GOVERNING PRIVACY IN THE DIGITAL AGE

By

Colton Fehr

A Thesis Submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

Faculty of Law

University of Alberta

Abstract

Courts and legislatures in Canada and around the world have struggled to respond to the challenges posed by rapidly advancing and complex technologies. As a result, American scholars have debated the appropriate role of each institution with respect to crafting criminal procedure rules implicating digital technologies. Yet, the Canadian literature has only sparsely addressed the ability of Canadian courts and legislatures to respond to the digital age. My dissertation begins to fill this gap in the literature. I do so by asking whether the judiciary and Parliament have been able to develop criminal procedure rules implicating digital technologies in an efficient, coherent, and fair manner. As with American courts, I find that the Canadian judiciary often lags behind technological advancement. Although for somewhat different reasons, Canadian judges also frequently fail to receive adequate evidence with which to craft digital privacy rules. Similarly, I conclude that Parliament's framework for governing state intrusions onto digital privacy has been patchwork and inconsistent. Unlike the American experience, however, public choice theory concerns rarely threaten Parliament's ability to legislate fairly.

I use these findings to serve two further aims. First, I conduct a comparative analysis of the American and Canadian experiences. In so doing, I identify several considerations relevant to the adversarial and legislative processes which impact judicial and legislative capacity to craft digital privacy rules. These factors include differences in each countries' method(s) for interpreting its constitution; the structure of the right to be protected from state searches and seizures; the available remedies for breaches of constitutional rights; the judicial system's willingness to depart from earlier precedents; the role of interveners in the adversarial system; and the particular legislative model used for passing digital privacy laws. Paying heed to these considerations will allow other

jurisdictions to learn from the Canadian and American experiences when refining their approaches to governing state intrusions onto digital privacy.

Second, I develop a variety of institutional strategies for governing digital privacy in the Canadian criminal procedure context. In so doing, I prescribe not only how courts and Parliament should respond to the challenges of governing digital privacy, I also consider whether an administrative governance framework might better achieve the aims of rendering more efficient, coherent, and even-handed rules. Utilizing administrative rulemaking can ensure rules are made more efficiently and with well-informed factual backgrounds. Yet, providing unelected, non-judicial decision-makers with significant deference when applying constitutional doctrine requires a more critical assessment than undertaken by its supporters. Majoritarian and public choice theory concerns, I maintain, serve as a strong, though not definitive, impediments to an administrative approach to crafting criminal procedure rules.

In light of these concerns, I contend that a multi-institutional approach ought to be adopted in Canada. Parliament should decide rules that will remain relatively stable. Agencies should create rules with unstable and complex factual backgrounds, such as searches and seizures of complex digital technologies. Courts, however, should not show deference to either actor. This refusal is justified for two reasons. First, judicial review is necessary to counter strong majoritarian concerns inherent to the criminal law. Second, my proposed external aid to assist courts in fact finding ensures judges will be equipped to conduct judicial review. Although this division of labour inserts some rule uncertainty into the field of criminal procedure, the trade-off best ensures that digital privacy rules are made in an efficient and coherent manner, as agencies are most likely to meet these ends. It also allows courts to do what they do best: ensure the rules balance the privacy and security interests at the heart of criminal procedure.

Preface

The following articles from my dissertation have been published. The final substantive Chapter of my thesis will be under peer review shortly. Each article appears at the places described below in the body of my dissertation:

(1) "Digital Evidence and the Adversarial System: A Recipe for Disaster?" (2018) 16 Canadian Journal of Law and Technology 437.
   - Chapters 1, 2, 6.

(2) "The Constitutionality of Using Production Orders to Obtain Stored Communications Content" (2018) 23 Canadian Criminal Law Review 171.
   - Chapter 2.

(3) "A Proposal for Police Acquisition of ISP Subscriber Information on Administrative Demand in Child Pornography Investigations" (2019) 24 Canadian Criminal Law Review 235.
   - Chapter 2.

(4) "Criminal Law and Digital Technologies: An Institutional Approach to Rule Creation in a Rapidly Advancing and Complex Setting" (2019) 65 McGill Law Journal 67.
   - Chapters 3, 6.

(5) "Criminal Law and Digital Technologies: Drawing Lessons from the Canadian and American Experiences" (2020) 53 University of British Columbia Law Review (forthcoming).
   - Chapters 4, 5

Acknowledgements

I would like to first and foremost express my deepest gratitude to my wife, Marian Thorpe, for her constant support during my graduate studies. I am also deeply indebted to my supervisor, Steven Penney, for his superb supervision and patience with me as I worked through my dissertation. I owe a similar debt of gratitude to my committee members, James Stribopoulos and Eric Adams, for providing insightful comments on my dissertation and for their general support of my academic pursuits. I would also like to extend a sincere thanks to several other scholars at the University of Alberta who worked with me on my thesis and other academic projects, namely, Matthew Lewans, Moin Yahya, and Patricia Paradis. Finally, I gratefully acknowledge the very generous financial support of the Government of Canada, Government of Alberta, as well as the College of Law and Faculty of Graduate Studies and Research at the University of Alberta.

Table of Contents

Chapter 8: Conclusion

Chapter One

Criminal Law & Digital Technologies

Introduction

Herbert Packer famously identified two competing models of criminal process.[1] The "Crime Control" model is primarily concerned with repressing criminal conduct. As a result, an emphasis is placed on efficient investigation, trial, and sentencing of those suspected of committing crime.[2] This emphasis on efficiency leaves little space for procedural rights, as they serve to slow down the criminal justice system.[3] The "Due Process" model is skeptical about the prospect of state actors pursuing investigations in an objective manner.[4] As a result, this model places a premium on judicial procedures aimed at ensuring that the criminal law is enforced fairly.[5] For Packer, the criminal process is best understood as a series of choices between the values underlying each of these models of criminal process.[6]

[1] See Herbert Packer, "Two Models of the Criminal Process" (1964) 113 University of Pennsylvania Law Review 1 at 6. See also Herbert Packer, *The Limits of the Criminal Sanction* (Stanford: Stanford University Press, 1968).
[2] *Ibid* at 9-11.
[3] *Ibid* at 13.
[4] *Ibid* at 14.
[5] *Ibid* at 16.
[6] *Ibid* at 5.

Packer further attached each of his criminal process models to a particular institution.[7] He reasoned that legislatures embraced the Crime Control model given the political necessity of protecting its citizens from crime.[8] Packer associated the judiciary with the Due Process model. As judges are tasked with upholding constitutional rights, they provide independent protection against excessive threats to liberty posed by the state.[9] In Packer's view, then, legislatures and courts can be expected to play vastly different, antagonistic roles within the criminal process.[10]

Packer proposed these institutional assumptions when empirical study of the criminal justice system was in its infancy.[11] As such, Packer cannot be faulted for failing to foresee the effect of the now vast empirical literature on the institutional assumptions underlying his criminal process models. Nevertheless, scholars have challenged the supposition that courts are best able to uphold rights while legislatures primarily care about prosecuting crime.[12] Although this debate has traditionally occurred in the field of criminal procedure more generally, its focus has recently shifted to the realm of digital technologies.[13]

---

[7] *Ibid* at 22-23.
[8] *Ibid*.
[9] *Ibid*.
[10] *Ibid*.
[11] See James Stribopoulos, "Packer's Blind Spot: Low Visibility Encounters and the Limits of Due Process versus Crime Control" in François Tanguay-Renaud & James Stribopoulos, eds, *Rethinking Criminal Law Theory: New Canadian Perspectives in the Philosophy of Domestic, Transnational and International Criminal Law* (Oxford: Hart Publishing, 2012) 193 at 196.
[12] Perhaps most importantly, American and Canadian courts have used their Bills of Rights to fill various gaps in police powers exposed by constitutional litigation. In Canada, see James Stribopoulos, "In Search of Dialogue: The Supreme Court, Police Powers, and the Charter" (2005) 31 Queen's Law Journal 1. In the United States, see Tracey Maclin, "What Can Fourth Amendment Doctrine Learn from Vagueness Doctrine" (2001) 3 University of Pennsylvania Journal of Constitutional Law 398 at 422-23.
[13] The key works include Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution" (2004) 102 Michigan Law Review 801; Daniel Solove, "Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference" (2005) 74 Fordham Law Review 747; Orin Kerr, "Congress, the Courts, and New Technologies: A Response to Professor Solove" (2005) 74 Fordham Law Review 779; Erin Murphy, "The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions" (2013) 111 Michigan Law Review 485**;** David Sklansky, "Two More Ways Not to Think about Privacy and the Fourth Amendment" (2015) 82 The University of Chicago Law Review 223.

I. Criminal Law and Digital Technologies

In questioning the ability of courts to govern digital technologies, scholars observe that the lag time between the introduction of new technologies and their eventual consideration by trial and appellate courts often renders judicial decisions of "historical interest only."[14] It may take many years before a technology used by suspects or police is legally challenged in a criminal trial.[15] If one of the parties appeals, there will be a further wait for an intermediate appellate court to decide the case.[16] And if a case is one of the very few to be heard by the apex court, its decision will come many years after the search took place.[17]

Scholars also argue that the adversarial nature of litigation tends to provide courts with only a "small snapshot of the technological whole."[18] In reaching their decisions, courts rely almost exclusively on the parties' submissions, which are limited by time and resource constraints and are framed to serve their own interests, not the broader public interest.[19] As a result, judges "run an unusually high risk of crafting rules based on incorrect assumptions of context and technological practice."[20] As one author observes, "if someone set out to design a process that

---

[14] See Daniel Scanlan, "Issues in Digital Evidence and Privacy: Enhanced Expectations of Privacy and Appellate Lag Times" (2012) 16 Canadian Criminal Law Review 301 at 312 and Kerr, "Fourth Amendment", *supra* note 13 at 868-69.
[15] See Kerr, "Fourth Amendment", *supra* note 13 at 868.
[16] *Ibid*.
[17] *Ibid* at 868-70.
[18] *Ibid*. See also Scanlan, "Issues", *supra* note 14 at 302; Steven Penney, "The Digitization of Section 8 of the *Charter*: Reform or Revolution?" (2014) 67 Supreme Court Law Review 505 at 530; Graham Mayeda, "My Neighbour's Kid Just Bought a Drone…New Paradigms for Privacy Law in Canada" (2015) 35 National Journal of Constitutional Law 59 at 79-81; Jordan Fine, "Leaving Dumb Phones Behind: A Commentary on the Warrantless Searches of Smart Phone Data Granted in *R v Fearon*" (2015) 13 Canadian Journal of Law and Technology 171 at 177-81.
[19] See Kerr, "Fourth Amendment", *supra* note 13 at 875.
[20] *Ibid* at 876 citing Cass Sunstein, "Foreword: Leaving Things Undecided" (1996) 110 Harvard Law Review 6 at 18. The issue of cell phone searches is a prime example in the Canadian context. See generally Tim Quigley, "*R. v. Fearon*: A Problematic Decision" (2015) 15 CR (7th) 281; Colton Fehr, "Cell Phone Searches Incident to Lawful Arrest: A Case Comment on the Ontario Court of Appeal's Decision in *R v Fearon*" (2014) 60 Criminal Law Quarterly 343; Colton Fehr and Jared Biden, "Divorced from (Technological) Reality: A Response to the Supreme Court of Canada's Reasons in *R v Fearon*" (2016) 20 Canadian Criminal Law Review 93; Fine, "Dumb Phones", *supra* note 18.

would yield illogical and inconsistent results [for digital technologies], they may well have come up with [the adversarial system]."[21]

Judges facing such problems are often aware of their limitations and, as a result, tend to craft broad rules to give future courts flexibility in assessing novel circumstances.[22] The result, however, is that judicial rules governing novel technological devices are often highly indeterminate. Law enforcement officers tasked with implementing such rules will favour *ex post* judicial determination of the legality of their conduct. This is because officers are expected to react quickly with little time to ponder the law, let alone what direction it might be headed. Erring on the side of caution by ensuring evidence is obtained is reasonable in these circumstances. It does, however, increase the likelihood that evidence implicating digital technologies will be challenged at trial. This in turn leads to increased instances where courts are prone to render untimely and ill-informed judgments.[23]

Some scholars therefore argue that legislatures are institutionally better equipped to govern digital privacy. Two main reasons are offered in support of this argument. First, legislatures are able to move more quickly to address evolving technologies, even in some cases legislating before such technologies are in mainstream use.[24] Second, legislatures have greater informational capacity as they commonly hear from a diverse range of groups before passing legislation.[25] Even if the legislative process does not initially strike an appropriate balance, democratic discourse will

[21] See Scanlan, "Issues", *supra* note 14 at 302.
[22] *Supra* note 20.
[23] See Kerr, "Fourth Amendment", *supra* note 13 at 869-70.
[24] See *Riley v California*, 134 S Ct 2473 (2014) (opinion of Justice Alito) at 6; Kerr, "Fourth Amendment", *supra* note 13 at 870-71; *Re Askin* 47 F3d 100 (1995) [*Askin*] at 105-06.
[25] See Kerr, "Fourth Amendment", *supra* note 13 at 875; Penney, "Digitization", *supra* note 18 at 531; Steven Penney, "Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach" (2007) 97 Journal of Criminal Law and Criminology 477 at 501; Marc Blitz, "Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Trades Image and Identity" (2004) 82 Texas Law Review 1349 at 1421; Stephen Breyer, "Our Democratic Constitution" (2002) 77 New York University Law Review 245 at 261-64.

tend to result in legislatures abandoning rules that provide insufficient privacy or security protections.[26]

Other American scholars nevertheless maintain that courts are better suited to govern digital privacy.[27] They assert that courts are more independent and therefore less susceptible to special interest influence and majoritarian dislike of criminal suspects, who are disproportionately members of disadvantaged minorities.[28] As these authors observe, studies in the United States have found that law enforcement agencies and corporations play an outsized role in shaping privacy policy given their "clear and constant voice in the political process."[29]

These scholars also show that legislatures are often unable or unwilling to update "obviously flawed and outdated provisions."[30] Legislative responses to privacy issues are instead "largely reactive, targeting industries on a case by case basis, and often responding only after extreme instances of privacy infringement."[31] Still other American studies contend that the degree of privacy protection from federal statutes is much more likely to turn on whether the information

---

[26] See Kerr, "Fourth Amendment", *supra* note 13 at 881.

