LAWFUL ACCESS, PRIVACY, AND TRUST

REPORT FOR THE

NATIONAL SECURITY AND INTELLIGENCE COMMITTEE

OF PARLIAMENTARIANS

NOVEMBER 2023

BENJAMIN J. GOOLD

PETER A. ALLARD SCHOOL OF LAW

UNIVERSITY OF BRITISH COLUMBIA

CONTENTS

INTRODUCTION

Over the last twenty years, there has been ongoing debate in Canada about encryption, privacy, and the investigative powers of the police and security services.[1] Beginning with the Lawful Access Consultations in 2002, followed by the publication of the National Security Green Paper in 2016, and most recently the Report of the Standing Committee on Access to Information, Privacy and Ethics in 2022, successive governments have grappled with the problem of how to ensure that the legal powers and investigative techniques used by the police and security services – often referred to as "lawful access" – keep pace with changes in technology while also respecting individual privacy and other rights guaranteed by the *Canadian Charter of Rights and Freedoms*.

Faced with what is often referred to as the "going dark" problem, senior officers within the RCMP have repeatedly called for additional powers to enable them to lawfully access encrypted data and communications in Canada.[2] Speaking in 2016, then-RCMP Commissioner Bob Paulson told CBS news that there is "criminal activity going on every day that's facilitated by technology that we aren't acting on" and drew attention to what the RCMP regarded as digital barriers to the investigation of crime and threats to national security.[3] In the years that have followed and in the absence of the RCMP's desired law reform,[4] the police have continued to look for ways to overcome the challenges posed by encryption. Most recently, in mid-2022 it

[1] For a recent account of this debate in Canada and elsewhere, see: Diab, R. (2019) "The Road Not Taken: Missing Powers to Compel Decryption in Bill C-59, Ticking Bombs, and the Future of the Encryption Debate" *Alberta Law Review* 57: 267–96.

[2] Seglins, D., Cribb, R., and Gomez, C. (2016) "RCMP Boss Bob Paulson Says Force Needs Warrantless Access to ISP User Data", *CBC News* (15 November 2016), https://www.cbc.ca/news/investigates/police-power-privacy-paulson-1.3851955 (accessed 24 August 2023); Tunney, T. (2018) "RCMP's Ability to Police Digital Realm 'Rapidly Declining,' Commissioner Warned" *CBC News* (5 October 2018), https://www.cbc.ca/news/politics/lucki-briefing-binde-cybercrime-1.4831340 (accessed 13 August 2023).

[3] Seglins, D., Cribb, R., and Gomez, C. (2016) "RCMP Boss Bob Paulson Says Force Needs Warrantless Access to ISP User Data" *CBC News* (15 November 2016).

[4] In the wake of the 2016 National Security Green Paper, the RCMP publicly supported the introduction of a range of new powers in Canada's Anti-Terrorism Act (C-51). See Seglins, D., Cribb, R., and Gomez, C. (2016) "RCMP Want New Powers to Bypass Digital Roadblocks in Terrorism, Major Crime Cases" *CBC News* (15 November 2016), https://www.cbc.ca/news/investigates/rcmp-digital-roadblocks-1.3850018 (accessed 24 August 2023); and Seglins, D., Cribb, R., and Gomez, C. (2016) "Inside 10 Cases Where the RCMP Hit a Digital Wall" *CBC News* (15 November 2016), https://www.cbc.ca/news/investigates/police-power-privacy-rcmp-cases-1.3850783 (accessed 24 August 2023).

was revealed that the RCMP had used spyware ("on-device investigative tools," or ODITs) to access suspects' mobile phones and laptops in a number of investigations between 2018 and 2020.[5] Strikingly, the use of such technology by the police was not only kept from the public but also from the Office of the Privacy Commissioner. Speaking to the Standing Committee on Access to Information, Privacy, and Ethics in August 2022, Commissioner Philippe Dufresne indicated that his office had not been consulted about or even informed of the RCMP's use of ODITs, and only became aware of the practice as a result of media reports.[6] Despite these revelations, the RCMP have since continued to maintain that more needs to be done to help them overcome the challenges posed by encryption. At the time of writing, for example, it remains the position of the Canadian Association of Chiefs of Police that the law should be amended to require the holder of an encryption key or password to make it available to law enforcement (provided judicial authorization has been obtained).[7]

In contrast to the position taken by the RCMP and the Canadian Association of Chiefs of Police, privacy advocates, civil society groups, and academics have raised significant concerns about the prospect of making it easier for the police and security services to access Canadians' encrypted data and communications. In a comprehensive 2018 independent report on encryption in Canada, *Shining a Light on the Encryption Debate: A Canadian Field Guide*, Citizen Lab and the Canadian Internet Policy and Public Interest Clinic argued that the police repeatedly exaggerate the extent of the "going dark" problem, and that their existing information sources are more than sufficient to deal with the challenges raised by encryption:

[5] Forrest, M. (2022) "Canada's National Police Force Admits Use of Spyware to Hack Phones" *Politico* (29 June 2022), https://www.politico.com/news/2022/06/29/canada-national-police-spyware-phones-00043092 (accessed 23 August 2023). In response to a question from Conservative MP Tako Van Popta on 6 May 2022, the RCMP admitted to using ODITs to access data and to take control of mobile phone cameras and microphones. See House of Commons, Order/Address of the House of Commons, Q-566, Sessional Paper 8555-441-566 (22 June 2022). Following the tabling of this response, the Standing Committee on Access to Information, Privacy and Ethics passed a motion to study the RCMP's use of ODITs. See House of Commons (Canada) Standing Committee on Access to Information, Privacy and Ethics. (2022) *Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues.* Report (November 2022), 44th Parliament, 1st Session [hereafter "Standing Committee Report on Device Investigative Tools"].

[6] Standing Committee Report on Device Investigative Tools (ibid), 12.

[7] Canadian Association of Chiefs of Police (2016) *Resolutions Adopted at the 111th Annual Conference*. August 2016, pp. 19–20 (Resolution #03), https://cacp.ca/resolution.html?asst_id=1197 (accessed 11 September 2023.

