2013-14*].
168. See Office of the Privacy Commissioner of Canada, *Privacy Commission, 2007-2008 Annual Report*, by Jennifer Stoddart, Catalogue No IP50-2008 (4 December 2008), online: <www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/200708/200708_pa> [perma.cc/Y8NR-9FKA].
169. See Office of the Privacy Commissioner of Canada, "Disclosure of information about complainant's attempted suicide in US Customs and Border Protection not authorized under the *Privacy Act*" (last modified 21 September 2017), online: <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2016-17/pa_20170419_rcmp> [perma.cc/3MLD-6DXX].
170. See Office of the Privacy Commissioner of Canada, *Special Report to Parliament on the OPC's Investigation Into the RCMP's Use of Clearview AI and Draft Joint Guidance for Law Enforcement Agencies Considering the Use of Facial Recognition Technology*, Catalogue No IP54-110/2021E-PDF (10 June 2021), online: <www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp> [perma.cc/GKR6-F9TW] [*Clearview AI Special Report*].
171. *Privacy Act Annual Report 2013-14*, *supra* note 167 at 3.

Provincial commissioners in Canada have also had opportunities to investigate the legality of police intelligence programs. For example, the Saskatchewan Information and Privacy Commissioner investigated "The Hub," an information-sharing project.[172] The report discouraged the use of Facebook as a data collection tool.[173] The British Columbia Privacy Commissioner has criticized the data sharing and retention practices of the Victoria Police Department.[174]

The powers of privacy commissioners and similar bodies (where they exist) in Australia are limited. As in Canada, the Office of the Australian Information Commissioner investigated police use of Clearview AI in Australia, focusing on non-compliance with a requirement to conduct a Privacy Impact Assessment.[175] In Australia, the problems of under-resourcing at the Office of the Australian Information Commission are particularly acute.[176] Powers to obtain documents are more limited than in Canada; in Australia, there is no such power where obtaining documents would "prejudice the effectiveness of the operational methods or investigative practices or techniques of agencies responsible for the enforcement of the criminal law."[177] Even in Canada, police sometimes withhold information from privacy commissioners, including in a context where the reporting was done by an internal unit unfamiliar with the practices of other internal units.[178] Unlike in the context of intelligence oversight, privacy

172. The Commissioner drew on powers in *The Local Authority Freedom of Information and Protection of Privacy Act*. See SS 2017, c 17, s 32.
173. See *Investigation Report 105-2014: Community Mobilization Prince Albert* (SK OIPC, 10 November 2014) at 38.
174. See Office of the Information and Privacy Commissioner for British Columbia, *Investigation Report F12-04: Use of Automated Licence Plate Recognition Technology by the Victoria Police Department*, by Elizabeth Denham (15 November 2012), online: <www.oipc.bc.ca/investigation-reports/1480> [perma.cc/5NGX-26VL]. Note that Victoria here refers to Victoria, British Columbia, Canada.
175. Office of the Australian Information Commissioner, *Commissioner Initiated Investigation into the Australian Federal Police (Privacy)* (26 November 2021), [2021] AICmr 74.
176. See Gabrielle Appleby, "Horizontal Accountability: The Rights-Protective Promise and Fragility of Executive Integrity Institutions" (2017) 23 Austl JHR 168. This might change with the increased powers and penalties recently enacted in the *Privacy Legislation Amendment (Enforcement and Other Measures)* (Cth) [*Privacy Legislation Amendment Act*] and the additional resources allocated in the May 2023 budget. The *Privacy Act 1988* (Cth), 1988/119 is also under review. Attorney-General's Department, "Review of the Privacy Act 1988" (10 January 2022), online: *Australian Government* <https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988> [perma.cc/3DKE-3SQM].
177. *Privacy Act 1988* (Cth), *supra* note 177, s 70(1)(g). While this section remains in place, there are increased powers under the *Privacy Legislation Amendment Act*, *supra* note 177 that post-date the analysis in this article.
178. See *Clearview AI Special Report*, *supra* note 170.

commissioners generally lack power to directly access internal documents in the course of investigations.

New Zealand has an interesting innovation in the form of reviews by the Privacy Commissioner of information-sharing agreements, including those entered into by police.[179] Such reports can deal with matters such as operation in unforeseen ways and infringement of privacy. However, no such reports could be found on the Commissioner's website.

Privacy oversight is not necessarily limited to traditional privacy oversight agencies such as privacy commissioners. In addition to privacy laws, some jurisdictions have a separate oversight regime for narrower domains. For example, in Australia, the Commonwealth Ombudsman has responsibility for oversight of compliance with the part 15 of the *Telecommunications Act 1997*, (concerning agencies seeking assistance from communications providers) and provisions of the *Telecommunications (Interception and Access) Act 1979* related to record keeping, retention, and destruction for telecommunications interceptions.[180] In addition, the Australian Signals Directorate has a role in ensuring that protected information is managed under secure protocols. Further, from time to time, other agencies can become involved in overseeing data governance. For example, Statistics New Zealand reported on a data quality review of NZ Police data at the Police's request in 2015.[181]

Oversight of compliance with privacy law can ensure that "if [our police agency is] using personal information or information relating to people, that we're doing it appropriately."[182] This requires that oversight bodies have sufficient access to information to make an assessment about compliance, which is not always the case. Privacy oversight, while important, is generally associated with limited powers to demand documents or interrogate officers.