[27] See Solove, "Fourth Amendment", *supra* note 13 at 761; Sklansky, "Two More Ways", *supra* note 13 at 224; Blitz, "Video Surveillance", *supra* note 25 at 1363; Daniel Solove, *Nothing to Hide: The False Trade-off between Privacy and Security* (New Haven: Yale University Press, 2011) at Chapter 17; Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books, 2006) at 222-23; Christopher Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* (Chicago: University of Chicago Press, 2007) at 201; William Fenrich, "Common Law Protection of Individuals' Rights in Personal Information" (1996) 65 Fordham Law Review 951 at 958.

[28] See Lessig, *Code*, *supra* note 27 at 216-22; Sklansky, "Two More Ways", *supra* note 13 at 227; Murphy, "Politics of Privacy", *supra* note 13 at 535-36; Penney, "Reasonable Expectations", *supra* note 25 at 505-06. See also Kent Roach, *Due Process and Victims' Rights: The New Law and Politics of Criminal Justice* (Toronto: University of Toronto Press, 1999). Some commentators note, however, that even if courts are better-equipped to regulate privacy, they may be reluctant to do so out of deference to legislatures and fear of being delegitimized by accusations of judicial activism. See Lessig, *Code*, *supra* note 27 at 167.

[29] See Murphy, "Politics of Privacy", *supra* note 13 at 533-35; Donald Dripps, "Constitutional Theory for Criminal Procedure: *Dickerson*, *Miranda*, and the Continuing Quest for Broad-but-Shallow" (2001) 43 William and Mary Law Review 1 at 4, 46; Solove, "Fourth Amendment", *supra* note 13 at 763-67; Solove, *Nothing to Hide*, *supra* note 27 at 165-67; Sklansky, "Two More Ways", *supra* note 13 at 227; Fenrich, "Common Law", *supra* note 27 at 958, 966. It is notable that Kerr, "Fourth Amendment", *supra* note 13 at 859 suggests in the criminal law context legislatures are not lobbied. His reasons for this assertion are sparse.

[30] *Ibid*.

[31] See Fenrich, "Common Law", *supra* note 27 at 966. See also Murphy, "Politics of Privacy", *supra* note 13 at 498, 500-01; Solove, "Fourth Amendment", *supra* note 13 at 771.

sought is useful to investigations than on widely shared notions of the degree of privacy objectively expected in the item searched.[32]

Scholars have also observed that case-by-case adjudication allows litigants to force rule-making in the absence of legislative action.[33] Numerous instances have been identified where legislatures were both slow and ineffective in enacting privacy laws.[34] Even though courts often generate broad and indeterminate rules, judicial rule-making at least guarantees the incremental, evolutionary development of policy in response to changing technological and social circumstances.[35]

The difficulties inherent in both the judicial and legislative processes have prompted other scholars to relegate both institutions in favour of an administrative approach to crafting criminal procedure rules. Although early attempts to develop such a framework were not implemented,[36] several American scholars have recently rejuvenated the idea.[37] As these scholars observe, agencies need not wait for a case to come before them to make a rule; nor need they be bogged down by daunting and slow legislative processes.[38] Rules may simply be developed by experts in the field—usually after ensuring public input on the content of the rules—thereby avoiding many of the challenges associated with governing new and complex search technologies.[39]

---

[32] See Murphy, "Politics of Privacy", *supra* note 13 at 506 citing Slobogin, *Privacy at Risk*, *supra* note 27 at 184.
[33] See Sklansky, "Two More Ways", *supra* note 13 at 227; Murphy, "Politics of Privacy", *supra* note 13 at 535.
[34] *Ibid*.
[35] *Ibid*.
[36] See Kenneth Culp Davis, "An Approach to Legal Control of the Police" (1974) 52 Texas Law Review 703; Anthony Amsterdam, "Perspectives on the Fourth Amendment" (1974) 58 Minnesota Law Review 349; Carl McGowan, "Rule-Making and the Police" (1972) 70 Michigan Law Review 659.
[37] See Barry Friedman and Maria Ponomarenko, "Democratic Policing" (2015) 90 New York University Law Review 1827; Christopher Slobogin, "Policing as Administration" (2016) 165 University of Pennsylvania Law Review 91; Daphna Renan, "The Fourth Amendment as Administrative Governance" (2016) 68 Stanford Law Review 1039.
[38] *Ibid*.
[39] *Ibid*.

Although administrative agency rule-making presents an intriguing institutional option, there are reasons to approach this proposal with caution. The logic of administrative law demands that courts show significant deference to administrative rules, even those implicating fundamental rights.[40] Yet, as with legislatures, agencies may be subject to majoritarian and lobbyist influence which courts are uniquely able to avoid. Equally important, deferring to administrative agencies may hinder the ability of courts and legislatures to work with administrative agencies to improve traditional governance approaches to implementing constitutional rights.[41]

All of these institutional options for governing digital privacy have been inadequately explored in the Canadian context. This is unsurprising as the literature has not thoroughly considered whether, and if so why, courts tend to receive inadequate evidence when crafting digital privacy rules.[42] Given that both countries use the adversarial system of justice, it is tempting to assume that the Canadian judiciary would face similar struggles as its American counterpart. As I discuss below, however, differences between each countries' adversarial models give rise to different types and degrees of challenges. This in turn can affect the relative capacity of each countries' judiciary to respond to the challenges of governing digital privacy.

Similarly, there is only limited scholarship engaging with Canada's legislative ability to govern digital privacy.[43] The existing literature relies on the first few Parliamentary responses to

---

[40] See generally *Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65; *Doré v Barreau du Québec*, 2012 SCC 12, [2012] 1 SCR 395. It is notable, however, that legislatures may displace the reasonableness standard with legislation.

[41] These criticisms are inspired by Andrew Crespo's article "Systemic Facts: Toward Institutional Awareness in Criminal Courts" (2016) 129 Harvard Law Review 2049.

[42] See Scanlan, "Issues", *supra* note 14; Penney, "Reasonable Expectations", *supra* note 25; Susan Magotiaux, "Out of Sync: Section 8 and Technological Advancements in Supreme Court Jurisprudence" (2015) 71 Supreme Court Law Review 501; Fine, "Dumb Phones", *supra* note 18; Fehr & Biden, "Divorced", *supra* note 20; Fehr, "Cell Phone", *supra* note 20.

[43] There are only a handful of Canadian authors writing on this point. Professor Steven Penney has been most active among Canadian scholars. Although his article "Reasonable Expectations", *supra* note 25 at 503-05 provides insights into my thesis question, the analysis is necessarily brief given the broader purpose of his article: applying economic theory to the reasonable expectation of privacy doctrine. Likewise, another Canadian author, Daniel Scanlan, references the debate which has developed in the American context, but provides little evidence to support the claim

novel and complex search technologies in concluding that Parliament is generally capable of providing efficient, coherent, and even-handed responses to digital privacy concerns.[44] As more difficult challenges have arisen since these initial legislative responses, more sustained study of Parliamentary capacity to respond to the unique challenges of governing digital privacy is necessary.

Finally, Canadian scholars have not considered whether an administrative approach to criminal procedure rules writ large (never mind those rules implicating digital technologies) would provide a superior governing framework. Although there is an intuitive appeal to utilizing administrative agencies in rule-making, the current American scholarship inadequately considers the potential pitfalls of utilizing unelected, non-judicial decision-makers to craft criminal procedure rules. Perhaps more importantly, the existing scholarship gives short shrift to the potential for legislatures and courts to work with administrative agencies to better address problems typically faced when crafting rules related to digital technologies.

II. Research Questions

The above review gives rise to several research questions. Can case-by-case rulemaking keep pace with technological change in the digital era? Does the adversarial process provide judges with sufficient and accurate information to allow them to effectively regulate modern surveillance technologies? Is Parliament passing laws that fail to consider technological implications or inadequately consider privacy interests, especially those of politically unpopular groups such as criminal suspects? How promptly is Parliament reacting to advances in technology? Do special

---

that these difficulties arise to the same degree in the Canadian context of for the same reasons they arise in the American context. See Scanlan, "Issues", *supra* note 14 at 311-12. Finally, although Michal Fairburn's work provides a valuable contribution to the field, she also only discusses Parliament's first response to the challenges of governing digital privacy. See Michal Fairburn, "Twenty-Five Years in Search of a Reasonable Approach" (2008) 40 Supreme Court Law Review 55.

[44] *Ibid*.

interest groups have excessive influence on the legislative process? Might agency rule-making facilitate more prompt, coherent, and even-handed rule-making? Finally, how might the answers to these questions affect institutional strategies for governing state intrusions onto digital privacy?

Answering these questions will serve three central purposes. First, it will allow me to develop a robust empirical record of the relative institutional capacities of Canadian courts and legislatures to govern digital privacy. By so doing, I will open the door to conducting a comparative analysis between the Canadian and American experiences. I use this comparison to address the second and broader aim of my dissertation: developing a suitable normative framework for determining the kinds of digital privacy regulation which each institution in any given polity is best suited. With a fuller understanding of the costs and benefits of relying on legislatures and courts to govern digital privacy, I will be able to address my final research question: whether administrative rule-making provides a superior institutional approach to crafting criminal procedure rules implicating digital technologies.

III. Dissertation Structure

My dissertation is divided into eight chapters. Chapter Two considers whether Canadian courts have been able to render digital privacy rules in a timely and well-informed manner. I conclude that they have had similar difficulties as their American judicial counterparts. In so concluding, however, I develop a more robust understanding of why Canadian courts have faced difficulties receiving adequate evidence about digital technologies. In my view, commentators have inadequately explored three factors: the high costs of providing courts with evidence implicating digital technologies, the (in)ability of judges to understand digital technologies, and the inability of traditional adjustments to the adversarial process (such as calling expert evidence

or relying upon intervener factums) to reliably fill evidentiary gaps. I examine each of these factors by reviewing the jurisprudence related to several controversial digital privacy issues.

Chapter Three addresses the question of Parliament's institutional capacity to respond to the challenges of governing digital privacy. The limited scholarship provides an optimistic outlook. This scholarship is not, however, comprehensive in its assessment. My review of Parliament's legislation governing digital privacy is both comprehensive and, unfortunately, much more pessimistic. Although I find that Parliament has not succumbed to lobbyist influence when crafting digital privacy rules in the criminal procedure context, I conclude that its legislative responses have often been woefully inefficient and incoherent.

Chapter Four turns to the American literature. The authors writing on this topic have diverged significantly on American judicial and legislative capacity to make expedient, coherent, and even-handed digital privacy laws.[45] Orin Kerr contends that Congress has proven far more competent than its judicial counterparts at responding to the challenges raised by digital technologies. As such, he asserts that courts should be highly deferential to legislative rules governing digital privacy.[46] Daniel Solove takes precisely the opposite view.[47] Erin Murphy and David Sklansky have since provided an intermediary and more cautious view of the empirical evidence.[48] The aim of this Chapter is to parse these disagreements and draw my own conclusions with respect to the relative institutional capacities of Congress and the American courts to respond to digital technologies.

Chapter Five uses this clearer understanding of the challenges arising in the American literature to facilitate a comparison of the American and Canadian experiences. Although Canada

[45] See generally the authors cited *supra* note 13.
[46] See Kerr, "Fourth Amendment", *supra* note 13.
[47] See Solove, "Fourth Amendment", *supra* note 13.
[48] See Murphy, "Politics of Privacy", *supra* note 13; Sklansky, "Two More Ways", *supra* note 13.

and the United States are similarly governed countries,[49] their different histories and cultures have affected how actors within these institutions operate. Studies suggest that American legislatures are more susceptible to the negative influences of lobbying.[50] This is in no small part due to differing campaign financing practices in each country. The greater need to receive large donations to finance future campaigns makes American legislatures more beholden to lobbyists' interests.[51] The legislative process in the United States also presents unique impediments to passing legislation.[52] Although Parliament is also often unable to pass coherent and timely digital privacy laws, I find that its parliamentary system of governance is better suited to ward off lobbyist influence.

In contrast to the Canadian judiciary, the American judiciary has proven better able to litigate complex digital facts. Although both courts lag behind technological change, I find that superior judicial resources and a greater willingness to allow interveners to affect the adversarial process has led to a more coherent understanding of digital technologies in American appellate courts. Whether judges in each system are able to pass even-handed, unpartisan rulings with respect to digital privacy rules is a question which cannot be answered with confidence. Even if judges are politically biased, I conclude that it is questionable whether digital privacy laws, even in the criminal law context, are impacted by these biases.

---

[49] Both are democratic, common law countries, with strong powers of judicial review vested in their judiciaries.

[50] See Barrie McKenna, "Corrupt Canada? We're Small Time Compared to the US" *Globe and Mail* (10 October 2010). It is also notable that American lobbyists may direct their efforts towards both Congress and the Senate as each can block laws. This makes lobbying economically more feasible. See Jerry Mashaw, "Public Law and Public Choice: Critique and Rapprochement" in Daniel Farber and Anne O'Connell (eds), *Research Handbook on Public Choice and Public Law* (Cheltenham: Edward Elgar Publishing Ltd, 2010) at 30.

[51] See e.g. Raj Chari, Gary Murphy, and John Hogan, "Regulating Lobbyists: A Comparative Analysis of the United States, Canada, Germany and the European Union" (2007) 78 The Political Quarterly 422.

[52] Legislation requires the approval of the House of Representatives, Senate, and President (subject to a two-thirds majority veto override by both houses). It is relatively rare for these institutions to be held by the same political party, and even within the House or Senate themselves it may be difficult to marshal a majority of legislators to support contentious initiatives.

My comparison exposes several factors which affect a court or legislature's ability to respond to digital privacy concerns in an efficient, coherent, and even-handed manner. These factors include differences in each countries' method(s) for interpreting its constitution; the structure of the right to be protected from state searches and seizures; the available remedies for breaches of invasions of privacy; the judicial system's willingness to depart from earlier precedents; the role of interveners in the adversarial system; and the particular legislative model used for passing digital privacy laws. Paying heed to these considerations will allow interested jurisdictions to learn from the Canadian and American experiences when refining their institutional approaches to governing state intrusions onto digital privacy.