> Though encryption will inevitably shield some data from state agencies, law enforcement and intelligence agencies generally do not lack the information necessary to do their work. Far from "going dark," more information about individuals' private lives is available today than at any previous moment in human history. Business incentives continue to favour the creation and aggregation of data in formats which remain accessible to service providers, state agents, and other third parties in unencrypted formats… A holistic and contextual analysis of the encryption debate makes clear that the investigative and intelligence costs imposed by unrestricted public access to strong encryption technology are often overstated.[8]

The authors of the report also went to considerable lengths to outline what is at stake when it comes to efforts to weaken or circumvent encryption. They noted that in addition to the economic benefits that flow from private and secure commercial and financial transactions, encryption is "intimately connected" to a number of fundamental rights, chief among them the right to privacy and the right to freedom of expression. Going further, they also argued that the availability of encryption – and the privacy that goes with it – provides a vital counterbalance to the growing surveillance capacities of the Canadian state:

> In an era where signals intelligence agencies operate with minimal restrictions on their foreign facing activities, encryption remains one of the few practical limits on mass surveillance... The mere awareness of mass surveillance exerts a significant chilling effect on freedom of expression. Vulnerable and marginalized groups are both disproportionately subject to state scrutiny, and may be particularly vulnerable to these chilling effects. Democracies pay a particularly high price when minority voices and dissenting views are pressured to self-censor or refrain from participating in public life... Uncompromised encryption systems can thus foster the security necessary for meaningful inclusion, democratic engagement, and equal access in the digital sphere.[9]

[8] Gill, L., Israel, T., and Parsons, C. (2018) *Shining a Light on the Encryption Debate: A Canadian Field Guide*. Citizen Lab and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf (accessed 24 August 2023), iv. The argument that the police have overstated the investigative challenges posed by encryption is one that has been echoed by Ann Cavoukian, Ontario's former privacy commissioner. According to Cavoukian, the police typically have more than enough information to investigate and prevent crime, and while encryption may be a barrier, it is far from an insurmountable one. Instead, the challenge lies with connecting the dots and putting "all the pieces together." See Seglins, Cribb, and Gomez (2016) "RCMP Want New Powers" (above n 4). A similar point has also been made by commentators in the US context. See Swire, P. and Ahmad, K. (2011) "'Going Dark' Versus a 'Golden Age for Surveillance.'" Center for Democracy and Technology, https://cdt.org/insights/going-dark-versus-a-golden-age-for-surveillance/ (Accessed 24 August 2023).

[9] Gill, Israel, and Parsons (2018) *Shining a Light on the Encryption Debate* (above n 8), i.

In the five years since the publication of *Shining a Light on the Encryption Debate*, these key arguments – that the police routinely overstate the extent of the "going dark" problem and that encryption is vital to the protection of privacy, freedom of expression, and a range of democratic values – remain at the heart of the debate over lawful access in Canada. At the same time, there is evidence to suggest that the public's attitudes towards the police and security services – which have generally been positive in Canada – may be changing.[10] According to the results of the last three RCMP Client and Partner Surveys, the public's trust and confidence in the RCMP has been steadily declining from 69% in 2019–20 to 60% in 2020–21 and yet further to 53% in 2021–22.[11] Similar declines have also been reported in relation to a number of provincial police services, particularly since March 2020 and the COVID pandemic.[12] Although attitudes towards the Canadian Security Intelligence Service (CSIS) remain largely positive, a recent report commissioned by CSIS found that only 63% of those surveyed 'somewhat' trusted the organization to safeguard Canadian's rights and freedoms.[13]

It is against the backdrop of the "going dark" problem and the changing landscape of attitudes towards law enforcement that this report offers some reflections on encryption and the lawful access debate in Canada. More specifically, it aims to draw attention to two often neglected aspects of this debate: the public dimensions of privacy and the importance of maintaining trust in the police and security services. Broadening our understanding of the type of privacy interests at stake in conversations about encryption – to include not just individual privacy but also public and collective aspects of privacy – is important if we are to properly weigh the costs of expanding the powers of the police to lawfully access encrypted communications and data.

[10] Ruddell, R. (2022) "The Changing Context of Canadian Policing: An Examination of the Public's Perceptions after 2020" *Journal of Community Safety and Well-Being* 7(2): 47–52.

[11] Royal Canadian Mounted Police (2020) *Client and Partner Survey Results, 2019–2020*; Royal Canadian Mounted Police (2021) *Client and Partner Survey Results, 2020–2021*; Royal Canadian Mounted Police (2022) *Client and Partner Survey Results, 2021–2022*. All available at https://www.rcmp-grc.gc.ca/en/reports-research-and-publications/client-and-partner-survey-results (accessed 11 September 2023).

[12] Ruddell (2022) (above n 10), 48–49.

[13] EKOS Research Associates. (2021) "Attitudes to the Canadian Security Intelligence Service (CSIS): Report," https://publications.gc.ca/collections/collection_2021/scrs-csis/PS74-8-2-2021-eng.pdf (accessed 31 October 2023). See also Marhnouj, S. (2022) "CSIS survey finds majority of Canadians leery of giving more powers to police, intelligence agencies" *The Globe and Mail* (16 January 2022), https://www.theglobeandmail.com/politics/article-csis-survey-finds-canadians-leery-of-giving-more-powers-to/ (accessed 14 November 2023).

Similarly, it is in the interest of the police and security services to consider the possible impact of any such an expansion on institutional trust. Given that law enforcement agencies in Canada rely extensively on the public's support to carry out many of their duties, any loss of trust or confidence arising from efforts to undermine or overcome encryption must be balanced against the supposed benefits of expanding lawful access and combating the "going dark" problem.

At the outset, it is important to note that this report does not consider whether lawful access in Canada should be reformed to make it easier (or more difficult) for the police and security services to respond to the challenges of encryption. Equally, it does not examine claims by law enforcement, privacy advocates, civil society, or academics about the nature, extent, or future of the "going dark" problem. There is already an extensive literature on both the legal landscape of lawful access in Canada and the question of whether the police and security services need additional powers to deal with the growing use of encryption.[14] What this report aims to do is to place the relationship between the public and the Canadian state at the heart of the discussion over lawful access.

To date, the "going dark" problem in Canada has largely been framed in terms of a tension between public goods (safety and security) on the one hand and individual rights (to privacy and freedom of expression) on the other.[15] The reality is, however, considerably more complex. While expanding lawful access clearly has the potential to weaken individual rights and

[14] In addition to works previously cited, see also Penney, S. and Gibbs, D. (2017) "Law Enforcement Access to Encrypted Data: Legislative Responses and the Charter" *McGill Law Journal* 63(2): 201–45; Dheri, P. and Cobey, D. (2019) *Lawful Access & Encryption in Canada: A Policy Framework Proposal*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3470957 (accessed 11 September 2023); Parsons, C. (2019) "Canada's New and Irresponsible Encryption Policy How the Government of Canada's New Policy Threatens Charter Rights, Cybersecurity, Economic Growth, and Foreign Policy" Citizen Lab (University of Toronto), https://citizenlab.ca/2019/08/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cybersecurity-economic-growth-and-foreign-policy/ (accessed 11 September 2023); West, L. and Forcese, C. (2020) "Twisted into Knots: Canada's Challenges in Lawful Access to Encrypted Communications" *Common Law World Review* 49(3–4): 182–98; and Masoodi, M.J. and Rand, A. (2021) *Why Canada Must Defend Encryption*, https://static1.squarespace.com/static/5e9ce713321491043ea045ef/t/61401f669251e7128c8bf757/1631592298920/WhyCanadaMustDefendEncryption_V5.pdf (accessed 11 September 2023).