E. AD HOC OVERSIGHT

All three jurisdictions have appointed bodies with limited oversight functions, either by reference to time, jurisdiction, or both. For example, a body might be appointed to consider the ethical use of artificial intelligence under a code

179. See *Privacy Act 1993* (NZ), 1993/28, ss 96W, 96X, as repealed by *Privacy Act 2020*, *supra* note 164, s 216(1). The relevant sections of the former Act are now reflected in ss 158, 159.
180. *Telecommunications Act 1997* (Cth), 1997/49; *Telecommunications (Interception and Access) Act 1979* (Cth), 1979/114, ss 83-92A.
181. Statistics New Zealand, "Review of Police Crime Data" (16 February 2015), online (pdf): *New Zealand Police* <www.police.govt.nz/sites/default/files/publications/report-of-review-of-police-crime-data.pdf> [perma.cc/XB75-MVG4].
182. AU13.

of conduct[183] or, more recently, government mandates related to automation, such as New Zealand's Algorithm Charter and Canada's Directive on Automated Decision-Making.[184] Royal commissions, commissions of inquiry, and independent reviews have always played an important role in relation to police illegality, both for post-mortems on what is not working[185] and as a motivator for new laws and oversight mechanisms.[186] While such efforts may be useful, or even cathartic, they are not considered in depth here as they do not form part of the general arrangements for oversight and cannot assist with accountability outside of their particular bounds.

IV. OTHER OVERSIGHT MECHANISMS

Not all oversight mechanisms have legal oversight of police intelligence as part of an official function. There are a variety of bodies serving different functions, such as entities performing political oversight; judges granting warrants, admitting evidence, resolving criminal disputes, and sitting on criminal matters; and other agencies that may investigate or work with police intelligence. In all of these cases, the focus here remains on the role that they play in legal oversight of police intelligence and not on their primary functions nor the role that political oversight might play in controlling quality, evaluating effectiveness and efficiency, and controlling budgets.

A. JUDICIAL OVERSIGHT

Oversight by the judiciary arises in a number of contexts, most notably through the issue of warrants, exclusion of evidence, civil action against police, and criminal action against police. There are rules upon rules in this context. Jurisdictions differ not only in relation to the substantive rules (such as the permissibility of

183. CA18.

184. See "Algorithm Charter for Aotearoa New Zealand" (July 2020), online: *Statistics New Zealand* <www.data.govt.nz/use-data/data-ethics/government-algorithm-transparency-and-accountability/algorithm-charter> [perma.cc/JHR6-SUME]; Canada, *Directive on Automated Decision-Making* (Treasury Board of Canada Secretariat, 2019), online: <www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592> [perma.cc/T9C2-HERP].

185. AU19.

186. NZ19. See *e.g.* Canada, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (Public Works and Government Services Canada, 2006) at 312-16 (with recommendations including the limited mandate of RCMP with respect to "collecting and analysing information and intelligence relating to threats to the security of Canada"); Hon Neil Wittmann, *Use of Force in the Calgary Police Service* (Calgary Police Service, April 2018).

particular information-collection practices or the existence of constitution-level rights), but in relation to the rules about the consequences of breach of those rules (such as when evidence is excluded or when police officers or police agencies are liable to civil action). While the judiciary has a role to play in all jurisdictions in assessing the legality of police conduct, the extent of its influence is thus varied. In particular, courts have less power over intelligence that is pre-investigative, being used neither in investigations nor as evidence.

Restrictions on admissibility of evidence mean that police can be required to account for intelligence practices where these are directed to or lead to the collection of evidence to be used in prosecuting a specific offender. There are examples in all three countries of the courts ruling as inadmissible intelligence sought to be admitted in evidence in criminal prosecutions due to impropriety in collection.[187] Intelligence officers across jurisdictions are aware, as they need to be, that procuring information illegally has consequences for prosecutions:

> So, if you're trying to secure evidence against an offender…and then you try and circumvent those legislative requirements, you're running a very big risk of your court case just being thrown out the door.[188]

> If the evidence is obtained illegally or unlawfully, then that evidence may be excluded and therefore not admissible at trial and the crown is left with well just that, whatever is left right? Once the evidence has been excluded then often times that exclusion is fatal to the prosecution so it's a full blown acquittal, right?[189]

> So, ultimately, what Police do in the main gets tested in a Court of Law. If we are seen to be deficient, then that's the way the system regulates itself.[190]

A number of participants in Canada identified the central influence of the judiciary over police investigative intelligence practices through the power to rule evidence inadmissible. In particular, there was a strong awareness of the need to avoid negative judicial outcomes as a result of non-compliant intelligence practices ("we have a saying in our office we do not want to make case law").[191] This was linked to a sense that judicial criticism had consequences beyond the particular case, as described by a manager: "You know when you're found doing things like that, that you shouldn't do you get bad court decisions and that impairs [your] ability…to use those tools at all."[192]

---

187. See *e.g. R v Ul-Haque*, [2007] NSWSC 1251 at paras 103-105.
188. AU08 (Manager).
189. CA05 (Lawyer and Lead Analyst).
190. NZ19 (Manager).
191. CA13 (Intelligence Analyst).
192. CA12.

There are two reasons why the role of Canadian courts is greater in the context of intelligence-led policing. First, Canadian courts are willing to exclude evidence found in the context of broadly discriminatory police practices.[193] Thus if a predictive policing program were to exhibit racial bias,[194] there is a reasonable likelihood that evidence collected through over-policing of racialized neighbourhoods or individuals would be excluded. Second, police are required to disclose information to the defence where "there is a reasonable possibility that the withholding of information will impair the right of the accused to make full answer and defence," unless the non-disclosure is justified by the law of privilege.[195] This means that, in many cases, even if a defendant were not otherwise aware of the intelligence practices lying behind direct engagements with police, this would need to be disclosed, thus allowing them to challenge evidence found in related searches.