Chapter Six applies the normative framework developed in Chapter Five to the Canadian experience. In so doing, I conduct a cross-institutional analysis to determine under what circumstances Parliament and courts are better able to govern digital privacy.[53] The approach that I propose requires both institutions to recognize that each will be better situated to govern under different institutional conditions. As these conditions change abruptly and unpredictably, I call for the adoption of rule-making strategies that not only mitigate the limitations of courts and Parliament to respond to the challenges of governing digital technologies, but also encourages each institution to defer to the other where its limitations provide a significant barrier to principled policy development.

Chapter Seven considers whether an administrative approach to crafting digital privacy rules might prove more feasible than relying on courts and Parliament. There is much to be gained from employing the administrative state in the criminal procedure context, as administrative

[53] See Neil Komesar, *Imperfect Alternatives: Choosing Institutions in Law, Economics, and Public Policy* (Chicago: University of Chicago Press, 1994) at 142; Adrian Vermeule, *Judging Under Uncertainty: An Institutional Theory of Legal Interpretation* (Harvard: Harvard University Press, 2006).

governance is readily capable of developing digital expertise and providing significantly more efficient rules. Yet, providing unelected, non-judicial decision-makers with significant deference when applying constitutional doctrine requires a more critical assessment than undertaken by its supporters. Majoritarian and public choice theory concerns, I maintain, serve as strong, though not definitive, impediments to an administrative approach to crafting criminal procedure rules.

Given the costs and benefits of administrative governance, I contend that a multi-institutional approach ought to be adopted in Canada. Parliament should decide rules that can be expected to remain relatively stable. Agencies should create rules with respect to unstable and complex factual backgrounds, such as searches and seizures of digital technologies. Courts, however, should refuse to show deference to either of these actors. This refusal is justified for two reasons. First, judicial review is necessary to counter the strong majoritarian concerns inherent in the criminal law. Second, my proposed external aid to assist courts in fact finding ensures judges will be equipped to conduct judicial review. Although this division of labour inserts some rule-making uncertainty into the field of criminal procedure, the trade-off best ensures that digital privacy rules are made in an efficient and coherent manner, as agencies are more likely to meet these ends. It also allows courts to do what they do best: ensure the rules balance the privacy and security interests at the heart of criminal procedure.

Chapter Eight concludes by summarizing the lessons drawn from the preceding chapters and highlights further avenues of research. I begin by emphasizing the importance of improving the way democratic institutions govern privacy. As Justice Karakatsanis observed in *R v Fearon*,[54] "[when] technology changes, our law must also evolve so that modern mobile devices do not become the telescreens of George Orwell's *1984*."[55] In other words, effective governance of

[54] 2014 SCC 77, [2014] 3 SCR 621.
[55] *Ibid* at para 102.

privacy is necessary to preserve fundamental rights and freedoms. At the same time, collection and dissemination of private information is often necessary to ensure state security and economic prosperity. Regardless of one's opinion of how this balance is best struck, it is necessary that the institutions governing digital privacy work to their strengths, not their weaknesses.

IV. Scope of Research

Before embarking on this study, it is prudent to explain what is *not* the subject of inquiry. First, I limit the Canadian aspect of my study to federal criminal laws. I do so for two reasons. First, the American literature has tended to focus on digital privacy concerns arising in the criminal procedure context. Focusing on the same area will facilitate cleaner comparison. Second, to include provincial legislation would make the study overly broad. As will become evident, Parliament's post-*Charter* criminal procedure legislation and its judicial consideration includes sufficient case studies to shed general light on the institutional capacity of Canadian courts and legislatures to govern digital privacy, at least in the criminal procedure context.

Second, my study excludes national security legislation. The reason for excluding this area is less concerned with the breadth of the topic, and more with the ability to gather sufficient information for study. To investigate the speed, coherence, and public choice theory questions central to my dissertation requires broad access to not only how Parliament develops such laws, but also how those laws are interpreted and acted upon. Such information generally is not sufficiently available in the national security context. As one author aptly puts it, "[a]bsent whistle-blowers, it is almost impossible to develop enough understanding of the intelligence agencies and their practices to identify what should even be negatively framed in the first place."[56] With these

[56] Christopher Parsons, "Stuck on the Agenda: Drawing Lessons from the Stagnation of 'Lawful Access' Legislation in Canada" in Michael Geist, ed, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (Ottawa: University of Ottawa Press, 2015) 257 at 273.

two limitations in place, I turn to an exploration of the judicial capacity of Canadian courts to govern digital privacy.

Chapter Two

Judicial Capacity to Govern Digital Privacy

Introduction

Judicial decisions concerning the legality of digital device searches have exposed two main weaknesses with the adversarial system of judicial decision making. First, the rapid evolution of digital technologies tends to result in judges rendering outdated decisions.[1] Second, the "unusually complex" nature of digital technologies results in courts receiving inadequate evidence upon which to develop digital privacy rules.[2] The literature has not, however, investigated in sufficient depth why these difficulties arise when courts make digital privacy rules.[3] This Chapter aims to fill this

[1] See Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution" (2004) 102 Michigan Law Review 801 at 858-59, 868-69; Daniel Scanlan, "Issues in Digital Evidence and Privacy: Enhanced Expectations of Privacy and Appellate Lag Times" (2012) 16 Canadian Criminal Law Review 301 at 312.
[2] See Kerr, "Fourth Amendment", *supra* note 1 at 875-77; Scanlan, "Issues", *supra* note 1 at 302; Steven Penney, "The Digitization of Section 8 of the *Charter*: Reform or Revolution?" (2014) 67 Supreme Court Law Review 505 at 530; Stephen Breyer, "Our Democratic Constitution" (2002) 77 New York University Law Review 245 at 261-63; Graham Mayeda, "My Neighbour's Kid Just Bought a Drone…New Paradigms for Privacy Law in Canada" (2015) 35 National Journal of Constitutional Law 59 at 79-81; Jordan Fine, "Leaving Dumb Phones Behind: A Commentary on the Warrantless Searches of Smart Phone Data Granted in *R v Fearon*" (2015) 13 Canadian Journal of Law and Technology 171 at 177-81.
[3] See Scanlan, "Issues", *supra* note 1; Steven Penney, "Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach" (2007) 97 Journal of Criminal Law and Criminology 477; Susan Magotiaux, "Out of Sync: Section 8 and Technological Advancements in Supreme Court Jurisprudence" (2015) 71 Supreme Court Law Review 501.

void by scrutinizing the process underlying how Canadian courts have developed rules with respect to several complex digital technologies.

My study exposes three main factors that hinder courts from effectively governing digital privacy.[4] First, the evidence submitted in the adversarial process is often limited by resource constraints. As judicial rules governing digital privacy typically emerge from allegations that the state breached section 8 of the *Charter*, it is criminal defendants who must prove that a constitutionally relevant search occurred and/or was highly invasive.[5] As I contend, however, it is practically impossible to expect criminal accused to adequately fill the evidential record with their limited resources. Second, there is some evidence to suggest that the inability of judges to understand digital technologies prevents courts from creating optimal rules.[6] Finally, traditional adjustments to the adversarial process, such as intervener briefs or expert testimony, are generally incapable of addressing the judicial information deficit.[7] To have expert testimony every time a digital legal issue arises is impractical given the high costs of hiring experts. Similarly, relying on interveners (usually civil rights groups) erroneously assumes that they will have adequate resources or be given a fair opportunity to fill the evidentiary lacuna.[8]

The Chapter proceeds as follows. I begin in Part I by overviewing my methodology for exploring the institutional capacity of courts to govern digital privacy. In Part II, I then provide a detailed review of several prominent issues which have arisen in the digital jurisprudence. In so

[4] As discussed in Chapter 1, these considerations are common problems more generally with courts crafting criminal procedure rules.
[5] For a "search" to occur under section 8 of the *Charter*, the accused person must have a reasonable expectation of privacy in the thing searched. See generally *Hunter et al. v Southam Inc*., [1984] 2 SCR 145, 33 Alta LR (2d) 193 [*Hunter*].
[6] See David Paciocco, "Proof and Progress: Coping with the Law of Evidence in a Technological Age" (2013) 11:2 Canadian Journal of Law and Technology 181 at 181.
[7] Daniel Solove asserts that these adjustments will correct the factual record. See Daniel Solove, "Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference" (2005) 74 Fordham Law Review 747 at 771-72.
[8] As discussed below, these considerations are evident in some of the Court's recent digital jurisprudence.

doing, I highlight a variety of mistakes and oversights which have occurred during litigation of these digital privacy issues. I conclude in Part III by assessing the extent to which the judicial treatment of digital technologies is affected by resource restrictions, judicial capacity to understand digital technologies, and whether traditional adjustments to the adversarial process are able to fill evidentiary gaps.

I. Methodology

The issues I have selected to explore the underlying reasons why judges face difficulties understanding digital technologies were chosen in light of two main factors. First, each issue must have spent significant time in lower courts. Second, the issue must have resulted in at least one Supreme Court of Canada decision. This approach allows me to test the duration of time it takes for the adversarial process to resolve digital legal issues. It also ensures that the adversarial process has reached its full potential, as the litigation process before the Court is the most detailed and widely participated in by interested litigants. All Attorneys General, for instance, are allowed to make submissions.[9] Interveners also tend to put their most robust efforts into hearings at the Court as it represents the best opportunity to influence the development of the law.[10]

The legal issues reviewed—outlined in detail in Part II—will assess whether three main issues arose. First, I consider whether resource restrictions have affected the quality of evidence submitted by counsel at trial. To answer this question, I ask whether there is a correlation between cases where the evidence was clearly inadequate and factors indicative of indigency. For instance, whether the defendant's lawyer was a private lawyer or Legal Aid counsel is a good indicator as

[9] See *Supreme Court Act*, RSC 1985, c S-26, s 53(5).
[10] Although I am unaware of any empirical evidence to support this proposition, it is a reasonable assumption given that interveners are generally non-profit corporations with limited funding. One can expect that they will use their resources when it counts most. Their jurisdiction to be heard derives from the *Supreme Court Act*, *supra* note 9, s 53(6).

Legal Aid lawyers are only available to low-income people and are notoriously underfunded.[11] Further, whether resource restrictions impacted the evidence submitted may be inferred by assessing whether necessary expert witnesses were called in support of a defendant's case, as well as if the defendant was able to appeal a loss at trial.

Second, I will consider whether judicial mistakes or oversights may be attributed to judicial inability to understand digital technologies. Justice David Paciocco, himself a prominent judge and former academic, put the issue as follows:

> The root of our insecurity is that many of us do not understand information technology, yet it is necessary to understand information technology to apply the law of evidence in an intelligent manner. The reason many of us do not understand information technology is that it takes many years to become jurists and even longer to become judges. This, of course, is my polite and indirect way of admitting that most judges are old enough to think that information technology is new and mysterious.[12]

Without a basic understanding of computer technologies, it would come as no surprise that judges make mistakes. Others, however, maintain that courts do not have any inherent difficulty understanding digital technologies.[13] As the evidence supporting both views is thin,[14] a detailed review of the digital jurisprudence will aid in determining the extent of this problem.

Finally, it is necessary to ask whether traditional adjustments to the adversarial system have been able to supplement the evidentiary record or correct technological misunderstandings. Some scholars assume that calling expert evidence or intervener factums will serve this function.[15] To

---

[11] See Shawn Logan, "Defence Lawyers Say Legal Aid 'Neglected and Degraded' in Alberta" *Calgary Herald* (30 April 2018), online: <http://calgaryherald.com/news/local-news/defence-lawyers-says-legal-aid-suffering-from-funding-crisis-in-alberta>; Lauren Krugel, "Alberta Defence Lawyers Demand Boost to Legal Aid Funding" *The Globe and Mail* (17 April 2018), online: <https://www.theglobeandmail.com/canada/alberta/article-calgary-defence-lawyers-group-demands-boost-to-legal-aid-funding/>; Ian Burns, "B.C. Budget Boosts Legal Aid Funding but it's still 'Woefully Underfunded,' Women's Equality Group says" *The Lawyer's Daily* (26 February 2018), online: <https://www.thelawyersdaily.ca/articles/5971/b-c-budget-boosts-legal-aid-funding-but-it-s-still-woefullyunderfunded-women-s-equality-group-says>.

[12] See Paciocco, "Proof", *supra* note 6 at 181. See also Kerr, "Fourth Amendment", *supra* note 1 at 876-77; Cass Sunstein and Adrian Vermeule, "Interpretations and Institutions" (2003) 101 Michigan Law Review 885 at 943.

[13] See Solove, "Fourth Amendment", *supra* note 7 at 771-72.

[14] See generally Paciocco, "Proof", *supra* note 6; Solove, "Fourth Amendment", *supra* note 7.

[15] See Solove, "Fourth Amendment", *supra* note 7 at 771-72.

test whether this is true, I assess the rate at which experts are called by both defendants and Crown prosecutors in controversial digital privacy cases. As experts are rarely called, it is difficult to test the quality of information they provide. In contrast, I find that interveners make submissions in controversial digital privacy cases much more frequently. As such, I assess the extent to which intervener factums engage with evidentiary gaps and help to correct factual misunderstandings present in the evidence submitted at trial.