[15] In this respect, such discussions echo broader and longstanding arguments over the appropriate balance to be struck between security and human rights in constitutional democracies such as Canada, with the central question being: to what extent are we willing to let the state infringe or weaken certain rights (such as privacy) in exchange for the promise of greater safety and security?

freedoms, insofar as those rights and freedoms have a public aspect, expanding lawful access may also undermine *collective* interests and values that are important to the proper functioning of Canada's constitutional democracy. Similarly, although it may be tempting for the police and security services to view more extensive investigatory powers as an unambiguous good when it comes to the challenges posed by encryption, the use of such powers may significantly undermine public trust and erode their relationship with the communities they seek to protect.

In the sections that follow, this report focuses on the role that privacy plays in setting boundaries for the exercise of state power, and the complex dynamics of trust when it comes to the use of that power by state agents such as the police and security services. In doing so, it aims to show that current debate over lawful access is as much about how we see the relationship between the public and the state as it is about the challenges posed by encryption and respect for individual rights.

LAWFUL ACCESS AND THE VALUE OF PRIVACY

To date, concerns about the implications of expanding lawful access in Canada – particularly as it relates to the use of encryption to secure data in transit and at rest – have largely focused on two related aspects of privacy: the importance of privacy as an individual right; and the relationship between privacy and other *Charter*-protected rights (such as freedom of expression and freedom of association). With regards to the first of these, civil society and human rights advocates have repeatedly drawn attention to the important role played by encryption in the protection of individual privacy. As more and more of our everyday activities are conducted online and the surveillance capacities of the state and private sector have steadily expanded, Canadians have understandably looked to encryption as a relatively accessible means of securing a degree of privacy in their digital lives. As the authors of *Shining a Light* have noted:

> Encryption is essential to preserving the privacy and integrity of countless digital interactions in an era where communication occurs on globalized traffic flows that are routinely subjected to mass and untargeted surveillance by a range of government agencies worldwide. Increasingly, encryption provides one of the only reliable, pragmatic

> safeguards against such untargeted state surveillance, carving out private spaces that would otherwise be impossible online.[16]

Although these private spaces may be virtual ones, their importance should not be underestimated. Through digital communications, the consumption of electronic media, and as members of online communities, Canadians are able to explore aspects of their identity, form personal and intimate relationships, and share views and information with others. Easy access to encrypted communications apps – such as Signal, Telegram, and WhatsApp – and the inclusion of on-device encryption provided by companies like Apple and Microsoft have made it possible for individuals to maintain a degree of privacy in their online activities, and to avoid the chilling effects of scrutiny by government, private companies, and other people.

As many commentators have noted, however, the value of privacy goes beyond justifications based on ideas of personal autonomy, identity, and self-determination.[17] Privacy is also important because it provides the foundation for the exercise of other fundamental rights and freedoms, chief among them freedom of expression and freedom of association. By enabling individuals to limit who has access to their communications – and to choose who they share their ideas and information with – privacy allows for the creation of spaces in which different opinions and beliefs can flourish. As noted by the US National Academy of Sciences:

> Since the explosion of Internet availability and electronic communications capability around the world, exercising of the freedoms of speech and belief, including the right to obtain information, depends more and more on the ability to access the Internet and communicate electronically. As electronic communications and Internet access are subject to electronic surveillance, the right to privacy for one's political, religious, and other communications, opinions, and activities has become even more important… These developments have led to the view that encryption, which protects the privacy of communications and sensitive information, has become an intrinsic part of the rights to freedoms of speech and belief.[18]

[16] Gill, Israel, and Parsons (2018) *Shining a Light on the Encryption Debate* (above n 8), 12.

[17] See: Regan, P.M. (1995) *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press); Solove, D.J. (2002) *Understanding Privacy* (Harvard University Press); Solove, D.J. (2004) *The Digital Person: Technology and Privacy in the Information Age* (New York University Press); and Nissenbaum, H. (2009) *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press).

[18] National Academies of Sciences, Engineering, and Medicine. (2018) *Decrypting the Encryption Debate: A Framework for Decision Makers* (National Academies Press), 34.

Looked at from this perspective, it is clear that privacy has an inescapably political dimension. Insofar as freedom of expression, freedom of association, and freedom of belief are central to the proper functioning of any healthy democracy, privacy is also fundamentally important. Without privacy, it becomes harder for individuals and communities to organise themselves politically or to engage in forms of political resistance. This is especially true for vulnerable populations and the politically marginalised faced with an antagonistic state:

> Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities.[19]

Although we may be reluctant to view the Canadian political, social, religious, and legal environment as hostile when discussing questions of lawful access and the powers of the police and security services, it is important for such discussions to look beyond the present. Once granted, powers conferred to agents of the state like the police are rarely withdrawn or curtailed, and while we may not be concerned about the misuse of such powers in the current political climate, circumstances can change. Similarly, before expanding the surveillance capacities of the state to allow the police and security services to use ODITs or other forms of lawful hacking, lawmakers and the public should consider the risk that such capacities may be misused in the future. Put another way, protecting privacy and maintaining limits on lawful access are as much about "future proofing" key political rights as it is about securing these rights in the present.[20]

As has already been noted, these two aspects of privacy – the personal and the political – have been repeatedly referred to in discussions about lawful access and encryption in Canada over the past twenty years. There is, however, another aspect of privacy that is also worthy of consideration in this context. This is the idea that privacy is essential to the rule of law and

[19] Kaye, D (2016) *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UNHRC, 29th Sess, UN Doc A/HRC/29/32, 5 (para. 12).