However, exclusion of evidence only controls the collection of information where there is an intention or a possibility that the information would be used in prosecutions. This leaves some kinds of intelligence gathering outside of the control of this form of oversight. Where intelligence is gathered for strategic purposes, as in the case of large-scale algorithmic surveillance, it may never be introduced in evidence in any particular trial. Some intelligence practices thus bypass this particular kind of scrutiny, as recognized by many participants, particularly in Australia and New Zealand:

> Intelligence is relatively unique as opposed to investigations because the investigations are essentially subject to judicial scrutiny in court.[196]
>
> A lot of it cannot be used as evidence.[197]
>
> What might get shown for operational police-use might need to be redacted and can't be shown in court.[198]

In Canada, an Intelligence Officer expressed a contrary view that "there's no such [thing] as covert information that is [for] police intelligence purposes only."[199] However, it is unlikely that Canadian law would have this strong an effect, at least in the context of intelligence products such as those discussed here.

193. See *e.g. R v Brown* (2003), 173 CCC (3d) 23 (Ont CA).
194. See Lyria Bennett Moses & Janet Chan, "Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability" (2018) 28 Policing & Society 806.
195. *R v Stinchcombe*, [1991] 3 SCR 326 at 340.
196. AU09 (Trainer).
197. AU01 (Manager).
198. NZ10 (Analyst).
199. CA18.

While the use of predictive policing that directly relates to a search or the existence of exculpatory facial recognition matches may need to be disclosed to the defence and could lead to the exclusion of evidence or acquittal of a defendant, there will likely remain intelligence practices that remain unmentioned in criminal trials.

One response to the limitation on judicial oversight through laws of evidence is that given by one Australian participant who suggested that oversight of intelligence that is not introduced as evidence is less important because it does not have "an effect on a citizen."[200] However, this is not necessarily the case. For example, predictive policing can enhance racial disparity in policing,[201] and the mere fact of surveillance can impact negatively on liberty and free speech.[202]

Related to the court's power to exclude evidence is its power to issue warrants, requiring *ex ante* assessment of whether particular searches or surveillance should be authorized:

> If we want to use the information as evidence, opposed to intelligence, and sometimes we use it for both, but if we're going to use it as evidence, we have to generally get a search warrant.[203]

> Everything has to have gone through judicial authorization in order to be used as part of the investigative process.[204]

> If we are having to do search warrants, we're confident in the way that we've collected that information and presented that to decision-makers is going to stand up.[205]

Procedural mechanisms, such as Public Interest Monitors in Victoria, Australia, can ensure that the interests of citizens who are to be surveilled are aired.[206] Despite processes differing by jurisdiction, there was a general perception among participants that the difficulty of obtaining warrants made them accountable for intelligence gathering, at least in circumstances where that requirement was in place:

> So, if we want to ground a search warrant based upon intelligence then we have to satisfy justice that there is sufficient intelligence to ground that warrant.[207]

---

200. AU15.
201. See Bennett Moses & Chan, *supra* note 194.
202. See Frank La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UNGAOR, 23rd Sess, UN Doc A/HRC/23/40 (2013).
203. AU13 (Manager).
204. CA18 (Intelligence Supervisor).
205. NZ06 (Lead Intelligence Analyst).
206. See *Public Interest Monitor Act 2011* (Vic), 2011/72.
207. AU06 (Former Manager).

> So, for Police to go to court and get a warrant, there has to be a certain bar.[208]

However, warrant mechanisms are primarily relevant where material will be used as evidence, as opposed to more strategic, broad intelligence practices. Warrants are not required to conduct threat assessments, match a face using a service such as Clearview AI, or procure predictive policing software. The need for warrants is also limited to circumstances in which such *ex ante* approval is required, which varies by jurisdiction. For example, telecommunications metadata can be accessed without a warrant in Australia, so there is no *ex ante*, independent oversight over decisions to access and use information about who an individual telephoned at which times.[209] Memoranda of understanding with, request portals built by, and free software trials offered by private sector organizations can also remove the need to get a warrant.[210]

The judiciary also has a role to play, either when civil action is brought by those dissatisfied with the complaints process[211] or when (rarely) investigations lead to criminal prosecution of police.[212] The purposes of these two are distinct—the former is about justice for an individual complainant rather than broader oversight on the public's behalf,[213] and it is only useful as an accountability mechanism if outcomes are disseminated.[214] Strong skepticism has been expressed about both.[215]

Civil actions are less likely in the context of some of the more diffuse harms associated with intelligence, such as predictive policing programs that target racialized neighbourhoods. The viability of civil actions against police varies by

---

208. NZ06 (Lead Intelligence Analyst).
209. See Sharon Rodrick, "Accessing Telecommunications Data for National Security and Law Enforcement Purposes" (2009) 37 Fed L Rev 375 at 410-11.
210. CA06. See Reuters, "Apple is Building an Online Tool That Lets Police Request User Data," *Venture Beat* (7 September 2018), online: <www.venturebeat.com/2018/09/07/apple-is-building-an-online-tool-that-lets-police-request-user-data> [perma.cc/86WB-SSMB].
211. See Seneviratne, *supra* note 64 at 331. See also Janet Ransley, Jessica Anderson & Tim Prenzler, "Civil Litigation Against Police in Australia: Exploring Its Extent, Nature and Implications for Accountability" (2007) 40 Austl & NZ J Crim 143.
212. See Tom Hughes, "Police Officers and Civil Liability: The Ties That Bind?" (2001) 24 Policing 240. For a recent example of criminal prosecution, see Scott Anderson & Andrew Culbert, "RCMP used covert search and surveillance powers before arresting high-level intelligence official," *CBC News* (28 October 2020), online: <www.cbc.ca/news/canada/rcmp-investigation-cameron-ortis-warrants-1.5778569> [perma.cc/F92A-7CSW].
213. See Ransley, Anderson & Prenzler, *supra* note 211.
214. See Smith, "Rethinking," *supra* note 94 at 19, 22.
215. See Goode, *supra* note 124 at 117.