II. Digital Privacy Jurisprudence

The right to be free from unreasonable search and seizure protected by section 8 of the *Canadian Charter of Rights and Freedoms*[16] has recently undergone a "digitization".[17] As a result, the Supreme Court of Canada has rendered multiple decisions reconciling section 8 doctrine with digital technologies.[18] How courts have dealt with three of these issues—cell phone searches incident to arrest; expectations of privacy in internet service provider subscriber information; and the definition of "intercept" under Part VI of the *Criminal Code of Canada*[19]—will shed light on the institutional capacity of courts to govern digital technologies.[20]

(a) Cell Phone Searches Incident to Arrest

As the capacity and use of modern cell phones increase, police have taken greater interest in searching cell phones as part of the common law power to search incident to arrest.[21] As the

[16] Being schedule B to the Canada Act 1982 (UK), 1982, c11.
[17] See Penney, "Digitization", *supra* note 2.
[18] From this decade see *R v Morelli*, 2010 SCC 8, [2010] 1 SCR 253 (privacy interests implicated by computer searches); *R v Gomboc*, 2010 SCC 55, [2010] 3 SCR 211 (digital tracking of electricity consumption); *R v Cole*, 2012 SCC 53, [2012] 3 SCR 34 (whether accused had reasonable expectation of privacy in computer issued by employer); *R v Vu*, 2013 SCC 60, [2013] 3 SCR 657 (whether computer searches must be specifically authorized in a warrant); *R v Fearon,* 2014 SCC 77, [2014] 3 SCR 621 (searches of cell phones incident to arrest); *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212 (reasonable expectation of privacy in ISP subscriber information); *R v Marakah*, 2017 SCC 59, [2017] 2 SCR 608 (reasonable expectation of privacy in text messages); *R v Jones*, 2017 SCC 60, [2017] 2 SCR 696 (definition of "intercept" under Part VI of the *Criminal Code*).
[19] RSC 1985, c C-46.
[20] My findings from this review are summarized in Appendix A.
[21] For the requirements of a valid search incident to arrest, see *R v Caslake*, [1998] 1 SCR 51, 121 CCC (3d) 97.

Court had previously prohibited,[22] or modified,[23] the legal framework for conducting particularly invasive searches incident to arrest, several courts heard arguments that cell phone searches incident to arrest ought to be prohibited as unjustifiable violations of section 8 of the *Charter*. In *R v Fearon*,[24] the Court found that conducting such searches was necessary for three reasons. First, public safety required searching cell phones to ensure suspects were not messaging criminal backup.[25] Second, searching a cell phone will sometimes be necessary to preserve evidence due to the threat of remote deletion.[26] Third, searching phones may lead police to new evidence which would otherwise be lost.[27] Many technological arguments were advanced to both undermine and support these points.

(i) Passwords and Biometric Identification

Most cases deciding the scope of cell phone searches incident to arrest arose before the prevalence of sophisticated, internet-connected "smartphones".[28] As a cursory review of the jurisprudence reveals, many of the phones at issue were not password protected.[29] With the advancement of smartphone technology, however, users became more protective of the information in their phones.[30] This likely explains why large cell phone companies made password protection ubiquitous among mobile phones. Yet, as Daniel Scanlan posited prior to the Court's decision in *Fearon*, it is debatable whether there is any "mechanism at law to force an accused to

[22] See *R v Stillman*, [1997] 1 SCR 607, 144 DLR (4th) 193 where the Court concluded that bodily samples could not be taken incident to arrest. See also *R v Godoy*, 33 OR (3d) 445, 115 CCC (3d) 272 (ONCA) aff'd [1999] 1 SCR 311, 168 DLR (4th) 257 where it was concluded that houses could not be searched incident to arrest.
[23] See *R v Golden*, 2001 SCC 83, [2001] 3 SCR 679 where the Court required a higher threshold for conducting strip searches incident to arrest.
[24] *Supra* note 18.
[25] *Ibid* at para 48.
[26] *Ibid* at para 49.
[27] *Ibid* at para 46.
[28] "Dumb" phones are those which can only receive calls and text messages.
[29] *R v Giles*, 2007 BCSC 1147, 77 WCB (2d) 469 is the only pre-*Fearon* decision involving a locked phone.
[30] See Colton Fehr, "Cell Phone Searches Incident to Lawful Arrest: A Case Comment on the Ontario Court of Appeal's Decision in *R v Fearon*" (2014) 60 Criminal Law Quarterly 343 at 356.

disclose a password and, if any such measures were created, they would not likely survive constitutional scrutiny."[31]

Other academics have expanded upon this view subsequent to the Court's decision in *Fearon*.[32] Authors maintain that the Court failed to undertake a full constitutional analysis due to the lack of password protection and biometric identification evidence submitted in the case.[33] If an accused is required to provide a password, it is arguable that the accused's self-incrimination rights are unjustifiably violated.[34] Similarly, requiring an accused to speak into a phone may violate the right to silence.[35] Finally, conscripting fingerprints or retina scans constitutes a warrantless seizure which raises section 8 constitutionality issues which were not considered by any of the courts which ruled on the constitutionality of searching cell phones incident to arrest.[36] Although these considerations are less intrusive compared to the warrantless search of a cell phone, conscripting passwords or biometric information adds to the severity of the overall intrusion.[37]

If there is merit to the argument that police cannot demand password or biometric evidence, then the Crown's argument in *Fearon* is significantly undermined. The desire to preserve evidence from remote deletion, inquire as to whether criminal backup is being requested, or discover evidence which is temporally vulnerable is only possible if the police have "prompt" access to the

---

[31] Daniel Scanlan, *Digital Evidence in Criminal Law* (Aurora: Canada Law Book, 2011) at 214 citing *R v Beauchamp* (2008), 58 CR (6th) 177 at paras 18, 66, 171 CRR (2d) 358 (OSCJ). It is possible that police might be able to compel an accused to provide their password via a section 487.02 assistance order. Although such an order typically applies to require third parties to assist an investigation, it is an open question whether the section authorizes police to compel an accused to provide a password and, if so, whether any such order would survive constitutional scrutiny. For cases refusing to grant such an order, see *R v Talbot*, 2017 ONCJ 814, 140 OR (3d) 104 leave to the Supreme Court of Canada refused 2018 CarswellOnt 5328; *R v Shergill*, 2019 ONCJ 54, [2019] OJ No 544.

[32] See Colton Fehr and Jared Biden, "Divorced from (Technological) Reality: A Response to the Supreme Court of Canada's Reasons in *R v Fearon*" (2015) 20 Canadian Criminal Law Review 93.

[33] *Ibid* at 95. The phone in *Fearon* was not password protected and did not require biometric identification to enter the phone.

[34] *Ibid* at 103

[35] *Ibid*.

[36] *Ibid* at 104-05

[37] *Ibid*.

phone.[38] Yet, modern smartphones have frequently proven capable of thwarting such access. For instance, major cell phone providers such as Apple and Google utilize secure device encryption systems to ensure that information service providers cannot access a user's encryption key to unlock their password.[39] This in turn requires police to utilize inefficient and inefficacious traditional methods of investigation to discover user passwords,[40] seek help from reluctant technology companies who have a strong interest in maximizing data security,[41] or attempting to exploit a narrow number of vulnerabilities in encryption technologies.[42]

Despite the above barriers to entering cell phones "promptly", the state of the technology was hardly considered in the jurisprudence.[43] Although the Crown *may* be able to justify any invasion of privacy arising from demanding a password or biometric identifier, the fact that these issues were not considered illustrates the general problem with courts deciding cases that involve digital technology issues.[44] At best, the constitutionality of searching locked cell phones incident

[38] See *Fearon*, *supra* note 18 at paras 49, 59, and 66.
[39] See Steven Penney and Dylan Gibbs, "Law Enforcement Access to Encrypted Data: Legislative Responses and the *Charter*" (2017) 63 McGill Law Journal 201 at 211 citing Apple, "iOS Security: iOS 11", (January 2018) at 12, online: <https://www.apple.com/business/docs/iOS/Security_Guide.pdf>; Google, "Android 7.1 Compatibility Definition" (21 June 2017) at 79, online: <http://source.android.con/compatibility/7.1/android-7.1-cdd.pdf>; Orin Kerr, "Apple's Dangerous Game", *The Washington Post* (19 September 2014), < https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game/>.
[40] See Penney and Gibbs, "Encrypted Data", *supra* note 39 at 206-09 for an extensive review of such strategies and the relevant weaknesses involved.
[41] *Ibid* at 212-13.
[42] *Ibid* at 213-16. As the authors observe, technology companies have strong economic incentives to maintain a high level of data security.
[43] The Ontario Court of Appeal's decision in *R v Fearon*, 2013 ONCA 106 at para 75, 296 CCC (3d) 331 [*Fearon ONCA*] arguably makes this suggestion when it concluded that a warrant was required for locked phones, but not unlocked phones. It is unclear if the Court was considering whether the accused's expectation of privacy was higher as a result, or if the Court realized the difficulties officers would have in entering a phone.
[44] Admittedly, it is not certain that the right against self-incrimination is engaged. See Steven Penney, "'Mere Evidence'? Why Customs Searches of Digital Devices Violate Section 8 of the *Charter*" (2016) 49:2 University of British Columbia Law Review 485 at 517 (see footnote 152 and the sources cited therein); Penney and Gibbs, "Encrypted Data", *supra* note 40 at 228-44. However, this argument has yet to prove successful (see *Talbot*, *supra* note 31; *Shergill*, *supra* note 31), and the fact that the courts were not presented with such an argument is indicative of judicial ability to govern digital privacy.

to arrest—which constitute the majority of cell phones today[45]—remains ambiguous post-*Fearon*. At worst, the Court's decision became inapplicable to most non-consensual cell phone searches incident to arrest the moment it was rendered.

(ii) Battery Removal

With respect to the rationale regarding the preservation of evidence, several courts,[46] as well as academic commentators,[47] have asserted that any deletion of cell phone data could be prevented if an officer removed a battery from a cell phone. Cell phone content cannot be deleted when a phone is turned off.[48] As long as the officer reboots the phone within an area that is isolated from the phone's cellular network, any remote-control deletion attempts will be thwarted.[49] As such, it is arguable that any concern about remote control destruction of evidence on a phone—which was forcefully argued by the Crown—is without merit.

An issue that judges and commentators failed to address concerns the way in which computers store data. Computers store a significant amount of data permanently.[50] However, not all data is non-volatile. Volatile memory, most common of which is Random Access Memory (RAM), stores frequently used program information in a temporary manner.[51] The benefit of using RAM is that it significantly increases the speed of a device by freeing up space that otherwise would be used for permanent memory storage.[52] Removing the battery from a computer or phone,

---

[45] See Peter Svensson, "Smartphones now Outsell 'Dumb' Phones" *Newshub* (28 April 2013), online: <http://www.newshub.co.nz/technology/smartphones-now-outsell-dumb-phones-2013042912>.
[46] See the dissenting reasons in *Fearon*, *supra* note 18 at para 144; *R v Liew*, 2012 ONSC 1826 at para 144, [2012] OJ No 1365; and *R v Cater*, 2012 NSPC 2 at para 32, 312 NSR (2d) 242 [*Cater NSPC*].
[47] See Fehr, "Cell Phone", *supra* note 30 at 352-53.
[48] *Ibid*.
[49] *Ibid*. These reboots typically occur at an area of a police station designed for such purposes.
[50] See Scanlan, *Digital Evidence*, *supra* note 31 at 159-67.
[51] *Ibid*.
[52] *Ibid*.

however, risks losing memory stored on the RAM.[53] Although computer developers have subsequently made significant progress with respect to making RAM memory less volatile,[54] the technology was much less capable when lower courts began deciding whether cell phone searches incident to arrest were constitutional.[55] As such, removing the battery upon seizing a cell phone does not provide a perfect solution as it risks (depending on the nature of the volatile memory used) losing potentially incriminating evidence.

(iii) Faraday Bags

A number of courts and scholars have also suggested that placing a phone in a Faraday bag would prevent any risk of remote control deletion.[56] Faraday bags are designed to prevent a phone from receiving any signals when powered on, and are relatively inexpensive.[57] As a result, it was argued that a police officer could simply place a phone into one of these bags to prevent remote control deletion.[58] However, as Daniel Scanlan observes, "these bags are not always completely effective at blocking transmissions."[59] Moreover, Faraday bags do not prevent "logic bombs" from operating.[60] A logic bomb is designed to overwrite information if a triggering event (such as entering a particular code) does not occur within a period of time.[61] A logic bomb may be activated

---

[53] *Ibid* at 160. See also Tim Schiesser, "Guide to Smartphone Hardware: Memory and Storage" *Neowin* (12 March 2012), online: <https://www.neowin.net/news/guide-to-smartphone-hardware-37-memory-and-storage>.
[54] See Sean Gallagher, "Memory that Never Forgets: Non-Volatile DIMMs Hit the Market" *Arstechnica* (4 April 2013), online: <https://arstechnica.com/information-technology/2013/04/memory-that-never-forgets-non-volatile-dimms-hit-the-market/>. RAM memory has long been susceptible to losing data upon losing power or shutting down. The new "non-volatile DIMMS" make such memory loss much less likely to occur.
[55] *Ibid*. The issue was first decided in *Giles*, *supra* note 29 in 2007.
[56] Most notably see the dissenting reasons in *Fearon*, *supra* note 18 at para 144. See also Fehr, "Cell Phone", *supra* note 30 at 352-53.
[57] *Ibid*.
[58] See for instance *Fearon*, *supra* note 18 at para 144. Post-*Fearon*, this argument still has some traction. See *R v Jones*, 2015 SKPC 29 at para 69, 468 Sask R 264.
[59] See Scanlan, *Digital Evidence*, *supra* note 31 at 160.
[60] See Eamon Doherty, "The Need for a Faraday Bag" *ForensicMag* (21 February 2014), online: <https://www.forensicmag.com/article/2014/02/need-faraday-bag>.
[61] *Ibid*.

by the user at any time.[62] Again, in the context of the adversarial trial, the vast majority of courts were not presented with evidence of the existence of Faraday bags, let alone evidence explaining its frailties.[63] Regardless of the lack of evidence, even the narrow minority in *Fearon* accepted without question the feasibility of battery removal and Faraday bags preventing destruction of evidence.[64]

(iv) Smartphone Capacity

In *Fearon*, the majority concluded that courts "should not differentiate among different cellular devices based on their particular capacities when setting the general framework for the search power."[65] In failing to draw a distinction between the device and its data, the courts have been criticized for missing an opportunity to distinguish smartphones from less sophisticated phones.[66] The latter generally have fewer features, significantly lesser capacity, and are much more difficult to trace as they are not connected to GPS technology.[67] As one author observes, the two types of phones are "too distinct to bear any categorical similarities besides the capacity for emailing, photographing, and making and receiving calls."[68] Yet, the Court's governing framework failed to give any weight to these technological differences. As a result, the Court's reasoning has been criticized for risking serious privacy intrusions, as smartphones provide a vast portal into intimate personal details, while non-smart phones do not.[69] This is not to say that

[62] *Ibid*.
[63] Faraday Bags were primarily discussed in the minority's decision in *Fearon*, *supra* note 18.
[64] See *Fearon*, *supra* note 18 at para 144. It is notable that the Court does not discuss the likelihood of this type of deletion occurring. No cases were cited to illustrate this problem. However, as technology advances it is not unreasonable to predict that this tactic will be employed by more criminals to hide or destroy evidence.
[65] *Ibid* at para 52
[66] See Fine, "Dumb Phones", *supra* note 2 at 179.
[67] *Ibid*.
[68] *Ibid*.
[69] See *Fearon*, *supra* note 18 at para 131.

distinguishing between types of cell phones is simple. However, ignoring the significant differences between the privacy interests in different phones is hardly more palatable.