[20] On this point and the relationship between surveillance and repression more generally, see Haggerty, K. (2014) "What's Wrong with Privacy Protections? Provocations from a Fifth Columnist" in A. Sarat (ed), *A World without Privacy: What Law Can and Should Do?* (Cambridge University Press), 190–222.

provides important limits on the powers of the state. This argument has been made by Professor Lisa Austin, who has suggested that the existing approach to privacy in Canada – particularly as it relates to questions of state surveillance – is overly restrictive:

> My argument is that these core aspects of the rule of law have implicitly shaped our legal definition of privacy but have done so in a partial manner and in a manner that supports a narrow conception of privacy. The ironic consequence is that the legal discourse of privacy now often helps to support the expansion of the discretionary authority of state agents rather than works to constrain it—undermining rather than upholding the rule of law. In order to be more responsive to new forms of surveillance, our privacy jurisprudence requires a more explicit focus and richer understanding of the demands of these core rule of law principles.[21]

According to Austin, the right to privacy established by the *Charter* – which derives from the prohibition on unreasonable search and seizure in Section 8 – is grounded not in ideas of property but rather in a commitment to the rule of law and the need to constrain the power of the state.[22] Looked at in this way, privacy plays an important role in regulating (and limiting) the discretionary authority of the police and security services by helping to ensure that those who have power over us exercise that power in a manner that is consistent with rule-of-law values such as accountability and transparency.

To better understand Austin's insight, it is helpful to return to the recent revelations regarding the RCMP's use of ODITs. Even though the RCMP must obtain judicial authorization before using such technology, the lack of transparency around the use of ODITs raises significant rule-of-law concerns – most notably regarding fair notice. The fact that individuals had no way of knowing prior to 2022 that ODITs were being used by the RCMP means that they were unable to make informed decisions about their personal devices and the information stored on them. As Austin has pointed out:

> There is a strong tradition of understanding the value of the rule of law in terms of its ability to guide action. According to this view, what is central to the rule of law is the ability of individuals to plan their activities in light of potential legal liability. Values such

[21] Austin, L. (2012) "Getting Past Privacy? Surveillance, the Charter, and the Rule of Law" *Canadian Journal of Law and Society* 27: 381–98, 383.

[22] Austin, L. (2014) "Enough about Me: Why Privacy Is about Power, not Consent (or Harm)" in A. Sarat (ed), *A World without Privacy: What Law Can and Should Do?* (Cambridge University Press).

> as predictability of expectations are central to this understanding. This planning role has been linked to an idea of legal liberty but also to ideas of autonomy and dignity.[23]

Looked at from this perspective, the use of ODITs by the RCMP was problematic not only in terms of individual privacy – and related rights to freedom of expression and association – but also for the rule of law. While important, legal accountability via judicial oversight only goes part of the way towards ensuring that the police are properly subject to the rule of law. In addition, there needs to be transparency around the range of powers and investigative techniques available to them. This is a point that was stressed by the Privacy Commissioner Philippe Dufresne in his recent evidence to the Standing Committee on Access to Information, Privacy and Ethics:

> [T]he impact of this type of information coming out in the public through media reports or questions can raise questions and can raise concerns. I think from a trust standpoint and generating confidence, it would be far preferable that privacy impact assessments be done at the front end, that my office be consulted, and that this can be conveyed somehow to Canadians so that they are reassured that there are institutions there, such as my office, to provide advice and to make sure that privacy is top of mind.[24]

Drawing rule-of-law concerns into discussions about lawful access and encryption is important because it reminds us that privacy is not just about protecting individual interests or facilitating the exercise of other rights. It is also about placing meaningful constraints on the power of the state. Indeed, Jed Rubenfeld and others have argued that focusing exclusively on the "personhood" aspects of privacy is a mistake, and we must instead place the state squarely at the heart of our analysis:

> The right to privacy is a political doctrine. It does not exist because individuals have a sphere of "private" life with which the state has nothing to do. The state has everything to do with our private life; and the freedom that privacy protects equally extends, as we have seen, into "public" as well as "private" matters. The right to privacy exists because

[23] Austin (2012) (above n 21), 386–87 (original footnote omitted).

[24] Standing Committee Report on Device Investigative Tools (above n 5), 12.

> democracy must impose limits on the extent of control and direction that the state exercises over the day-to-day conduct of individual lives.[25]

Although Rubenfeld's "anti-totalitarian" account of privacy has been criticized, his key insight that privacy can play an important role in constraining the expansionist tendencies of the state is important in the context of lawful access.[26] No matter how well intentioned, calls from the police and security services for more tools to address the "going dark" problem and the challenges of encryption demand that we ask ourselves a fundamental question: how far are we, as members of a constitutional democracy, willing to let the state enter into our lives in the pursuit of security and public safety? Although concerns about individual privacy, freedom of expression, freedom of association, and the rule of law take us some of the way to answering this, we also have to consider larger questions about the role of the state and the limits of its power.

Aside from providing a different perspective on the "going dark" debate, putting the state at the heart of our analysis is also helpful when it comes to addressing one of the unique features of encryption: the possibility of absolute privacy. As law enforcement agencies often point out, the use of encryption differs from other forms of privacy protection – such as locks, passwords, and codes – in that it doesn't just make it harder for the state to access certain types of personal information: in some cases, encryption makes such access virtually impossible. Looked at from the perspective of the modern Canadian state – which has steadily expanded its surveillance powers over the course of the last century – the idea that individuals can now easily prevent law enforcement agencies from accessing their information is a disturbing one. However, for those concerned about the ever-expanding scope of state surveillance, the advent of encryption is a welcome development, not least because it forces us consider whether absolute privacy should be possible in a democracy like Canada. Put another way, if the only way to combat the challenges of the "going dark" problem is to restrict the use of encryption – or to allow law enforcement

[25] Rubenfeld, J. (1989) "The Right to Privacy" *Harvard Law Review* 102: 737–807, 804–5 (original footnote omitted).

[26] Solove, D.J. (2002) "Conceptualizing Privacy" *California Law Review* 90(4): 1087–155, 1120.

agencies to use deceptive means to circumvent it – then we can not avoid the asking the question: "Are there ever things the state simply cannot know about us?"[27]

As a final point, when thinking about lawful access and privacy it is helpful to reflect on other contexts in which the law imposes significant constraints on those involved in the administration of criminal justice. Although the analogy is far from perfect, a strong commitment to privacy in the context of policing helps to level the playing field between individuals and the state in a manner not dissimilar from due process rights in the context of the criminal trial. Just as the law deliberately places hurdles in front of the police and prosecutors via rules of procedure and evidence in recognition of the overwhelming power imbalance between criminal defendants and the Crown, restrictions on lawful access serve as a constraint on the surveillance power of the state. Put another way, it *should* be difficult for the police and security services to access encrypted information, if only because individuals are already at a significant disadvantage when it comes to maintaining a degree of privacy vis-a-vis the state.