jurisdiction,[216] including as to whether the state can be made vicariously liable.[217] Civil actions can be brought in relation to a breach of the New Zealand Bill of Rights or the *Canadian Charter of Rights and Freedoms*,[218] whereas Australian rights protections are generally statutory schemes and are not necessarily accompanied by a right to civil action.[219] Such civil rights can be used to challenge police intelligence, as illustrated by the use of article 8 of the European Convention on Human Rights to stop a Dutch predictive policing program.[220] However, civil actions related to police intelligence are rare,[221] possibly due to the lack of public awareness of intelligence practices, but also because of greater concern surrounding physical interactions with police.

Where police commit crimes, criminal penalties, including imprisonment, can be imposed by courts. The ability to seek criminal penalties for criminal conduct is crucial for police accountability[222] and very much in line with the basic rule of law idea that those who enforce the law are also subject to it. This possibility can have a strong disciplinary effect:

> So the internal investigators will investigate, there are sanctions available internally, but ultimately if [there are] criminal breaches then the courts will decide on the penalty.[223]

> [I]f you put a listening device in someone's house and you haven't got the appropriate legislative authority to do it, you could go to jail. There's every chance you probably

---

216. In Australia, see *Bunning v Cross* (1978), 141 CLR 54 (HCA).
217. See *Enever v The King* (1906), 3 CLR 969 (HCA) (the State is not liable for tortious actions or omissions of individual police officers).
218. *Canadian Charter*, *supra* note 13, s 24(1); *Simpson v Attorney General*, [1994] 3 NZLR 667 (CA). Note that the situation is more limited in Australia even in those jurisdictions that have a statutory bill of rights. See *Charter of Human Rights and Responsibilities Act 2006* (Vic), 2006/43, s 39; *Human Rights Act 2004* (ACT), 2004/5, s 40C; *Human Rights Act 2019* (Qld), 2019/5, s 59.
219. For example, despite a recommendation of the Australian Law Reform Commission, there is no tort for serious breach of privacy. See Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, ALRC Report No 123 (Ligare for ALRC, 2014).
220. See Rechtbank Den Haag [District Court of the Hague], 5 February 2020, *Nederlands Juristen Comité Voor De Mensenrechten v The State of the Netherlands*, ECLI:NL:RBDHA:2020:865, No C-09-550982-HA ZA 18-388 (Netherlands). For a discussion of this decision, see Litska Strikwerda, "Predictive Policing: The Risks Associated with Risk Assessment" (2021) 94 Police J 422.
221. See Ransley, Anderson & Prenzler, *supra* note 211 at 147-48, 152-54.
222. See Graham Smith, "Police Complaints and Criminal Prosecutions" (2001) 64 Mod L Rev 372 at 373, 391.
223. AU16 (Manager).

> would because I'd imagine the courts would frown quite harshly on police doing that sort of thing. So, no, we wouldn't do it.[224]

Nevertheless, criminal prosecution remains "the most cumbersome tool for the accountability of officials."[225] Police have an advantage in criminal investigations and prosecutions against them, and thus rarely lose.[226] The success in particular cases, even among the small number prosecuted, is thus not guaranteed. Further, most of the examples of criminal liability relate to matters such as assault, false arrest or imprisonment, and harassment, as opposed to the generation of intelligence reports that might affect the behaviour of front-line police.[227]

B. POLITICAL OVERSIGHT AND ASSURANCE OF LEGALITY

Oversight of police by political actors such as responsible ministers, parliamentary committees, and (in Canada) municipal police boards is a complex domain.[228] Important limits on political control of police, stemming from the rule of law, the English case of *R v Commissioner of Police of the Metropolis, Ex parte Blackburn*,[229] and statutory provisions, exist in all jurisdictions studied.[230] There seems, however, to be agreement that relevant political actors can, at a minimum, require legal accountability from police.[231] This is particularly so in the context of statutory powers of direction, where they exist.[232]

Responsible ministers are answerable to parliament for the legality of matters within their jurisdiction. In the case of ministers responsible for policing, the primary obstacles to exercising a legal oversight function are likely to be lack

224. AU08 (Manager).
225. Paul G Chevigny, "Police Accountability in Historic Perspective" in Mendes et al, eds, *supra* note 52, 69 at 72.
226. See Bernard D Bongiorno, "A DPP's Approach: Some Problems in the Prosecution of Police Officers" in Moore & Wettenhall, eds, *supra* note 47, at 37.
227. See Graham Smith, "Actions for Damages Against the Police and Attitudes of Claimants" (2003) 13 Policing & Society 413.
228. See Kent Roach, "The Overview: Four Models of Police-Government Relations" [Roach, "Four Models"] in Beare & Murray, eds, *supra* note 49 at 16; Duncan Kerr, "Government and the Police" in Moore & Wettenhall, eds, *supra* note 47, 13.
229. [1968] 2 QB 118 at 135 (CA).
230. For Canada, see *R v Campbell*, [1999] 1 SCR 565. For Australia and New Zealand, see generally Stenning, "Political Independence," *supra* note 49.
231. See Lorne Sossin, "The Oversight of Executive-Police Relations in Canada: The Constitution, the Courts, Administrative Processes, and Democratic Governance" in Beare & Murray, eds, *supra* note 49, 96 at 129.
232. See *e.g. RCMP Act*, *supra* note 100, s 5(1); *Police Services Act, 1990*, *supra* note 107, s 17(2); *Police Act 1998*, *supra* note 50, s 6; *Police Service Administration Act 1990* (Qld), 1990/4, ss 4.6-4.8.