Of equal concern is the assumption that officers searching a smartphone will be able to conduct the nuanced types of searches permitted by the Court. The majority permitted searching "only recently sent or drafted emails, texts, photos and the call log."[70] The intrusiveness of a cell phone search therefore appears to be low. Yet, as Jordan Fine observes, conducting such searches on modern smartphones is much more complex:

> Unless law enforcement has been given precise testimony as to where in a device discoverable evidence can be found, *an indefinite search through data will have to be made*. Even if police received a tip that photographic evidence existed on a phone, its location would be a mystery. Would it be in Instagram, a photo sharing application, or is it hidden on the SD card? If the evidence is a text message, is it in a common messaging platform like WhatsApp, or encrypted inside TextSecure?[71]

In criticizing a pre-*Fearon* rule developed in *R v Polius*,[72] which permitted police to conduct what the court termed a "cursory" search of a cell phone incident to arrest, Steven Penney made a similar observation:

> The problem is the indeterminacy of "cursory". Depending on the nature of the device and its operating system, quantity and type of information contained in it, sophistication of the police examining it, and other factors, the intrusiveness of a cursory search may vary greatly.[73]

Given the fundamental differences between searches of different types of modern phones, it is unlikely that these courts had the evidence necessary to fully appreciate the ways in which such phones would be searched. As the courts were likely conscious of this evidentiary lacuna, it was

---

[70] *Ibid* at para 76.
[71] See Fine, "Dumb Phones", *supra* note 2 at 180-81 [emphasis added].
[72] (2009), 196 CRR (2d) 288, 84 WCB (2d) 343 (ONSC).
[73] See Steven Penney, "Searches of Digital Devices Incident to Arrest: R v Fearon" (2014) 23 Constitutional Forum Constitutionnel 1 at 3.

only reasonable for the majority in *Fearon* to have developed a vague rule as it gave future courts flexibility in deciding cases with more robust factual records.[74]

(v) Privacy Interests

A number of lower court decisions did not focus on the technological facts addressed above. Instead, these decisions focused primarily on the degree of privacy that an accused had in his or her cell phone.[75] In so doing, judges frequently employed questionable metaphors in deciding that cell phone searches were permissible incident to arrest. By comparing digital storage devices to filing cabinets, briefcases, and cupboards, appellate courts, as well as a multitude of trial courts, relied on precedents that permitted such searches in upholding the lawfulness of cell phone searches incident to arrest.[76]

By relying upon such metaphors the lower courts overlooked both qualitative and quantitative differences with respect to modern smartphones.[77] These phones contain substantially more information (much of which is private), store records of every action taken on the device, retain information even after users believe the evidence is destroyed, and permit access to

---

[74] For a more detailed explanation of the inherent indeterminacy of the rule in *Fearon*, see Tim Quigley, "*R. v. Fearon*: A Problematic Decision" (2015) 15 CR (7th) 281. I should also note that I do not agree that cell phone searches incident to arrest are constitutional. See Fehr, "Cell Phone", *supra* note 30; Fehr & Biden, "Divorced", *supra* note 32. My point is that if these searches are going to be allowed, a vague rule was inevitable given the lack of evidence before the court.

[75] *R v Hiscoe*, 2011 NSPC 84 at para 15, 310 NSR (2d) 142 [*Hiscoe NSPC*] and *Cater*, *supra* note 46 are good examples.

[76] See *Vu*, *supra* note 18 at para 43 overturning the British Columbia Court of Appeal (2011 BCCA 536, 285 CCC (3d) 160) for use of such a metaphor. In the search of cell phone incident to arrest context, see *R v Beauchamp* (2008), 58 CR (6th) 177 at para 40, 171 CRR (2d) 358 (OSCJ); *R v Fearon*, 2010 ONCJ 645 at para 51, [2010] OJ No 5745 [*Fearon ONCJ*]; *Giles*, *supra* note 29 at paras 56 and 63; *Polius*, *supra* note 72 at para 45; *R v Mann*, 2012 BCSC 1247 at para 68, CRR (2d) 49 (adopting *Giles*); *R v Dhillon*, 2013 BCSC 869, 106 WCB (2d) 503 (adopting *Giles*); *Young v Canada*, [2010] NJ No 389, 91WCB (2d) 452 (adopting *Giles*); *R v Howell*, 2011 NSSC 284 at para 26, 313 NSR (2d) 4; *R v Franko*, 2012 ABQB 282 at paras 157, 173-75, 541 AR 23; *Cater NSPC*, *supra* note 46 at para 54 (though the judge restricted his comments to "dumb phones"). Some courts found otherwise. See *Hiscoe NSPC*, *supra* note 75 at paras 40-43 affirmed on appeal 2013 NSCA 38 at para 75, 297 CCC (3d) 35 [*Hiscoe NSCA*]; *R v Mann*, 2014 BCCA 231, 310 CCC (3d) 143. See also Kerr, "Fourth Amendment", *supra* note 2 at 875 for some American examples.

[77] See *Fearon*, *supra* note 18 at paras 125-34. See also *Vu*, *supra* note 18 at para 47. It should be noted, however, that the Supreme Court of Canada corrected this mistake in *Fearon* and *Vu*.

information not "in" the cell phone itself.[78] Despite these differences, a surprising number of lower courts significantly downplayed the privacy interests that an individual has in his or her modern cell phone.[79]

One potential explanation for courts relying on inapt analogies lies in the adversarial system's tendency to focus on the narrow facts of a case. In the cases dealing with older generation phones, the capacity of the phone at issue was significantly less than any smartphone. An analogy to a briefcase or an address book makes much more sense in this context. At least one court explicitly stated that it was relying exclusively on the technological capabilities of the phone at issue when relying on such a metaphor.[80] The fact that relatively few courts drew this more nuanced analogy suggests that many courts failed to understand the differences between smartphones and cupboards.[81]

The courts that did focus on the capacities of phones revealed yet a different problem: the failure of the adversarial system to consider a complete picture of available and foreseeable technology. The Nova Scotia Provincial Court's decision in *R v Cater*[82] is illustrative. In her decision, Justice Derrick provided an extensive overview of the limited capacity of the accused's cell phone.[83] She then distinguished the accused's phone from smart phones which she analogized to "mini-computers."[84] Relying only on the evidence of the non-smart phone at issue, Justice Derrick concluded that searching it incident to arrest was constitutional. Allowing a search of the

---

[78] See *Vu*, *supra* note 18 at paras 41-44. When a file on a personal computer is uploaded to the cloud, it may be synchronized with one's cell phone. See Brian Chen, *Always On: How the iPhone Unlocked the Anything-Anytime-Anywhere Future—and Locked Us In* (Boston: Da Capo Press, 2012) at 130-143.
[79] See note 76 above.
[80] See *Cater NSPC*, *supra* note 46 at para 54.
[81] My overview of the cases revealed that only four courts explicitly drew this more nuanced analogy. See *Cater NSPC*, *supra* note 46; *Fearon ONCA*, *supra* note 43; *Fearon ONCJ*, *supra* note 76; *R v Manley*, 2011 ONCA 128, 269 CCC (3d) 40.
[82] *Supra* note 46.
[83] *Ibid* at paras 41-42.
[84] *Ibid*.

cell phone at issue could not, however, result in a broader "one size fits all" rule for searching cell phones incident to arrest.[85] Deciding the merits of any search of a smartphone incident to arrest would have to wait for another day, or more likely another year.

(b) Internet Service Provider Subscriber Information

The inability of police to immediately ascertain who is behind the keyboard when a criminal act is committed online has led to numerous investigative challenges. Foremost among these issues is whether police must obtain preauthorization before obtaining subscriber information from Internet Service Providers (ISPs).[86] Subscriber information in this context includes the name, address, and telephone number of the customer using a targeted Internet Protocol (IP) address.[87] Whether users had a reasonable expectation of privacy in their subscriber information in turn depended in large part on what type of information an IP address could reveal about a user's online activity.[88] Courts developed several different views on this point, many of which affected their legal conclusions as to the appropriate constitutional protections applicable to ISP subscriber information.

(i) IP Addresses

An IP address is a numerical identification assigned to computer devices that are using a computer network linked to the internet.[89] IP addresses may either be static or dynamic.[90] Static

[85] *Ibid* at para 46.
[86] See *Spencer*, *supra* note 18 at paras 8-13. Police typically begin such investigations by obtaining the IP address that obtained the child pornography files. The investigating officer can then run the IP address through a database which matches IP addresses with approximate locations and service providers. The officer then makes a "law enforcement request" to the relevant service providers requesting that it release the subscriber information related to the IP address. With this information, the police may then obtain a warrant to seize and search the suspect computer.
[87] *Ibid*.
[88] The case law will be discussed below.
[89] Office of the Privacy Commissioner of Canada, "What an IP Address Can Reveal About You" (May 2013), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/> at 8.
[90] *Ibid*.

addresses are permanently assigned, typically to a server, firewall, or router.[91] Dynamic addresses, which are more common for personal use, are assigned to network-connected devices on a temporary basis.[92] A dynamic IP address may be assigned for different time periods, varying from a few days to a few months.[93] The duration of the assignment depends on several factors including the number of IP addresses available to the ISP, the number of subscribers using those IP addresses, and the stability of the ISP's network.[94]

Every communication conducted on the internet involves an exchange of the sending and receiving parties' IP addresses.[95] These IP addresses are in turn frequently logged by internet servers for future use and are readily retrievable by sending and receiving parties.[96] With knowledge of a parties' IP address, anyone can use a publicly available database to learn which ISP allocated that IP address, as well as the approximate location of the ISP.[97] The identity of the person assigned an IP address is not detectable, however, without assistance from the issuing ISP.[98] As ISPs exclusively assign IP addresses, they have sole access to the information revealing which computer was using a particular IP address at any given time.[99]

(ii) What an IP Address Reveals

---

[91] *Ibid*. Resources such as servers or printers are generally given static IP addresses to allow users on the relevant network to readily find these devices. See Joshua McIntyre, "Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information" (2011) 60 DePaul Law Review 895 at 900 citing Frederick Lah, "Are IP Addresses 'Personal Identifiable Information'?" (2008) 4:3 I/S: A Journal of Law & Policy for the Information Society 681 at 690. However, as Lah observes, some cable and broadband connections use static IP addresses.

[92] *Ibid*.

[93] *Ibid*. As Lah, "IP Addresses", *supra* note 91 observes at 689, "[i]n theory, the address a user gets from the DHCP can change over time, but in practice servers often return the same address to the same client for weeks to months at a time."

[94] *Ibid*.

[95] See McIntyre, "Balancing", *supra* note 91 at 900.

[96] For a good overview, see McIntyre, "Balancing", *supra* note 91 at 895-96.

[97] See Lah, "IP Addresses", *supra* note 91 at 695. He cites the public database known as "RIPE Database Search" as an example of an IP address detector. Although there are ways to inhibit people from finding your exact location—such as use of a Virtual Private Network (VPN)—many users do not take these steps.

[98] See Lah, "IP Addresses", *supra* note 91 at 694-95.

[99] See McIntyre, "Balancing", *supra* note 91 at 897; Lah, "IP Addresses", *supra* note 91 at 694-95; Daniel Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy" (2002) 75 California Law Review 1083 at 1143.

The privacy interests implicated by acquisition of IP addresses has the ability to affect several legal issues, ranging from whether a reasonable expectation of privacy exists in such information to the requirements for any law allowing such searches to be considered "reasonable" under section 8 of the *Charter*.[100] For instance, if only a "snapshot" of a user's internet history is revealed, an authorizing law *may* pass constitutional muster on the reasonable suspicion standard, or on some lower requirement such as an administrative demand letter. This follows as the intrusiveness of a breach is inherently less serious if it only revealed what was necessary to obtain a warrant.[101] Such a low standard is obviously problematic if acquisition of an IP address results in police obtaining an extensive history of a user's internet activity. Unfortunately, the evidence submitted in the jurisprudence did not resolve this question.

Several courts concluded that nothing of importance was revealed by supplying police with an IP address.[102] Only a name, address, and telephone number—all of which, these courts maintained, do not attract a reasonable expectation of privacy.[103] As Justice Ottenbreit of the Saskatchewan Court of Appeal reasoned, any potential for IP addresses to reveal intimate details of internet usage was "neither here nor there."[104] Defendants generally responded by contending that it is necessary to look beyond the mundane information revealed by IP addresses.[105] Police,

---

[100] The Ontario Court of Appeal's discussion in *R v Ward*, 2012 ONCA 660, 112 OR (3d) 321 is illustrative. The Court used the fact that only a "snapshot" of the accused's internet history was revealed to police (as opposed to the user's whole internet history) as a factor when considering whether the accused maintained a reasonable expectation of privacy in ISP subscriber information. As will be explained in more detail below, the Court ultimately found the expectation of privacy was unreasonable.

[101] *Ibid*.