SURVEILLANCE, TRANSPARENCY, AND TRUST

Outside of privacy, discussions of lawful access in Canada have also raised concerns about the possible impact on public trust – in the security provided by encryption technologies, and also in law enforcement agencies and other state institutions. With regard to the first type of public trust, it is perhaps enough to acknowledge here that encryption technologies are vital to commerce (the digital marketplace in particular), and there are fairly obvious economic costs that would flow from weakening public trust in such technology. It is the second type of public trust – trust in the police, the security services, and the state more generally – that will be explored in this section, particularly with respect to its relationship to lawful access, surveillance, and encryption.

Although maintaining trust in government and state institutions is often cited as a reason for limiting lawful access for the police and security services, what is meant by trust and why it is important in this context is not always clear. In some cases, trust is simply presented as a good *per se*, with the need to maintain public trust used as a justification for increased transparency

[27] I am grateful to Robert Diab for his insights regarding the relationship between encryption and absolute privacy.

and accountability in policing and state surveillance. More recently, however, trust has come to been framed in terms of its role in fostering democratic participation and public engagement. For example, in evidence given to the Standing Committee on Access to Information, Privacy and Ethics during their inquiry into the use of ODITs by the RCMP, the Privacy Commissioner of Canada drew a direct link between privacy, trust, and the public's engagement with government:

> Privacy as an accelerator of Canadians' trust in their institutions and in their participation as digital citizens means that when organizations such as the RCMP consider privacy impacts at the front end and are seen to be doing so, this generates trust and reassures Canadians about the necessity of the tools and the measures put in place to mitigate privacy impacts and ensure proportionality between the measures and the objectives.[28]

Speaking in a similar vein, the Minister of Public Safety Marco Mendicino noted later the same day that "trust is one of the keys to openness and transparency," before going on to state that "we need to maintain trust everywhere so that we can use this tool in a way that respects the Charter and all the rights it provides."[29]

Although linking trust and transparency in this way – with the promotion of trust serving as a justification for greater transparency – might appear to be unproblematic, the assumption that more transparency is always and inevitably a good thing is one that deserves further examination. This is particularly true when it comes to the use of surveillance technologies by the police and security services. Although transparency is often cited as a necessary prerequisite for institutional accountability, it can also play a role in the normalization of activities that should be seen as exceptional. In the introduction to a recent collection of academic papers on trust, transparency, and surveillance, the editors have noted that if we consider "transparency as a political practice, rather than merely as the disclosure of information, we can begin to understand how transparency can come to have counter-intuitive effects, such as the legitimation, and even extension, of state surveillance powers."[30] In a chapter in the same volume, Lora Anne Viola has argued that in certain instances, transparency – particularly when it comes as a response to

[28] Evidence to the Standing Committee on Access to Information, Privacy and Ethics, 44th Parliament, 1st Session, Number 030 (Monday, August 8, 2022), 2.

[29] Evidence to the Standing Committee on Access to Information, Privacy and Ethics, 44th Parliament, 1st Session, Number 031 (Monday, August 8, 2022), 5.

[30] Viola, L.A. and Laidler, P. (2022) *Trust and Transparency in an Age of Surveillance* (Routledge), 7.

revelations about previously undisclosed state surveillance activities – can have what she refers to as a *condoning effect*:

> [This effect] is triggered when high levels of revealed noncompliance reduce the perceived social opprobrium for violating the norm and lead instead to demands for normalizing or legitimizing the behavior. The revelations that follow from transparency offer an opportunity not only to condemn the behavior, as an accountability approach might argue, but also to discuss and normalize it. In the case of surveillance, exposure of illegal surveillance led both to public outrage and to debates about how to legalize it. Thus, under the guise of reform legislation, many illegal surveillance practices exposed by Snowden were given a legal basis and, therefore, legitimized. Arguably, the widespread revelations of surveillance—not just by the NSA but also by private firms such as Facebook—have normalized the idea of collecting and utilizing mass data. Exposure and disclosure imply that the behavior is more widespread than anticipated, thus removing the taboo.[31]

Returning to the 2022 revelations regarding the RCMP's use of ODIT, it is easy to see this condoning effect in action. Despite initial concerns, the debate over the use of such technology quickly shifted from questions of whether it should be allowed to questions about how it should be better regulated – with discussions about the need for greater transparency and accountability moving to the forefront of the debate. Looked at from this perspective, it can be argued that policymakers and legislators need to exercise care when revisiting longstanding calls for expanded powers of lawful access: discussing new police investigative techniques and surveillance technologies, even when accompanied by calls for increased transparency and clearer regulation, may have the effect of normalising them.

Assuming that the benefits of greater transparency outweigh the dangers of any potential condoning effect when it comes to lawful access, the end goal – the promotion and maintenance of public trust – still needs to be interrogated in the context of discussions about encryption and police powers. Although rarely stated explicitly, the importance placed on trust in discussions about lawful access is predicated on a key assumption: that there is a direct relationship between surveillance, privacy and trust, and that any changes to the regime of lawful access – particularly changes that undermine individual privacy – may lead to a loss of that trust. Writing in 2019,

[31] Viola, L.A. (2022) "The Limits of Transparency as a Tool for Regulating Surveillance: A Comparative Study of the United States, United Kingdom, and Germany" in Viola and Laidler (eds) (2022) (ibid), 21–46, 28 (original footnote omitted).

Dheri and Cobey drew on this assumption in their arguments for law enforcement agencies developing and publishing their own best practice guidelines for encryption workarounds:

> Currently, the public is unaware of how law enforcement agencies, and the Canadian Public Safety portfolio as a whole, deals with encryption. … [N]ondisclosure of internal policies [regarding encryption workarounds] allows critics to fill the void with speculation—however accurate or inaccurate it may be. Speculation can result in negative reputational and public trust consequences for an organization and may even work to undermine legitimate law enforcement objectives. Since Canadian law enforcement agencies are operating in a time of mistrust and fake news, and in a time when democracies across the world are under threat, public perception considerations take on even greater eminence. The development and disclosure of encryption best practices would be an important step towards greater transparency and a healthier democracy.[32]

This same assumption underpins much of the discussion of ODITs in Chapter 1 of the 2022 Standing Committee report. The need to maintain confidence in public institutions – such as the police and security services – is referred to by a number of witnesses as a justification for greater transparency around the use of such technology, as well as for more oversight from privacy regulators and the courts. What is not discussed, however, is the nature of the relationship between surveillance, privacy, and trust, or why more surveillance leads to less trust.