of political benefit, lack of sufficient expertise, and lack of resources and power to run inquiries or investigations.[233] None of this implies that ministers are incapable of insisting on legality; their leadership can have a positive impact on creating a culture of compliance. However, if government and its ministers are concerned about police illegality or misconduct and are motivated to act, they are more likely to launch a formal inquiry,[234] task force, royal commission, or similar ad hoc oversight mechanism with the necessary powers and expertise (and political distance).[235]

Parliamentary committees, if constructed well and accompanied by necessary powers, can play an important role in the legal oversight of police, although this will rarely be their main focus.[236] For example, in Australia, the Committee on Intelligence and Security has a limited oversight role in relation the Australian Federal Police, focusing on terrorism.[237] The Australian Federal Police fall primarily under the Parliamentary Joint Committee on Law Enforcement. In Canada, the relevant committees for the RCMP are the National Security and Intelligence Committee of Parliamentarians (in relation to intelligence), the Standing Senate Committee on National Security and Defence, the House of Commons Standing Committee on Public Safety and National Security, and the House of Commons Standing Committee on Access to Information, Privacy, and Ethics.[238] However, parliamentary committees in Canada lack access to classified information and are generally under-resourced.[239] In New Zealand, the main committee would be the Justice Select Committee (responsible for scrutiny of police), although the Intelligence and Security Committee may intersect on

233. See Arar Report: Policy Report, *supra* note 24 at 488-89.
234. See *Inquiries Act*, RSC 1985, c I-11.
235. See Sossin, *supra* note 231 at 107, 121 (noting that this has become a norm in Canada).
236. See Lewis, *supra* note 39 at 36-38.
237. *Intelligence Services Act 2001* (Cth), 2001/152, s 29.
238. Cat Barker et al, *Oversight of Intelligence Agencies: A Comparison of the 'Five Eyes' Nations* (Parliamentary Library of Australia, 15 December 2017), online: <www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1718/OversightIntelligenceAgencies> [perma.cc/68H6-XUUE].
239. See Kent Roach, "Review and Oversight of Intelligence in Canada: Expanding Accountability Gaps" in Zachary K Goldman & Samuel J Rascoff, eds, *Global Intelligence Oversight: Governing Security in the Twenty-First Century* (Oxford University Press, 2016) 175.\\uc0\\u8220{}Review and Oversight of Intelligence in Canada: Expanding Accountability Gaps\\uc0\\u8221{} in Zachary K Goldman, Samuel J Rascoff & Jane Harman, eds, {\\i{}Global Intelligence Oversight: Governing Security in the Twenty-First Century} (New York: New York: Oxford University Press, 2016

some issues.[240] Parliamentary committees require not only jurisdiction but also a willingness to hold hearings or write reports on matters related to police legality.

In Canada, municipal police would rarely come to the attention of a parliamentary committee. Democratic oversight is generally through police service boards, where they exist.[241] These boards provide financial governance and strategic management, primarily as a buffer between political direction and chiefs of police.[242] The nature and powers of such police boards vary but, like ministers and parliamentary committees, the focus is not primarily on legal accountability but rather policy. Expertise and access to operational information is also low, as they are not responsible for operations. Although some Australian states have historically used police boards, this is no longer the case.[243]

Few participants mentioned political actors as examples of oversight to which their activities were subject.[244] Where it was mentioned, it was generally in the context of reporting (in that reporting may formally be to a minister or parliamentary committee). This is likely because such oversight is at a higher strategic and policy level, focused on matters of high policing such as terrorism, and generally excludes oversight of operations. Further, such political actors typically lack expertise in police intelligence. The ordinary work of ministers, parliamentary committees, and police service boards are rarely significant players in *legal* oversight.

C. HORIZONTAL OVERSIGHT

There are some contexts in which one agency oversees the conduct of another. For example, officers in the Australian Criminal Intelligence Commission might be referred to the Australian Federal Police for investigation,[245] and the RCMP has been called in to investigate charges of corruption against the Toronto Police Service.[246]

There is also a less formal sense in which agencies with intelligence functions oversee compliance by other agencies, and that is in the context of information

240. For information on the jurisdiction of New Zealand select committees, see "Select Committees," online: *New Zealand Parliament* <www.parliament.nz/en/pb/sc>.
241. See Roach, "Four Models," *supra* note 228 at 60.
242. See Mark Crowell, *Police Officers' Attitudes Toward Civilian Oversight Mechanisms in Ontario, Canada* (PhD Thesis, University of Waterloo, 2016) [unpublished] at 1-2. See also Sossin, *supra* note 231 at 96-146.
243. See Stenning, "Political Independence," *supra* note 49 at 220-21.
244. AU01.
245. AU03.
246. See Sossin, *supra* note 231 at 104.

sharing. Such horizontal oversight or peer constraints also exist among non-police intelligence services.[247] Domestic and foreign agencies that share information with police for intelligence purposes do so conditionally and often monitor compliance with those conditions. The rules may already exist, may be created through agreements or memoranda of understanding, or may be implied.[248] The potential sanction here is refusal to continue to voluntarily share information and cooperate—which can create powerful incentives. For example:

> [M]any of our people would know somebody that works at those energy providers and might just pick up the phone and say, listen, can you tell me who's power on at such and such an address?…[T]he reason it's jumped on pretty quickly, is it potentially jeopardises those formal arrangements because what potentially happens is that service provider turns around and says, well, if you're not playing by the rules, we're shutting up shop and we're not telling you anything, so don't bother coming back.[249]

> I know in the closed units that deal with top-secret stuff, it's always about trust and if you breach that once you know you'll be cut-off.[250]

> So we had to look at data standards, we had to look at you know how do we build an environment where health feels comfortable sharing certain things with us.[251]

In Canada, the third-party rule was discussed by a number of participants. Essentially, where information that was provided by a third party is marked for intelligence use only, it cannot be used in court or further distributed without that party's permission. This rule is enforced on a similar basis as information sharing, in that breach will reduce willingness to provide information in the future. While this terminology did not come up in Australian and New Zealand interviews, similar restrictions were said to exist under some inter-agency agreements.