[102] See *R v Ward*, 2008 ONCJ 355 at paras 55-70, 79 WCB (2d) 129; *R v Friers*, 2008 ONCJ 740 at paras 23-24, [2008] OJ No 5646; *R v Spencer*, 2009 SKQB 341 at paras 17-18, 361 Sask R 1; *R v Trapp*, 2009 SKPC 5 at para 14, 330 Sask R 169; *R v Wilson*, [2009] OJ No 1067 at para 42, 2009 CarswellOnt 2064 (ONSC); *R v McNeice*, 2010 BCSC 1544 at para 49, 91 WCB (2d) 178; *R v Brousseau*, 2010 ONSC 6753 at paras 34-37, 264 CCC (3d) 562; *R v Smith*, (unreported, December 19, 2003, BCSC 119747). For courts determining that a reasonable expectation of privacy existed in ISP subscriber information see *Re C.(S.)*, 2006 ONCJ 343,71 WCB (2d) 241; *R v Kwok*, [2008] OJ No 2414, 78 WCB (2d) 21; *R v Cuttell*, 2009 ONCJ 471, [2009] OJ No 4053.

[103] *Ibid*.

[104] See *R v Spencer*, 2011 SKCA 144 at para 110, 377 Sask R 280.

[105] See *Spencer*, *supra* note 18 at paras 24-25.

after all, did not want ISP subscriber information for any other reason than to determine who was using the internet for a specific purpose.[106]

The courts that understood that some internet activity was revealed were unable to discern the quality and quantity of that information. The divergent views found in the Saskatchewan Court of Appeal's decision in *R v Trapp*[107] and the Ontario Court of Appeal's decision in *R v Ward*[108] are illustrative. As Justice Cameron (Justice Jackson concurring) concludes in *Trapp*, identifying a customer's IP address can provide a complete history of the accused's activity.[109] However, he also observes that the initial police request only concerned activity occurring within a one-minute period on the internet.[110] In determining whether a reasonable expectation of privacy existed, Justice Cameron suggests that "[t]he point…is not about what the police did, but rather about the *quality* of this kind of information, namely *its potential to reveal much about the individual*".[111] Yet, if the relevant request only provided for a small snapshot of the user's browsing history, it is entirely unclear how this would "reveal much about the individual."

The Court in *Ward* rejected the view endorsed by the majority in *Trapp*.[112] As Justice Doherty observes, the police testimony revealed that the investigating officers had access to only seconds of the user's internet activity.[113] As such, Justice Doherty concludes: "[o]n this record, what is revealed is more in the nature of a snapshot than a history of one's Internet

---

[106] See *Ward ONCA*, *supra* note 100 at paras 67-68; *Cuttell*, *supra* note 102 at para 22.
[107] 2011 SKCA 143, 377 Sask R 246.
[108] *Supra* note 102.
[109] *Ibid* at para 36.
[110] See *Trapp*, *supra* note 107 at para 28.
[111] *Ibid* at para 37 (second emphasis added). Justice Cameron repeats this conclusion in *Spencer SKCA*, *supra* note 104 at para 98. See also *Cuttell*, *supra* note 102 at para 21.
[112] See *Ward ONCA*, *supra* note 100 at paras 18, 69, 109. Justice Doherty further cites *Kwok*, *supra* note 102 at para 8 for this proposition.
[113] See *Ward ONCA*, *supra* note 100 at para 25. The specific times and place that the offender accessed child pornography were provided by German authorities. A German-based general forum was being used nefariously for accessing and sharing child pornography. The owner of the website informed German authorities, and the relevant IP addresses were subsequently sent to Canadian authorities.

activity."[114] Ultimately, he concludes that revealing even small amounts of anonymous internet activity touched on intimately personal information usually attracting a reasonable expectation of privacy.[115] However, the fact that the information was turned over to a third party—the ISP—negated the reasonableness of the expectation of privacy. A reasonable person would consider the ISP's self-interest as well as civic interest in disclosing narrow information for the purpose of a child pornography investigation to be objectively reasonable.[116]

Which view is correct? The answer is: it depends. The extent of the information revealed turns on what the police actually do with a person's IP address. Although police retrieved a robust history of Mr. Trapp's internet activity, it is important to recognize that this required a *further* search to be conducted. As Justice Ottenbreit unwittingly describes in his dissenting reasons, the investigating officer independently "generated an 'IP History' for [the accused's] IP [address] by means of a software program available to the police for that purpose."[117] As the Office of the Privacy Commissioner has explained,[118] this is easily done with tools such as WHOIS, an "online service used for… querying databases that store the registered users or assignees of domain names or IP address blocks."[119]

As websites frequently store IP addresses,[120] it is possible to come to reasonable inferences about where an IP address has been on the internet. These inferences may become less reliable as time passes as dynamic IP addresses are frequently reassigned; however, this would not be the

---

[114] *Ibid*. See also para 18.
[115] *Ibid* at para 93.
[116] *Ibid* at paras 93-109 citing Andrea Slane and Lisa Austin, "What's in a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations" (2011) 57 Criminal Law Quarterly 486.
[117] See *Trapp SKCA*, *supra* note 107 at para 78. I say "unwittingly" because Justice Ottenbreit does not describe this technique or use this information in assessing whether a breach of section 8 of the *Charter* occurred independent of the initial request.
[118] See OPC, "IP Address", *supra* note 89 at 2-7.
[119] *Ibid* at 2.
[120] See McIntyre, "Balancing", *supra* note 91 at 895-96.

case with permanently assigned or "static" IP addresses. For present purposes, it is important to observe that this additional search was not necessary to obtain a warrant to seize either offender's computer. This follows as knowledge that a known user's IP address possessed and/or shared child pornography on one occasion will generally provide police with reasonable and probable grounds to obtain a warrant to seize the suspect computer and search its contents.[121]

When the issue finally reached the Supreme Court of Canada in *R v Spencer*,[122] this factual confusion had not been corrected. As the Court observed, "[t]here is little information in the record about the nature of IP addresses in general or the IP addresses provided by Shaw to its subscribers."[123] Although the Court notes that other cases have discussed what an IP address may reveal,[124] the record only allowed for the conclusion that an IP address was able to "match" computer activity.[125] The Court's conclusion that the request at issue "engages a high level of informational privacy"[126] suggests the Court was sympathetic to the view that IP addresses inherently reveal a user's general web history.[127] This cannot be assumed, however, as police may look no further than the precise moment in time when it discovered that a particular IP address viewed, possessed, and/or distributed criminal content.

Given the above, the Court's conclusion in *Spencer* that accused persons have a reasonable expectation of privacy in ISP subscriber information remains controversial.[128] If the state need only access a moment when an accused was on the internet, it is more sensible to weigh the potential to reveal some narrow—though often personal—information about an individual against

[121] See generally *Spencer*, *supra* note 18; *Ward ONCA*, *supra* note 100.
[122] *Supra* note 18.
[123] *Ibid* at para 8.
[124] *Ibid* citing *Ward ONCA*, *supra* note 100.
[125] See *Spencer*, *supra* note 18 at para 8.
[126] *Ibid* at para 51.
[127] Steven Penney makes a similar point. See Penney, "Digitization", *supra* note 2 at 529-30.
[128] *Ibid*. See also the reasons of Justice Doherty in *Ward ONCA*, *supra* note 100.

law enforcement needs. Justice Doherty's reasons in *Ward* become much more palatable with this corrected factual record. Even if a reasonable expectation of privacy were recognized, a search on a lower standard than reasonable grounds to believe an offence occurred could qualify as a "reasonable" search under section 8 of the *Charter*. With a clearer evidential record, the Court in *Spencer* would have been in a position to provide such a dialogical response to Parliament's legitimate law enforcement concerns.[129] Instead, the Court restricted itself to a finding that the search was not "authorized by law".[130]

(iii) Responding to Spencer

In determining the appropriate standard for police to access ISP subscriber information, it is necessary to strike a reasonable balance between the law enforcement and privacy interests at the heart of section 8 of the *Charter*.[131] Privacy interests are most clearly implicated by the fact that some intimate information—sexual preferences in *Spencer*—is revealed when police are able to access ISP subscriber information. However, as the state need only access a moment when an accused was on the internet, it is more sensible to weigh the potential to reveal some narrow—though potentially intimate—information about an individual against law enforcement needs.

The fact that some intimate information will be revealed must also be considered in light of the number of requests that are made by police. Post-*Spencer*, police representatives have urged the public to trust them with warrantless access to ISP subscriber information, claiming that police have been careful not to abuse such authority in the past.[132] This claim is difficult to support in

---

[129] For an overview of dialogue theory see Peter Hogg and Allison Bushell, "The *Charter* Dialogue Between Courts and Legislatures (Or Perhaps the *Charter of Rights* isn't Such a Bad Thing After All)" (1997) 35 Osgoode Hall Law Journal 75.

[130] For a law to qualify as reasonable under section 8 of the *Charter*, it must be authorized by law, the authorizing law must be reasonable, and the search itself must be carried out in a reasonable manner. See *R v Collins*, [1987] 1 SCR 265 at 278, 38 DLR (4th) 508. Any dialogical response would at least require an answer to the second question.

[131] See *Hunter*, *supra* note 28 at 159-60.

[132] See Patricia Joseph, "A TheCourt.ca Exclusive Interview: R v Spencer One Year Later" *TheCourt.ca* (24 September 2015), online: <http://www.thecourt.ca/a-thecourt-ca-exclusive-interview-r-v-spencer-one-year-later/>.

light of the vast number of warrantless requests that were made for ISP subscriber information in Canada pre-*Spencer*.[133] As the amount of requests greatly outnumber any prosecutions for online crimes, it is reasonable to infer that police were at times making requests which were more akin to fishing expeditions than searches founded upon a reasonable basis.[134]

Consideration of the countervailing law enforcement interests must begin with the fact that internet-based crimes are inherently difficult to detect. As Justice Doherty observed in *Ward*, "[e]asy entry to the Internet, from almost anywhere, the international nature of the trade in child pornography and user anonymity combine to make effective law enforcement difficult."[135] Detective Sergeant Kim Gross has expanded upon this view post-*Spencer*, noting that applying for a production order provides yet another significant barrier:

> [T]he paperwork involved with obtaining a Producti[on] Order is extensive. Depending on the circumstances, it could take an officer days or even weeks to construct a Production Order. At that point we must wait for approval from a Justice of the Peace, if we even get approval, and then submit it to the ISP to be fulfilled. At the point it reaches the ISP, it often takes 30 days to receive the subscriber information back from the company.[136]

As this statement implies, requiring police to use significantly more resources per investigation will inevitably slow down investigations and, in some cases, prevent police from furthering investigations.[137] It is therefore no surprise that police have described the long-term consequences of *Spencer* as "extremely detrimental".[138]

With these competing interests in place, it is also necessary to ask whether any privacy concerns may be assuaged. This may be accomplished in several ways. First, any proposed law

---

[133] See generally Matthew Ponsford, "The Lawful Access Fallacy: Voluntary Warrantless Disclosures, Customer Privacy, and Government Requests for Subscriber Information" (2017) 15 Canadian Journal of Law and Technology 153.
[134] *Ibid*.
[135] See *Ward ONCA*, *supra* note 100 at para 1.
[136] See Joseph, "One Year Later", *supra* note 132.
[137] *Ibid*.
[138] *Ibid*.

could require that police have a reasonable basis to conclude that a child pornography-related offence has been committed. In a typical investigation such as the one in *Spencer*, this would be easy to prove. Undercover police officers are generally able to determine upon viewing a file whether it qualifies as child pornography.[139] Making this requirement explicit would nevertheless mitigate police fishing expeditions.

A second limitation could require that any authorizing law focus on investigations that do not require broad access to a user's internet history. Child pornography investigations fit this description. Very rarely is there controversy over whether an accused actually possessed or accessed child pornography. The issue is whether the police acquired internet user history in accordance with *Charter* standards. As even a limited duration of possession provides sufficient grounds to grant a warrant, there can be little concern about whether the police will catch innocent conduct when they ask for ISP subscriber information in a typical child pornography investigation.[140]

A third limitation could require that police report the number and type of searches undertaken. As discussed above, police have been accused of overshooting their boundaries when given free rein to access users' ISP subscriber information.[141] A reporting requirement would allow for detection of trends in police acquisition of ISP subscriber information. A similar limitation was constitutionally required for warrantless interception orders under Part VI of the *Criminal Code*.[142] Given the potential for abuse, this requirement provides a safeguard that can help ensure police are held accountable.

---

[139] It is very much a "know it when you see it" type of offence.
[140] Compare the level of difficulty police would face in identifying child pornography as opposed to whether certain speech constituted hate speech. The latter is highly contextual, as the words used and the underlying intent of the speaker takes its meaning from the context surrounding the speech. More expansive investigation into an accused's online activities would therefore likely be necessary to make out grounds for a warrant.
[141] See Ponsford, "Lawful Access", *supra* note 133.
[142] See generally *R v Tse*, 2012 SCC 16, [2012] 1 SCR 531.

Finally, to illustrate the seriousness of any broader invasions of privacy, it would be prudent to provide for automatic exclusion of all evidence if the police overstep their boundaries and search the relevant IP address. As explained above, this additional search is capable of disclosing a broad history of the accused's internet access. Automatic exclusion of all evidence should provide police with sufficient deterrence from such invasive warrantless searches. As such a search is unnecessary to obtain a warrant in typical online child pornography investigations, it is unlikely that courts would need to apply such a provision.

With these limitations in place, it is possible that a significantly lower standard may be used to obtain ISP subscriber information, at least in child pornography investigations. The only private information that is at risk of being revealed is the offender's sexual interests which, although private, are unlikely to be mistaken for anything other than illegitimate, harmful, and criminal activity. This must be balanced against the importance of prosecuting child pornography offences, which are notoriously difficult to investigate as a result of their pervasiveness on the internet. So long as police are not allowed to conduct a secondary search of the relevant IP address, it is my view that a legislative version of the previous status quo—requiring only that police make an administrative demand to ISPs—ought to pass constitutional muster.

(c) The Definition of "Intercept"

The advent of email and text messaging have posed novel challenges for police investigations. If the email or text does not exist at the time of a warrant application, the Court has concluded that police must meet the stringent requirements of an intercept warrant under Part VI of the *Criminal Code*.[143] If the same message is accessible to a third party at the time of the

[143] For instance, such authorizations must be made by the Attorney General, Minister of Public Safety and Emergency Preparedness, or an agent specially designated by one of those parties (section 185(1)). The application must be brought to a superior court (*ibid*), with numerous detailed requirements with respect to the type of information that must be put before the justice hearing the application (186(1)). After a stipulated amount of time has elapsed, the

application, police may apply for an order compelling that party to produce its contents pursuant to the less onerous production order scheme in section 487.014 of the *Criminal Code*.[144] Whether this judicial interpretation of the term "intercept" accords with technological reality has been the subject of significant disagreement.