Although it may seem obvious that the use of surveillance technologies by the state has the potential to undermine public trust – in both the particular institutions carrying out surveillance and the state more generally – the picture that emerges from the research literature is less clear. As Björklund has noted, there is empirical evidence to suggest that "high levels of trust predict positive attitudes to surveillance."[33] More specifically, she has pointed to recent surveys conducted in Europe that found that the level of trust in state institutions, security agencies in particular, can have a positive impact on the public's willingness to accept certain types of surveillance practices and technologies. According to a 2015 study conducted in Europe, for example, there appeared to be a clear relationship between how people view security services

[32] Dheri, P. and Cobey, D. (2019) *Lawful Access & Encryption in Canada: A Policy Framework Proposal*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3470957 (accessed 11 September 2023), 29.

[33] Björklund, F. (2022) "Trust and Surveillance: An Odd Couple or a Perfect Pair?" in Viola and Laidler (eds) (2022) (above n 30), 183. Björklund has also drawn attention to specific case studies, a number of which involve the surveillance of Muslim communities in the United States and United Kingdom, where it was found that surveillance had the opposite effect, leading to a loss of trust in state agencies.

and their willingness to accept certain types of surveillance-orientated security technologies [SOSTs]:

> The more people trust scientific and political institutions, in this case security agents, the more acceptable a technology would be. Our study clearly confirms this hypothesis. In practical terms, this means that, when it comes to SOSTs, security agencies and institutions should be significantly more concerned about the degree of trust they enjoy than about how well technologies are known to the public or how familiar people are with those technologies. If we wanted to know more about the effect of each sub-dimension of institutional trustworthiness on acceptability, we might look at other analyses of these data reported in other publications and notice how security agents' ability, integrity and benevolence play a more or less important role in the case of each specific SOST.[34]

As the authors of this study go on to note, many other factors may also affect how the public responds to surveillance technologies, including perceived intrusiveness, perceived effectiveness, and concerns about privacy. What these and similar findings suggest is that existing levels of trust matter when it comes to the subsequent willingness (or unwillingness) of the public to accept an expansion in the surveillance powers of the state. Given that confidence in the RCMP has fallen in recent years, there is a danger that any move to expand the scope of lawful access in Canada may meet considerable public resistance and only exacerbate existing problems of trust.

Returning to Björklund's work on trust, she has also noted that institutional ideas of trust – such as the ones that underpin the survey cited above – are problematic because the public is often not in a position to judge the effectiveness of particular surveillance practices or the performance of agencies such as the police or security services. It is for this reason that Björklund argues for studies that also encompass what she refers to as a sociocultural perspective:

> The real merit of a sociocultural perspective on trust and surveillance is that it can account for movements coming from below that reflect what happens in people's everyday lives. Norms are not easily changed, but from a sociocultural perspective trust as a norm originates in experiences that we have from people we meet in our daily contacts and personal networks. Therefore, a sociocultural perspective accommodates the

[34] Pavone, V., Degli-Esposti, S., and Santiago, E. (2015) *Key Factors Affecting Public Acceptance and Acceptability of SOSTs* (European University Institute), 136. See also Degli-Esposti, S., and Santiago Gómez, E. (2015) "Acceptable Surveillance-Orientated Security Technologies: Insights from the SurPRISE Project" *Surveillance & Society* 13(3/4): 437–454.

> possibility that surveillance may destroy trust as we know it. If trust is about socialization and comes from experiences in close relations, then negative experiences with, for example, the local police may destroy trust from below with long-term effects on other types of trust and on norms of trust in a society. Thus, although social survey studies find a positive relationship between trust and acceptance of surveillance, the more qualitative case studies referred to above, indicating a negative association, may tell something about what we should expect from the future.[35]

What is being suggested here is that trust operates on different levels and can work in different directions. Although high levels of trust in the police as an institution may lead the public to be more accepting of certain types of surveillance, at the same time, the actual experiences of the individuals and communities exposed to that surveillance may lead to a subsequent loss of trust – in both the police and the state more generally. Returning to the context of lawful access and encryption, what this suggests is that *how* the police and security services use any new technologies and powers aimed at combating the "going dark" problem is likely to play a role in the generation (or erosion) of trust. For example, if there is an expansion in the use of lawful access techniques – and these techniques are primarily used to investigate individuals and communities that are already over-policed – public trust is likely to suffer. Taken together, the institutional and socio-cultural perspectives on trust demonstrate that in the context of surveillance at least, trust is a *resource* that can be drawn on when introducing new surveillance measures, but it can easily be lost depending on how those measures are implemented and experienced by the public.

Before leaving questions of transparency and trust, it is important to address issues of scope in relation to lawful access and the "going dark" debate. On the one hand, it can be argued that efforts on the part of the police and security services to overcome encryption are most likely to be limited in scope and targeted narrowly at a very small number of individuals and criminal organisations.[36] As a consequence, care needs to be taken when discussing the likely impact of such measures on public trust in the police and security services. Having said this, it is also important to be mindful of two related factors: the ubiquity of encryption and the dangers of

[35] Björklund (2022) (above n 33), 194.

[36] See, for example, statements made to the Standing Committee on Access to Information, Privacy and Ethics as part of their inquiry into the use of ODITs. Standing Committee Report on Device Investigative Tools (above n 5), 21.

function creep. Because the encryption of data-at-rest and in-transit has now become so widespread, the current limited use of techniques such as lawful hacking and ODITs may be expanded by law enforcement in the future, particularly as the technology to do so becomes cheaper and easier to deploy. Certainly, this has been true with respect to other forms of police surveillance in Canada, with electronic wiretapping and video surveillance being key examples. As a consequence, any discussion of expanding lawful access should be premised on the assumption that the use of encryption workarounds may become more commonplace over time.

In a similar vein, the argument that lawful hacking and the use of ODITs are only ever likely to be used in the investigation of serious crime or terrorism needs to be treated with a degree of scepticism. Surveillance technologies have a well-documented tendency towards function creep, frequently being used in ways not originally intended when they are first developed or deployed.[37] Moreover, this tendency is often accelerated by events that generate fear about crime, security, and public safety – as seen in the years following the attacks of 11 September 2001 and more recently during the COVID pandemic.[38] Once authorised by law and normalised via efforts at ensuring transparency and accountability. it becomes relatively easy for exceptional powers of lawful access to be used in contexts that go well beyond the "going dark" problem. As noted earlier, the prospect of lawful access being expanded in the future – particularly with regard to the use of encryption – should not necessarily prohibit policymakers, legislators, law enforcement, and the public from discussing the merits of new technologies and expanded powers. We should, however, be clear-eyed about the fact that, as history has shown time and time again, once authorised by law and normalised through use, surveillance practices and technologies are rarely if ever reconsidered, curtailed, or otherwise abandoned.