---

247. See Ashley Deeks, "Intelligence Services, Peer Constraints, and the Law" in Goldman & Rascoff, eds, eds, {\\i{}Global Intelligence Oversight: Governing Security in the Twenty-First Century} (New York: Oxford University Press, 2016*supra* note 239.
248. Unwritten understandings are particularly relevant in the context of international data sharing. For an example of the consequences of sharing information outside expectations, see Michael McKenzie, *Common Enemies: Crime, Policy, and Politics in Australia-Indonesia Relations* (Oxford University Press, 2018), ch 3.
249. AU08 (Manager).
250. NZ08 (Intelligence Analyst).
251. CA12 (IT Personnel).

V. THE CHALLENGE OF TRANSPARENCY

There is a close link between accountability and transparency. Unless a police oversight agency is aware of particular intelligence practices, it cannot launch a review of the legality of such practices. While intelligence oversight agencies have strong investigatory powers in the absence of a specific investigation, most oversight mechanisms rely on a degree of transparency by police themselves.

Intelligence work is notoriously secret. Jean-Paul Brodeur recounts an old example (from 1973) of members of the RCMP being required to sign an "indoctrination undertaking."[252] In it, they promised "not to disclose any information whatsoever concerning this matter to any unauthorised person"—there was no exception for disclosure of illegal conduct in the course of the operation.[253] While this is not a recent example, many of the ways in which police currently obtain information and intelligence remain relatively obscure. Whistle-blowing is generally restricted.[254] Privacy and freedom of information legislation restricts the ability of individuals to learn that their personal data is being collected or shared for law enforcement purposes.[255] Although we like to describe police as being accountable to the communities they serve, the public are most likely to be in the dark about police intelligence practices. Even oversight agencies may lack access to all of the information needed to assess legality.

Some information about police intelligence practices is available through accountability reporting, although this is largely statistical in nature and insufficient for legal accountability. For example, in Australia, aggregate information is available about the use of surveillance device warrants and computer access warrants by law enforcement agencies. This includes statistical information about the number and type of warrants sought and obtained by each relevant agency and the rate of resulting prosecutions and convictions.[256] Similar information is available in Canada, although the reporting in different provinces

252. Brodeur, "Accountability," *supra* note 52 at 148-50.
253. *Ibid* at 148.
254. See *e.g. Public Interest Disclosure Act 2013* (Cth), 2013/133, ss 26, 41(1)(g), 41(2).
255. See *e.g.* BC *Freedom of Information Act*, *supra* note 166, s 33; Ontario *Freedom of Information Act*, *supra* note 166, ss 42(1)(f)-(g); *Information Privacy Act 2000* (Vic), 2000/98, Sched 1, ss 2.1(d)-(h).
256. See, *e.g.* Austl, Commonwealth, Department of Home Affairs, *Surveillance Devices Act 2004 Annual Report 2020-21* (Australian Government, 2021), online: <www.homeaffairs.gov.au/nat-security/files/surveillance-devices-act-2004-annual-report-2020-21.pdf> [perma.cc/R3MP-W5GN].

is variable and sometimes difficult to obtain,[257] and in New Zealand.[258] Such reporting has been criticized as based on selective categorization that obscures operational realities, but is in any event of little value in assessing legality or compliance with human rights.[259] It may provide hints to an astute observer comparing statistics across years that something is awry,[260] but does not on its face confirm or cast doubt on the legality of processes followed. Such reporting is also limited in scope, for example relating to the use of particular warrants, and fails to capture activities that (in the view of law enforcement) do not fall into reportable categories.[261] For example, there is no mention of the use of Clearview AI by the Australian Federal Police in its 2019–2020 report, despite the fact that it was used in this period, because this use did not involve a relevant warrant.[262] Such reporting is thus useful, if at all, as a mechanism for political scrutiny (where certain types of surveillance can be shown to be excessive or ineffective), not as a mechanism for legal accountability beyond demonstrating compliance with the legal requirement to produce the report.[263]

From the public's perspective, the media play an important role in identifying and publicizing illegal intelligence practices.[264] Indeed, it is often the media who have exposed illegal or problematic police intelligence practices, such as racial profiling in Toronto,[265] different search warrant targets for different Sydney suburbs,[266] and the use of Clearview AI for facial recognition.[267] The media's

257. See Christopher Parsons & Adam Molnar, "Government Surveillance Accountability: The Failures of Contemporary Canadian Interception Reports" (2018) 16 CJLT 143.
258. This is provided in annual reports of New Zealand Police. See *Search and Surveillance Act 2012* (NZ), 2012/24, s 172.
259. See Adam Molnar & Ian Warren, "Governing Liberty Through Accountability: Surveillance Reporting as Technologies of Governmentality" (2020) 28 Crit Criminol 13.
260. *Ibid* at 21.
261. *Ibid* at 20-21.
262. See Austl, Commonwealth, Department of Home Affairs, *Surveillance Devices Act 2004 Annual Report 2019-20* (Australian Government, 2020), online: <www.homeaffairs.gov.au/nat-security/files/surveillance-devices-act-2004-annual-report-2019-20.pdf> [perma.cc/73AW-Q2AW].
263. See Parsons & Molnar, *supra* note 257 at 165.
264. See Claudia Hillebrand, "The Role of News Media in Intelligence Oversight" (2012) 27 Intelligence & National Security 689. See also Jerome H Skolnick, "Democratic Policing Confronts Terror and Protest" (2005) 33 Syracuse J Intl L & Com 191 at 211.
265. See *e.g.* Jim Rankin et al, "Singled Out," *Toronto Star* (19 October 2002), online: <www.thestar.com/news/gta/knowntopolice/2002/10/19/singled-out.html> [perma.cc/J6G8-8Y5P].
266. See Thompson & Singhal, *supra* note 99.
267. See The Detail, *supra* note 8.