(i) Jurisprudence

In *R v Telus Communications Co*.,[145] the Court considered whether an intercept warrant was required for the prospective, daily production of messages stored on Telus' computer database.[146] As the messages were voluntarily stored, the Crown maintained that it was not intercepting the communications.[147] Although intercept warrants apply whenever police listen to, record, or acquire the substance of a communication,[148] the Crown contended that the plain meaning of the word "intercept" excluded any instances where a third party disclosed communications it independently obtained.[149] The police therefore sought to have Telus produce the messages pursuant to the general warrant provision in section 487.01.[150] As the prerequisites for obtaining a general warrant are easier to meet than those required for an intercept warrant,[151] it was necessary to determine whether the police investigative technique qualified as an intercept.

---

police must also notify the subject that the interception took place (sections 189 and 196). The state must also issue annual reports with respect to how often they utilize Part VI intercepts (section 195). Finally, and most importantly, the issuing justice must be satisfied that granting the application is not only in the "best interests of the administration of justice" (section 186(1)(a)), but also that "no other reasonable alternative method of investigation in the circumstances of the particular criminal inquiry [is available]" (section 186(1)(b) as interpreted in *R v Araujo*, 2000 SCC 65 at para 29, [2000] 2 SCR 992).

[144] This provision requires only that police have reasonable grounds to believe that an offence has been committed and that information in the documents sought will aid in an investigation. Contrast this with the more onerous standard described for intercept warrants *supra* note 143.

[145] 2013 SCC 16, [2013] 2 SCR 3.

[146] *Ibid* at para 1.

[147] *Ibid* at paras 10, 21. Section 487.01(c) requires that no other provision be available before police can resort to the general warrant. If the tactic at issue constituted an "intercept", then Part VI was available thus precluding resort to the general warrant.

[148] See section 183.

[149] See *Telus*, *supra* note 145 at paras 140-44.

[150] *Ibid* at para 7.

[151] *Ibid* at para 9. For an expansive explanation of each section, see paras 116-22.

The Court recognized the need to ensure that technological advancement did not render the definition of intercept meaningless.[152] As Justice Abella wrote for the plurality, text messages are different from traditional voice communications.[153] Receipt of the message depends on many factors such as whether the receiving phone is activated, within range of a cell tower, or been viewed by the recipient.[154] Regardless of whether a message has been delivered, a copy of the message may (as occurs with Telus users) be stored on a server the moment it is sent.[155] As such, allowing police to access such messages on a prospective and daily basis makes it possible for police to obtain the communication before its intended recipient.[156] As a result, Justice Abella concluded that "[a] narrow or technical definition of 'intercept' that requires the act of interception to occur simultaneously with the making of the communication itself is…unhelpful in addressing new, text-based electronic communications."[157]

Justice Moldaver, writing for the remaining members of the majority, concurred in the result of Justice Abella's plurality decision.[158] However, he did not base this conclusion on an interpretation of Parliament's definition of "intercept".[159] Instead, he drew the more cautious conclusion that the police tactic was "substantively equivalent" to an intercept.[160] As the police could have applied for a Part VI intercept warrant, the legal prerequisite for a general warrant to

[152] Although she wrote for a plurality, the judgement of Justice Moldaver (Justice Karakatsanis concurring) agreed with this general view. See para 52.
[153] See *Telus*, *supra* note 145 at para 34.
[154] *Ibid* at para 34.
[155] *Ibid* at para 34.
[156] *Ibid* at para 40. For instance, this could occur if police access the "sent" message before it arrives at the intended recipient's phone.
[157] *Ibid* at para 34.
[158] *Ibid* at para 53.
[159] *Ibid*.
[160] *Ibid* at para 52.

issue found in section 487.01(c) that no other available provision be available had not been met.[161] As such, the warrant was quashed by the majority.[162]

Writing in dissent, Justice Cromwell concluded that Part VI drew a fundamental distinction between *intercepting* a communication and *retention, use, or disclosure* of a communication.[163] As Telus independently intercepted the relevant communications, the police were merely asking that Telus disclose those communications at some specified future point in time. Part VI therefore did not apply. Moreover, as the application was prospective, the production order scheme was also inapplicable. Such orders, Justice Cromwell concluded, only apply to communications already in existence at the time of the application.[164] As such, the general warrant requirement that no other provision be available had been satisfied.[165]

The issue of whether production orders could be used to obtain stored communications content was directly raised four years later in *R v Jones*.[166] Relying primarily on Justice Abella's plurality reasons in *Telus*, the accused argued for a broad interpretation of the word "acquire" under the definition of "intercept."[167] If given its plain meaning, the accused contended, the police "acquire" a "private communication" when requiring a telecommunication company to produce *any* text messages.[168] Justice Abella, writing for herself, reiterated her earlier position that this

[161] *Ibid* at paras 50-53.
[162] *Ibid*. Justice Abella's plurality opinion agreed with Justice Moldaver's alternative resolution, but also went one step further and incorporated this understanding into the definition of intercept. See para 20.
[163] *Ibid* at paras 132-48.
[164] *Ibid* at para 10.
[165] See section 487.01(1)(c).
[166] 2017 SCC 60, [2017] 2 SCR 696.
[167] *Ibid* at para 56.
[168] *Ibid*. This contention received at least some support Pre-*Telus* and post-*Telus*. Pre-*Telus* see Charles Morgan, "Employer Monitoring of Employee Electronic Mail and Internet Use" (1999) 44 McGill Law Journal 849 at 875; Jarrod White, "E-Mail@Work.Com: Employer Monitoring of Employee E-Mail" (1997) 48 Alabama Law Review 1079 at 1083; Tatsuya Akamine, "Proposal for a Fair Statutory Interpretation: E-mail Stored in a Service Provider Computer Is Subject to an Interception Under the Federal Wiretap Act" (1999) 7 Journal of Law and Policy 519 at 561-65. Post-*Telus* see *R v Croft*, 2013 ABQB 640, 573 AR 339; Steven Coughlan, "Telus: Asking the Right Questions About General Warrants" (2013) 100 CR (6th) 290; Alan Gold, '"If the Shoe Fits…and Wonderfully so': Part VI of the Criminal Code Should be Applied to Digital Communications" (2016) 28 CR (7th) 44; Gerald Chan, "What Does

approach was consistent with the need to ensure that "the broad and general right to be secure from unreasonable search and seizure… keep[s] pace with technological development".[169] As stored private communications arguably raise similar intrusions as prospective captures of the same content,[170] reading the term "acquire" broadly allows section 8 jurisprudence to respond to technological change in a more principled manner.[171]

The Crown successfully repeated the minority's argument in *Telus* that this understanding of "acquire" was inconsistent with the statutory scheme in Part VI. The key distinction drawn by Part VI is between "interception" and "disclosure."[172] As Telus intercepted the communications for its own purposes, the state was merely requesting that Telus disclose those communications.[173] As disclosure of material in third party possession fits squarely within the production order scheme, it was unnecessary to meet the more onerous demands of Part VI.[174] This interpretation was also supported by the fact that accepting a broad reading of "acquire" would result in many common searches of private communications—such as searching a computer pursuant to section 487(2.1) or ordering production of cell phone or email communications under section 487.014—coming within the ambit of Part VI. As a substantial body of jurisprudence held to the contrary, the Court was not willing to accede to this view.[175]

(ii) The Prospective/Retrospective Distinction

Telus Say About Retrospective Seizures of Private Communications?" For the Defence Magazine Vol 34:4 (28 October 2013).

[169] See *Jones*, *supra* note 166 at para 101 citing *R v Wong*, [1990] 3 SCR 36 at 44, 60 CCC (3d) 460.

[170] See *Jones*, *supra* note 166 at paras 104-05.

[171] *Ibid* at paras 101-05.

[172] *Ibid* at para 61.

[173] *Ibid* at para 75-81.

[174] *Ibid*.

[175] See *Telus*, *supra* note 145 at para 155 citing *Cole*, *supra* note 18 at para 73; *R v Jones*, 2011 ONCA 632 at para 33, 107 OR (3d) 241; *R v Bahr*, 2006 ABPC 360, 434 AR 1; *R v Cross*, 2007 CanLII 64141 at paras 25-27 (ONSC); *R v Little*, 2009 CanLII 41212 at para 154, [2009] OJ No 3278; *R v Tse*, 2008 BCSC 906 at para 198, [2008] BCJ No 1766; *R v Weir*, 2001 ABCA 101 at para 19, 281 AR 333.

Although the decision in *Jones* does not affect the majority ruling in *Telus* that Part VI intercepts will be required when prospective messages are retrieved,[176] its narrow interpretation of the term "intercept" may have constitutional implications.[177] At the heart of any constitutional challenge will be whether the distinction between prospective and retrospective searches has broken down due to technological advancement. Although Justice Rowe in *Jones*[178] and Justice Moldaver in *Telus*[179] raised this issue, neither Justice was willing to go as far as Justice Abella,[180] who would have subjected all stored private communications to the intercept regime.[181] Although such restraint is reasonable, it leaves open the question of whether some stored retrospective communications engage the same privacy interests as prospective communications.

Compared to retrospective searches, prospective searches or "interceptions" have traditionally been thought to be more invasive for several reasons.[182] First, they are more likely to invade the privacy of unknown and innocent individuals.[183] With a wiretap, for instance, it may be impossible to tell in advance whether a communication is relevant to the police's investigation.[184] Second, the "indiscriminately acquisitive" nature of interceptions make them more likely to reveal sensitive information that is unrelated to criminal activity.[185] Third, interceptions tend to extend for longer periods of time and acquire substantially more content as private communications have

---

[176] Justice Abella's plurality opinion agreed with Justice Moldaver's reasons but went one step further and incorporated this understanding into the definition of intercept. See *Telus*, *supra* note 145 at para 20. As the majority in *Jones*, *supra* note 166 rejected Justice Abella's extension of the reasons in *Telus*, that reasoning is no longer authoritative.
[177] A constitutional challenge is especially likely to happen given Justice Rowe's caution in *Jones*, *supra* note 166 at paras 83-87 that section 487.014 may be constitutionally infirm.
[178] See *Jones*, *supra* note 166 at paras 83-87.
[179] See *Telus*, *supra* note 145 at para 68, footnote 2 (Justice Karakatsanis concurring).
[180] Justices Fish and LeBel concurring.
[181] See generally her dissenting reasons in *Jones*, *supra* note 166.
[182] See Steven Penney, "Updating Canada's Communications Surveillance Laws: Privacy and Security in the Digital Age" (2008) 12 Canadian Criminal Law Review 115 at 131-32.
[183] *Ibid* citing *Berger v New York*, 388 US 41 (1967) at 65.
[184] *Ibid*.
[185] *Ibid* citing *Scott v United States*, 436 US 128 (1978) at 145; *R v Thompson*, [1990] 2 SCR 1111 at 1166, 73 DLR (4th) 596 (per Justice La Forest).

historically not been consistently recorded.[186] Finally, interceptions make it more difficult to filter irrelevant material.[187] Some stored communications, such as emails on an inbox, are relatively easy to sort through while wiretapping will generally require listening through the content of each communication.[188]

Do these distinctions still hold in the digital age? Consider the following example.[189] The police receive a transmission data recorder warrant under section 492.2 of the *Criminal Code*. Such an order issues on reasonable suspicion that an offence has been or will be committed.[190] Although the transmission data recorder does not retain content of a communication, it tells police when, and with what number, a phone is communicating. Police would therefore be able to apply for a production order shortly after any messages were sent or received by a Telus customer's phone to retrieve the *content* of the suspect's communications.[191] As the police believe that the suspect is communicating criminal content generally,[192] they search all the communications disclosed to them pursuant to the production order.

Each of the four considerations drawn above are applicable in this scenario. Whether innocent people will have their communications interfered with is equally probable with respect to production of stored text messages shortly after they are delivered. This follows because the police do not necessarily know which communications are relevant. The same reasoning applies

---

[186] *Ibid* citing James Dempsey, "Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy" (1997) 8 Alberta Law Journal of Science and Technology 65 at 70; Orin Kerr, "Internet Surveillance Law After the USA Patriot Act: The Big Brother that Isn't" (2003) 97 Northwestern University Law Review 607 at 616-17.
[187] See Penney, "Updating", *supra* note 182 citing Kerr, "Internet Surveillance", *supra* note 186 at 617.
[188] *Ibid*.
[189] This example provides more procedural reality to the interesting example raised by Justice Rowe in his reasons in *Jones*, *supra* note 166 at para 84.
[190] See section 492.1(1).
[191] In *Telus*, *supra* note 145 at para 194, Justice Cromwell observed that the practice of having messages sent to the police on a daily basis for two weeks was "effective and practical". As such, there is good reason to believe that he would permit multiple orders to issue day after day, as contemplated in this scenario.
[192] This is likely to occur in the common scenario of a drug dealer communicating with his or her clientele.

in considering whether the seizure of a private communication via production order is any less likely to inadvertently reveal intimate information. If the police do not know in advance exactly which messages are likely to reveal criminally relevant information, they are just as likely to inadvertently learn of intimately private information about innocent individuals.

Although it is possible for the state to sort through stored communications—the example of an email inbox used above is illustrative—it is unclear how police would accomplish this end with respect to the text messages used in the scenario outlined above. Although police might not observe the contents of a communication if they know a number to be irrelevant, the same can be said when police apply for a Part VI wiretap of a telephone line. A judge might even impose such a requirement in the provisions of the intercept warrant.[193] As such, the ability to sift through irrelevant information and capture only conduct likely to be incriminating is not necessarily more likely with stored messages than it is with traditional wiretaps.