[37] Koops, B. J., (2021) "The concept of function creep" *Law, Innovation and Technology* 13(1): 29‒56.

[38] See: Lyon, D., and Haggerty, K. D. (2012) "The surveillance legacies of 9/11: Recalling, reflecting on, and rethinking surveillance in the security era" *Canadian Journal of Law and Society* 27(3): 291‒300; Newell, B. (2021) "Introduction: surveillance and the COVID-19 pandemic: views from around the world" *Surveillance & Society* 19(1): 81‒84.

CONCLUSION

Over the last twenty years, discussions about encryption, police powers, and lawful access in Canada have focused on a range of issues related to privacy, transparency, and trust. This report has sought to highlight some neglected aspects of each of these issues, most notably:

(1) The relationship between privacy, the rule of law, and the boundaries of state power;

(2) The role that transparency can play in condoning or otherwise legitimising forms of state surveillance; and

(3) The complex nature of trust in the context of surveillance, particularly with respect to public attitudes to the police and security services.

In attempting to show that the value of privacy goes beyond its status as an individual right – and that the relationship between transparency, trust and surveillance is inherently complex and multidirectional – this report aims to provide members of the National Security and Intelligence Committee of Parliamentarians with additional perspectives on the "going dark" debate. In particular, this report should be seen as a call to put our vision of the state at the centre of any discussion of lawful access, police powers, and the challenges of encryption. Too often, debates about new forms of surveillance start from the assumption that it is for individuals and the community to provide reasons why the state should not be able to expand its surveillance powers in response to some newly identified threat to public safety or security. In this respect, the public is almost always "playing defence", having to provide reasons why privacy still matters and why limits need to be imposed on emerging police surveillance technologies. However, if we start from a different place, one that accepts that there may be things the state cannot know and places it cannot go, then the discussion takes a different turn.

Encryption clearly presents a significant challenge to the police and security services. Regardless of whether the "going dark" problem has been overstated by law enforcement agencies in Canada or not, there is little doubt that encryption does make investigating serious crime more difficult. But encryption, for perhaps the first time, also offers individuals the possibility of absolute privacy, setting real limits on the expanding surveillance powers of the state. As a consequence, debates about the future of lawful access in Canada should look beyond the tension between individual rights and the pursuit of security, and instead be seen more broadly as part of an ongoing discussion about the fundamental relationship between Canadian state and the public it serves.

REFERENCES

Austin, L. (2012) "Getting Past Privacy? Surveillance, the Charter, and the Rule of Law" *Canadian Journal of Law and Society* 27: 381–98.

—— (2014) "Enough about Me: Why Privacy Is about Power, not Consent (or Harm)" in A. Sarat (ed), *A World without Privacy: What Law Can and Should Do?* (Cambridge University Press).

Björklund, F. (2022) "Trust and Surveillance: An Odd Couple or a Perfect Pair?" in L.A. Viola and P. Laidler, *Trust and Transparency in an Age of Surveillance* (Taylor & Francis).

Canadian Association of Chiefs of Police. (2016) "Resolutions Adopted at the 111th Annual Conference" (August 2016), https://cacp.ca/resolution.html?asst_id=1197 (accessed 31 October 2023).

Degli-Esposti, S., and Santiago Gómez, E. (2015) "Acceptable Surveillance-Orientated Security Technologies: Insights from the SurPRISE Project" *Surveillance & Society* 13(3/4): 437–454.

Dheri, P. and Cobey, D. (2019) "Lawful Access and Encryption in Canada: A Policy Framework Proposal," https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3470957 (accessed 11 September 2023).

Diab, R. (2019) "The Road Not Taken: Missing Powers to Compel Decryption in Bill C-59, Ticking Bombs, and the Future of the Encryption Debate" *Alberta Law Review* 57: 267–96.

EKOS Research Associate. (2021) "Attitudes to the Canadian Security Intelligence Service (CSIS): Report," https://publications.gc.ca/collections/collection_2021/scrs-csis/PS74-8-2-2021-eng.pdf (accessed 31 October 2023).

House of Commons (Canada) Standing Committee on Access to Information, Privacy and Ethics. (2022) Evidence: Number 030 (Monday, 8 August 2022), 44th Parliament, 1st Session, https://publications.gc.ca/collections/collection_2022/parl/xc73-1/XC73-1-2-441-30-eng.pdf (accessed 15 November 2023).

—— (2022) Evidence: Number 031 (Monday, 8 August 2022), 44th Parliament, 1st Session, https://publications.gc.ca/collections/collection_2022/parl/xc73-1/XC73-1-2-441-31-eng.pdf (accessed 15 November 2023).

—— (2022) Evidence: Number 032 (Tuesday, 9 August 2022), 44th Parliament, 1st Session, https://publications.gc.ca/collections/collection_2022/parl/xc73-1/XC73-1-2-441-32-eng.pdf (accessed 15 November 2023).

—— (2022) Evidence: Number 033 (Tuesday, 9 August 2022), 44th Parliament, 1st Session, https://publications.gc.ca/collections/collection_2022/parl/xc73-1/XC73-1-2-441-33-eng.pdf (accessed 15 November 2023).

Forrest, M. (2022) "Canada's National Police Force Admits Use of Spyware to Hack Phones" *Politico* (29 June 2022), https://www.politico.com/news/2022/06/29/canada-national-police-spyware-phones-00043092 (accessed 23 August 2023).

Gill, L., Israel, T., and Parsons, C. (2018) *Shining a Light on the Encryption Debate: A Canadian Field Guide*, Citizen Lab and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-Light-Encryption-CitLab-CIPPIC.pdf (accessed 24 August 2023).

Government of Canada. (2016) *Our Security, Our Rights: National Security Green Paper Background Document*, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/index-en.aspx (accessed 11 September 2023).

—— (2022) *Response to the Seventh Report of the Standing Committee on Access to Information, Privacy and Ethics*, https://www.ourcommons.ca/content/Committee/441/ETHI/GovResponse/RP12299295/441_ETHI_Rpt07_GR/TreasuryBoardOfCanada-e.pdf (accessed 15 November 2023).

Haggerty, K. (2014) "What's Wrong with Privacy Protections? Provocations from a Fifth Columnist" in A. Sarat (ed), *A World without Privacy: What Law Can and Should Do?* (Cambridge University Press).

House of Commons, Order/Address of the House of Commons, Q-566, Sessional Paper 8555-441-566 (22 June 2022).