ability to investigate and expose police intelligence practices is thus important—while not formally exercising "oversight," it can seem that way:

> I suppose I learned this rule early on in my law enforcement career was what I knew was the Daily Telegraph rule; was how would this look on the front page of the newspaper with half the story, possibly bodgy, with hysterical ministers all around it, how would this look?[268]
>
> I think that in the New Zealand context [oversight] is what the media says to the public, unfortunately.[269]
>
> I guess the media play a big part in…holding them to account.[270]

The media has the capacity to conduct its own investigations of police impropriety and can exert pressure on organizations to comply with the law. As noted at the outset, such pressure is not the same thing as accountability, as the media lacks power to impose consequences or remedy non-compliance with rules. However, it can generate public awareness that can unleash other forms of accountability (such as political pressure to launch an inquiry). There is an irony in this—the role of the media in exposing illegal police intelligence practices illustrates the limitations of the oversight system as a whole. As one Canadian study commented, "Information such as the fact that Canadian police services are testing controversial face recognition technology should not be made available to the public only following exposure by the news media."[271]

The existence of a free press is not alone sufficient to ensure the transparency necessary for oversight mechanisms to come into play. Media often rely on outsiders' accounts and perceptions, which may be incomplete. The practical ability of the media to report on law enforcement intelligence is hampered by exemptions in freedom of information laws[272] and requirements of operational

---

268. AU03 (Manager).
269. NZ14 (Intelligence Supervisor).
270. NZ17 (Manager).
271. Robertson, Khoo & Song, *supra* note 10 at 93.
272. See *e.g. Access to Information Act*, RSC 1985, c A-1. The Act demonstrates exemption for information obtained or prepared by an investigative body in the course of lawful investigations pertaining to the detection, prevention or suppression of crime, the enforcement of [law], or activities suspected of constituting threats to the security of Canada). See *e.g. ibid*, s 16(3) (allows for refusal to disclose a record that contains information that was obtained or prepared by the RCMP while performing services for a province or municipality where there is an agreement with the province or municipality not to disclose); *Re Royal Canadian Mounted Police* (Order) (2017), F2017-81 (AB OIPC) (provincial legislation does not apply).

secrecy.[273] Freedom of information laws are crucial in ensuring transparency as to the kinds of things (albeit not the operational specifics) that occur in the context of police intelligence. These laws thus play a crucial link in initiating other mechanisms of accountability:

> [Freedom of Information requirements] makes us…much more accountable…it does kind of affect what we do just to ensure that we are doing our jobs without over-stepping where we should be.[274]

> New South Wales police…I think they have 4000 or 5000 [freedom of information] requests a year.…and a lot of it is not from journalists wanting to know stories but from people wanting to know what their records are.[275]

Greater *public* transparency, where this is possible, is one avenue through which to facilitate accountability. Where police agencies do or are required to provide public accounts of their activities, this can provide public assurance of the legality and appropriateness of those activities.[276] However, as the media examples above illustrate, intelligence methods are often kept secret without a clear operational justification.

VI. RECOMMENDATIONS

The question of whether or not, in any jurisdiction, the different elements of oversight fit together into a consistent and reliable network, with positive impacts on police intelligence practices, is an important one. Ultimately, there should be bodies that, collectively, have jurisdiction, function, power, and expertise to oversee law enforcement intelligence. There is no need for uniformity here—it will often be appropriate for different jurisdictions to adopt different approaches based on their own political, social, legal, and cultural contexts. However, it is possible for jurisdictions with limitations in their own oversight frameworks to consider improvements based on practices in similar jurisdictions. This Part describes some of the concrete reforms suggested by this comparative analysis.

Canadian police agencies should, if they are not already doing so, consider introducing regular auditing of access to databases, as is currently being done extensively in Australia and New Zealand. Part III(A), above, sets out some of the ways in which auditing can pick up corrupt or poor practices, including by

273. AU09; AU14.
274. CA15 (Patrol Analyst).
275. AU18 (Intelligence Analyst).
276. See Bennett Moses & De Koker, *supra* note 30.

red flagging suspicious searches and monitoring compliance with data handling requirements. While auditing should not be a meaningless box-ticking exercise, and audits that are not followed up serve no purpose, audits do have a role to play in identifying and rectifying non-compliance. While our study is not comprehensive, so this may be taking place in some Canadian jurisdictions, it should be extended to all.

Research participants in all jurisdictions mentioned technological controls embedded into systems that might be loosely grouped around the idea of "compliance by design." Beyond auditing, this included embedding processes into systems, using visible warnings, and building permissions and restrictions into access protocols. As in the case of auditing, technological controls are not perfect, and there may be work arounds. However, police agencies can potentially learn from each other in procuring and designing systems that reduce the risk of non-compliance.