House of Commons (Canada) Standing Committee on Access to Information, Privacy and Ethics. (2022) *Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues*. Report (November 2022), 44th Parliament, 1st Session, https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP12078716/ethirp07/ethirp07-e.pdf (accessed 31 October 2023).

House of Commons (Canada) Standing Committee on Public Safety and National Security. (2017) *Protecting Canadians and their Rights: A New Road Map for Canada's National Security*. Report (May 2017), 42nd Parliament, 1st Session, https://publications.gc.ca/collections/collection_2017/parl/xc76-1/XC76-1-1-421-9-eng.pdf (accessed 31 October 2023).

Koops, B. J., (2021) "The concept of function creep" *Law, Innovation and Technology* 13(1): 29–56.

Kaye, D (2016) *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UNHRC, 29th Sess, UN Doc A/HRC/29/32.

Lyon, D., and Haggerty, K. D. (2012) "The surveillance legacies of 9/11: Recalling, reflecting on, and rethinking surveillance in the security era" *Canadian Journal of Law and Society* 27(3): 291–300.

Marhnouj, S. (2022) "CSIS survey finds majority of Canadians leery of giving more powers to police, intelligence agencies" *The Globe and Mail* (16 January 2022), https://www.theglobeandmail.com/politics/article-csis-survey-finds-canadians-leery-of-giving-more-powers-to/ (accessed 14 November 2023).

Masoodi, M.J. and Rand, A. (2021) *Why Canada Must Defend Encryption*, https://static1.squarespace.com/static/5e9ce713321491043ea045ef/t/61401f669251e7128c8bf757/1631592298920/WhyCanadaMustDefendEncryption_V5.pdf (accessed 11 September 2023).

National Academies of Sciences, Engineering, and Medicine. (2018) *Decrypting the Encryption Debate: A Framework for Decision-Makers* (National Academies Press).

National Security and Intelligence Review Agency (NSIRA). (2019) "Review of the CSIS–RCMP Relationship in a Region of Canada through the Lens of an Ongoing Investigation." NSIRA Review 2019-04, https://www.nsira-ossnr.gc.ca/wp-content/uploads/Redacted-Regional-NSIRA-Review-e-Updated.pdf (accessed 31 October 2023).

Newell, B. (2021) "Introduction: surveillance and the COVID-19 pandemic: views from around the world" *Surveillance & Society* 19(1): 81–84.

Nissenbaum, H. (2009) *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press).

Parsons, C. (2019) "Canada's New and Irresponsible Encryption Policy: How the Government of Canada's New Policy Threatens Charter Rights, Cybersecurity, Economic Growth, and Foreign Policy." Citizen Lab (University of Toronto), https://citizenlab.ca/2019/08/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cybersecurity-economic-growth-and-foreign-policy/ (accessed 11 September 2023).

Pavone, V., Degli-Esposti, S., and Santiago, E. (2015) *Key Factors Affecting Public Acceptance and Acceptability of SOSTs* (European University Institute).

Penney, S. and Gibbs, D. (2017) "Law Enforcement Access to Encrypted Data: Legislative Responses and the Charter" *McGill Law Journal* 63(2): 201–45.

Regan, P.M. (1995) *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press)

Royal Canadian Mounted Police. (2020) *Client and Partner Survey Results, 2019–2020*. Available at https://www.rcmp-grc.gc.ca/en/reports-research-and-publications/client-and-partner-survey-results (accessed 11 September 2023).

—— (2021) *Client and Partner Survey Results, 2020–2021*. Available at https://www.rcmp-grc.gc.ca/en/reports-research-and-publications/client-and-partner-survey-results (accessed 11 September 2023).

—— (2022) *Client and Partner Survey Results, 2021–2022*. Available at https://www.rcmp-grc.gc.ca/en/reports-research-and-publications/client-and-partner-survey-results (accessed 11 September 2023).

—— (2022) "Response to Order Paper Question Q-566, June 23, 2022, https://www.priv.gc.ca/en/privacy-and-transparency-at-the-opc/proactive-disclosure/opc-parl-bp/ethi_202200808/rcmp-response/ (accessed 22 June 2023).

Rubenfeld, J. (1989) "The Right to Privacy" *Harvard Law Review* 102: 737–807.

Ruddell, R. (2022) "The Changing Context of Canadian Policing: An Examination of the Public's Perceptions after 2020" *Journal of Community Safety and Well-Being* 7(2): 47–52.

Seglins, D., Cribb, R., and Gomez, C. (2016) "Inside 10 Cases Where the RCMP Hit a Digital Wall" *CBC News* (15 November 2016), https://www.cbc.ca/news/investigates/police-power-privacy-rcmp-cases-1.3850783 (accessed 24 August 2023).

—— (2016) "RCMP Boss Bob Paulson Says Force Needs Warrantless Access to ISP User Data" *CBC News* (15 November 2016), https://www.cbc.ca/news/investigates/police-power-privacy-paulson-1.3851955 (accessed 24 August 2023).

—— (2016) "RCMP Want New Powers to Bypass Digital Roadblocks in Terrorism, Major Crime Cases" *CBC News* (15 November 2016), https://www.cbc.ca/news/investigates/rcmp-digital-roadblocks-1.3850018 (accessed 24 August 2023).

Solove, D.J. (2002) "Conceptualizing Privacy" *California Law Review* 90(4): 1087–155.

Solove, D.J. (2002) *Understanding Privacy* (Harvard University Press).

Solove, D.J. (2004) *The Digital Person: Technology and Privacy in the Information Age* (New York University Press).

Swire, P. and Ahmad, K. (2011) "'Going Dark' Versus a 'Golden Age for Surveillance,'" Center for Democracy and Technology, https://cdt.org/insights/going-dark-versus-a-golden-age-for-surveillance/ (accessed 24 August 2023).

Tunney, T. (2018) "RCMP's Ability to Police Digital Realm 'Rapidly Declining,' Commissioner Warned" *CBC News* (5 October 2018), https://www.cbc.ca/news/politics/lucki-briefing-binde-cybercrime-1.4831340 (accessed 13 August 2023).

Viola, L.A. (2022) "The Limits of Transparency as a Tool for Regulating Surveillance. A Comparative Study of the United States, United Kingdom, and Germany" in L.A. Viola and P. Laidler (eds). (2022) *Trust and Transparency in an Age of Surveillance* (Routledge).

Viola, L.A. and Laidler, P. (eds). (2022) *Trust and Transparency in an Age of Surveillance* (Routledge).

West, L. and Forcese, C. (2020) “Twisted into Knots: Canada’s Challenges in Lawful Access to Encrypted Communications” *Common Law World Review* 49(3–4): 182–98.