This study demonstrated gaps in the jurisdiction of agencies overseeing police, which limited their ability to provide sufficient oversight over intelligence practices. What is needed for effective oversight here is powers of investigation that do not rely on members of the public raising complaints, and jurisdiction that extends to both intelligence practices (including where no corruption or physical harm is involved) and intelligence practitioners (including those who are not sworn officers). One option to fill such gaps, where they exist, is to base the oversight model on that used for intelligence and national security agencies, as in the case of the NSIRA in Canada and, more recently, IGIS in Australia. However, no jurisdiction is considering this below the federal or national level. At least for state and provincial police, the solution would likely involve extending the powers and jurisdiction of an existing oversight body.

Privacy oversight tends to operate independently of other mechanisms for police oversight. Privacy oversight bodies (such as privacy commissioners) need sufficient investigatory powers and resources if they are to play a role in oversight of police intelligence activities that concern data collection and processing. Among the jurisdictions considered, the Canadian Privacy Commissioner has powers and resources that allow it to call out situations where the RCMP is falling short of its legal obligations. This has allowed it to make broad recommendations on cross-border information sharing and reliance on the illegal acts of third parties, beyond any particular event. While there is room for improvement, particularly with respect to powers to demand information, Australia and New Zealand can look to Canada as an example of what can be achieved with better privacy oversight. In all jurisdictions, it should not only be the media who point

out the problems of police relying on systems that fail to meet their own legal obligations, such as Clearview AI.

While political oversight of police is diverse, information should be available to relevant political entities to help them understand the intelligence context, make them aware of intelligence practices, and provide resources to consider the legality of those practices. This is ultimately a question of good leadership; political actors, whether ministers or members of parliamentary committees, should see the legality of law enforcement practices as a core part of their mission. However, the current reality is that political oversight plays a relatively minor role in legal oversight of law enforcement intelligence.

Secrecy is a significant problem in the context of oversight of law enforcement intelligence. It is also a problem that cannot be completely resolved—operational effectiveness often relies on secrecy about methods. Independent oversight can help reduce the impact of secrecy on accountability. Australia's IGIS is an example of an independent oversight agency operating inside the secrecy curtain with high levels of access that allow it to identify wrongdoing within otherwise secret practices. However, even there, there is no public accountability; the public instead relies on the effectiveness of the independent agency. Transparency, where it does not compromise operational effectiveness, is crucial in ensuring public accountability. Too often, secrecy is deployed not for operational effectiveness but to avoid public accountability. For example, there is no reason that a decision to use predictive policing software or facial recognition tools cannot be made openly, ideally in the context of consultation with communities around how limitations (including the potential for racial bias) will be managed. As demonstrated in those situations where the media was able to disclose poor practices, for example around Clearview AI, such public scrutiny of illegal practices can be effective at preventing or halting illegal practices. This is more likely where media pressure is supplemented with review by an independent oversight body.

Given existing oversight bodies, none of the jurisdictions considered *needs* a new independent statutory agency to oversee specific law enforcement practices, such as the use of biometrics.[277] That is not to say that we might not need better rules around which such biometrics can be used, but only that the creation of a new agency might add additional complexity to the already crowded oversight space. However, what is important is ensuring that the specific issues associated with police intelligence, including the use of biometrics, fall within the jurisdiction, power, and expertise of oversight mechanisms. The recommendations set out in this Part aim to have that effect.

277. *Contra* Mann & Smith, *supra* note 17 at 137-45.

VII. CONCLUSION

Accountability mechanisms in the jurisdictions studied are a patchwork, with internal professional standards units operating alongside independent bodies, which exercise oversight over police or public sector agencies, over intelligence activities of different agencies, or over compliance with privacy laws specifically. In addition, there are important oversight functions performed by judges, ministers, police services boards, parliamentary committees, and other agencies. Ad hoc processes such as public inquiries and royal commissions can play a crucial role but lack permanent jurisdiction, so they cannot be relied on for oversight. Where information is available, and sometimes filtered through the media, there can also be a measure of public accountability. As stated at the outset, this complex web of oversight provides its own challenges. As one participant noted, "[H]ow do we make sure that [the various oversight agencies] don't crash up against each other?"[278] However, while a single oversight agency for law enforcement intelligence might be simpler (from that narrow perspective), the various components collectively cover substantial ground. Further, many jurisdictions provide guidance on jurisdictional boundaries and overlap.

The previous Part contained a number of specific recommendations that would ensure more robust oversight of the legality of police intelligence practices. While it is in the interests of everyone in the community that police obey the law in carrying out their duties, the costs of failing to ensure this are not evenly distributed. Illegal surveillance and targeting are not only more likely to happen to racialized minorities; they are more likely to lead to physical and psychological harm among those groups as well as increase marginalization and community distrust. Those concerned about the disproportionate impact of policing on marginalized communities thus ought to pay particular attention to gaps in oversight.

While this article has focused on oversight for the purposes of ensuring the legality of police intelligence practices, there are important questions that lie beyond that domain. Rosamunde Van Brakel has interrogated oversight of "algorithmic police surveillance" in Belgium,[279] insisting that such oversight should not be limited to legality but extend to socio-ethical evaluation in line with the public interest. This is not oversight in the same sense as considered in this article in that it raises more subjective, even political, questions. Public

278. AU03.

279. See "How to Watch the Watchers? Democratic Oversight of Algorithmic Police Surveillance in Belgium" (2021) 19 Surveillance & Society 228.

demands around policing reform and social movements seeking change are more likely to improve the broader socio-ethical orientation of policing than reorienting the functions of oversight agencies. Conversely, reforms that focus on areas of agreement, such as the need for assurance that police comply with the law, are more likely to be adopted if separated from more hotly contested reforms. However, Van Brakel's point highlights that, while legal oversight is crucial and the reforms canvassed in the previous Part ought to be considered to improve it, this will not be enough to ensure ethical policing for the benefit of all.