It is nevertheless true that intercepts tend to extend over long periods of time and therefore will gather significant amounts of information. Under Part VI, for instance, an intercept order may be issued for up to sixty days.[194] Yet, some authors contend that the storage capacity available in the digital age will often ensure that *more* information will be available to the state via retrospective seizures of private communications.[195] This follows as "'acquisition' of a digital private communication is not limited temporally to simultaneous acquisition as in the case of 'wiretaps'".[196] At the least, the interests are likely to be the same in the hypothetical scenario under

[193] See section 184.2(4)(d).
[194] See section 184.2(4)(e).
[195] See Chan, "Telus", *supra* note 168. "Consider Justice Cromwell's example of the police seizing the emails and Internet chats stored on a computer. Rather than simply allowing the police to access an individual's private communications over a 13-day period like the general warrant in *TELUS*, such seizures could allow the police to access an individual's private communications over a multi-year period, going all the way back to when the individual first had the computer in personal use. As we now know, computer data always leaves a record, and even deleted files can be recovered forensically."
[196] See Gold, "If the Shoe Fits", *supra* note 168.

consideration. Regardless of whether police apply for a production order every day over a specified period, or have an intercept order over that same period, the same messages would be retained.[197]

Although the distinctions between retrospective and prospective seizure have been eroded by technological development, this does not mean that Justice Abella was correct in concluding that "[t]he only difference between… prospective… and… historical text messages, is the [potentially negligible] timing of the state's request for authorization."[198] This will *sometimes* be the case. Allowing a production order to issue in circumstances where the same interests are engaged therefore raises the potential for a breach of section 8 of the *Charter*.[199] This does not necessarily mean that more carefully tailored searches will be unconstitutional. The majority of the Court was clearly aware of this issue but chose to leave it for another day as it was not strictly necessary to resolve the case at hand.[200]

The constitutionality of the production order scheme is therefore contestable. Although the Court required that notice be given to search targets at some prescribed period after an intercept,[201] it has not considered whether any other prerequisites are constitutionally required. Several lower courts have rejected the contention that Parliament's elimination of the investigative necessity requirement for terrorism and criminal organization offences is unconstitutional.[202] Whether this

---

[197] There are two obvious differences between the intercept and production order procedures. First, as police would have to wait for evidence of a communication before applying for a production order, acquisition of the communications would be delayed for at least a short period of time. Second, the production order procedure would require police to expend more resources. Although applying for multiple production orders requires human capital, it is nevertheless likely that such orders would be nearly identical in content thereby making the orders simple to draft. The real cost, then, would be in the physical application for the order and communicating multiple times with the relevant telecommunication service provider to request the court-ordered communications.

[198] See *Jones*, *supra* note 166 at para 105.

[199] *Ibid*.

[200] Justice Rowe's reasons in *Jones*, *supra* note 166 are illustrative. The minority reasons in *Telus*, *supra* note 145 at paras 189-94 (adopted by the majority in *Jones*) also strongly implied that such searches would be impermissible.

[201] See *Tse*, *supra* note 142.

[202] See *R v Lucas*, 2014 ONCA 561, 121 OR (3d) 303 leave to appeal refused [2014] SCCA No 461; *R v Doiron*, 2007 NBCA 41, 315 NBR (2d) 205 leave to appeal refused [2007] SCCA No 413; *R v Pangman*, 2000 MBQB 85, 147 Man R (2d) 93; *R c Doucet*, 18 CR (6th) 103, [2003] JQ No 18497.

same rationale would apply to other less serious crimes remains questionable. *Obiter* comments by the Court in *Araujo* suggest the investigative necessity requirement is constitutionally required. As the Court concludes, investigative necessity is "one of the safeguards that made it possible for this Court to uphold these parts of the *Criminal Code* on constitutional grounds".[203]

The above review shows that the Court had difficulties defining the term "intercept" in Part VI. This is to be expected given the complexities of modern communication devices. What is most notable about *Telus* and *Jones*, however, is the absence of any critique of the evidentiary record upon which the Court ruled. This is especially notable given that email and text communications are relatively complex phenomenon. The fact that the Court had a wealthy and experienced litigant in *Telus* lay the factual foundation resulted in a clear evidentiary record. The Court took its time in deciding these issues and certainly left more to be decided in the future. However, this appears to result more from a tendency to approach constitutional rules cautiously than because of a misunderstanding of the relevant technology or lack of belief that the evidence was sufficient to make a broader ruling.

III. Digital Technologies and the Adversarial System

Digital privacy jurisprudence affirms that courts often receive inadequate evidence pertaining to digital technologies. It also provides the necessary background to assess whether the three considerations identified in the introduction impact judicial ability to receive adequate evidence implicating digital technologies. Beginning with the resources available to criminal defendants, the cell phone searches incident to arrest cases reveal that most lawyers were

[203] See *Araujo*, *supra* note 143 at para 26. See also *R v SAB*, 2003 SCC 60 at para 53, [2003] 2 SCR 678; *R v Belcourt*, 2015 BCCA 126 at para 47, 322 CCC (3d) 93.

experienced private counsel.[204] Similar conclusions were drawn in the context of ISP subscriber information cases.[205] With respect to the *Telus* and *Jones* cases, the defendant that laid the evidential foundation applied in both cases was a large corporation with the knowledge and resources to explain the nuances of the applicable technology.[206]

The cell phone search and ISP subscriber information cases were not appealed as frequently as expected.[207] As these cases were highly controversial, one might expect accused persons to frequently appeal losses at trials. While the cell phone searches incident to arrest cases were

---

[204] Private: *Polius*, *supra* note 72 (now Justice Victor Giourgas, online: <https://www.linkedin.com/in/vgiourgas/> with co-counsel Marco Sciarra); *Liew*, *supra* note 46 (Alan Gold; Vanessa Arsenault was co-counsel as a member of Gold's firm; online, <https://www.lawyerscanada.net/vanessa-g-arsenault/>); *Cater NSPC*, *supra* note 46 (Elizabeth Cooper, online: <https://www.criminallawyerhalifax.ca>); *Fearon ONCJ*, *supra* note 76 (Sam Goldstein, online: <http://samgoldstein.ca/biography.php>); *Manley ONCA*, *supra* note 81 (Brian Snell, online: <https://www.linkedin.com/in/brian-snell-64462684/>); *R v Finnikin*, 2009 CanLii 82187 (ONSC) (the full names of the lawyers were not provided but the fact that three defence lawyers were assigned suggests they were private not Legal Aid); *R v Otchere-Badu*, 2010 ONSC 1059, 87 WCB (2d) 29 (similarly the full name of counsel was not provided, though as far as I can tell it was private lawyer Michael Quigley, who is now Justice Quigley of Ontario Superior Court of Justice); *Mann*, *supra* note 76 (BSCS and BCCA) (Peter Wilson, Queen's Counsel, online: <https://www.wilsonbutcher.com/lawyers/peter-wilson/>; he was joined by Professor Micah Rankin on appeal); *Dhillon*, *supra* note 76 (Peter Laliberte, Queen's Counsel, online: <https://bc-criminal-law.com/terry-la-liberte/>); *Young*, *supra* note 76 (Renee Appleby, online: <https://www.linkedin.com/in/renee-appleby-676b1398/>); *Franko*, *supra* note 76 (Robert Davidson, partner at a criminal law firm, online: <https://www.davidsongregory.com>). Legal Aid: *Hiscoe NSPC*, *supra* note 75 (Stephen Mattson, QC, online: <https://www.lawyerscanada.net/stephen-mattson/>); *Howell*, *supra* note 76 (Matthew Darrah, online: <https://www.lawyer.com/canada-matthew-darrah.html>). It is notable that the lawyers at the Supreme Court of Canada are not always the same lawyers as those responsible for establishing the trial record.

[205] All of the lawyers running the cases concerning the constitutionality of retrieving ISP subscriber information without a warrant were private counsel. See *Ward ONCJ*, *supra* note 102 (Vanora Simpson, online: <https://www.linkedin.com/in/vanora-simpson-351a9a18/>); *Friers*, *supra* note 102 (the lawyer for the accused, Geoffrey Read, has only minimal presence online but appears to run a solo practice); *Spencer SKQB*, *supra* note 102 (Mark Brayford and Professor Glen Luther); *Trapp SKPC*, *supra* note 102 (Ronald Piche, online: <https://www.linkedin.com/in/ron-piché-73b9596a/>); *Wilson*, *supra* note 102 (Ron Ellis, online: <https://ronellislaw.com>); *McNeice*, *supra* note 102 (Michael Ng, online: <https://www.linkedin.com/in/michael-ng-b3a67b13/>); *Brousseau*, *supra* note 102 (Richard Fedorowicz, online: <https://www.linkedin.com/in/richard-fedorowicz-96598b105/>); *Kwok*, *supra* note 102 (Richard Posner, online: <https://www.linkedin.com/in/richard-posner-4443687a/>); *Cuttell*, *supra* note 102 (Jill Presser, online: <https://www.linkedin.com/in/jill-presser-79918b36/>). I left out *Smith*, *supra* note 102 as I could not track down who he retained as counsel and *Re C.(S.)*, *supra* note 102 as there was no defendant in that case.

[206] See generally *Telus*, *supra* note 145. The Court in *Jones*, *supra* note 156, relied heavily on the *Telus* decision in determining the relevant facts.

[207] The *Telus*/*Jones* cases were based on more nuanced facts and a type of search (intercept) that is far less common. See *Telus*, *supra* note 145 at para 75.

appealed by defendants half the time,[208] those considering the constitutionality of warrantless acquisition of ISP subscriber information were appealed just over a quarter of the time.[209] Although many of the defendants hired private counsel, a private client may be stretching to pay a private retainer and therefore have no funds for appeals. Legal Aid may also deny a request to fund appeals given their limited resources. It is difficult to predict exactly which of these reasons were at play, but it is likely some combination thereof.

The fact that accused generally did not call expert testimony bolsters this view. The accused faces a difficult hurdle to prove that the police tactic at issue constituted a search and was highly invasive.[210] Yet, trial judges were only provided with an expert in digital technologies in one of the main cases ruling on the constitutionality of cell phone searches incident to arrest.[211] Although the Crown frequently called officers to explain the nature of investigations relating to ISP subscriber information,[212] accused generally did not provide experts to rebut any misconceptions or fill any gaps left by the Crown's witnesses.[213] This is problematic as the accused's counsel is relied upon to ask relevant questions of police witnesses which requires that counsel has the time to develop an intensive understanding of the relevant digital technologies. Moreover, there is no

---

[208] The cases that were not appealed were *Otchere-Badu*, *supra* note 204; *Finnikin*, *supra* note 204; *Dhillon*, *supra* note 76; *Young*, *supra* note 76; *Franko*, *supra* note 76; *Howell*, *supra* note 76; *Polius*, *supra* note 72 (though it is notable that *Polius* was well litigated as it had six reported trial level decisions).

[209] The four cases that were appealed included *Ward ONCA*, *supra* note 100; *Spencer SKCA*, *supra* note 104; *Trapp SKCA*, *supra* note 107; *R v McNeice*, 2013 BCCA 98, [2013] BCWLD 4244

[210] As seen in Part II, the Crown frequently would argue that digital technologies are no different from other physical items, and thus did not need special rules. Defence counsel therefore faced a tactical burden of providing evidence about the applicable digital technology to counter such assertions.

[211] In *Mann BCSC*, *supra* note 76 the court relied on expert evidence. It is notable, however, that the expert was called by the Crown. The courts in *Fearon ONCJ*, *supra* note 76, *Hiscoe NSPC*, *supra* note 75, *Liew*, *supra* note 46, *Polius*, *supra* note 72, *Mann*, *supra* note 76; *Dhillon* , *supra* note 76; *Young*, *supra* note 76; *Howell*, *supra* note 76; *Franko*, *supra* note 76; *Manley* ONCA, *supra* note 81, *Finnikin*, *supra* note 204; *Otchere-Badu*, *supra* note 204 did not rely on expert evidence.

[212] This would generally involve discussion of the investigation, which included steps taken to retrieve ISP subscriber information, not what IP addresses revealed. A good illustration is found in *Trapp SKCA*, *supra* note 107 at para 78.

[213] Only one out of the eleven accused *supra* note 102 called expert testimony. See *Ward ONCJ*, *supra* note 102. Again, it is likely that many accused are funded by legal aid or simply not of significant means to afford an expert. Legal aid does not fund appeals automatically. If a case is pushing the envelope on a constitutional issue, they often will not take the risk of funding the appeal, as it is not seen as a good use of public resources.

guarantee that a Crown witness will have put any thought into means to limit the invasiveness of searches. There is thus no guarantee that even an informed counsel will receive optimal evidence from a Crown witness.

As for the intercept cases, the fact that Telus laid a robust evidentiary record resulted in a clear understanding of the relevant digital technologies. Although the Court failed to address potential problems with the prospective/retrospective distinction, there is no indication that it did so due to a lack of evidence. It was simply unnecessary to decide the issue on the facts before the Court.[214] One might reasonably speculate, then, that resource availability has some impact on the quality of evidence submitted in digital privacy cases.

It was also clear that courts at times fundamentally misunderstood digital technologies. Several courts in the cell phone search incident to arrest context compared computers and smartphones to cupboards, briefcases, or address books.[215] Some judges also failed to recognize the fact that internet usage could be revealed by ISP subscriber information,[216] or at least thought this was of little importance.[217] This shows a misunderstanding of the privacy issues engaged by knowledge of a user's internet history, even if the history revealed is minute. The fact that these errors percolated in the lower courts until 2013/2014 should raise concern about judicial capacity to govern digital technologies.[218]

---

[214] See generally *Jones*, *supra* note 166.
[215] *Supra* note 76.
[216] *Supra* note 102. It is important to note, however, that most of the judges came to this conclusion because the ISP subscriber agreement was found to negate what was otherwise a reasonable expectation of privacy in ISP subscriber information due to the ability of that information when combined with an IP address being able to reveal an accused's internet activity.
[217] For instance, Justice Ottenbreit reasoned in *Spencer SKCA*, *supra* note 104 at para 110 that any potential to reveal internet browsing history was "neither here nor there".
[218] See generally *Vu*, *supra* note 18 where the first issue was corrected, and *Spencer*, *supra* note 18 where the second issue was rectified.

Finally, it is notable that the above jurisprudence rarely revealed instances where intervener submissions significantly updated the evidentiary record. Interveners participated in all the Supreme Court of Canada cases, but only sparsely at other levels.[219] Overall, each individual brief inadequately dealt with the relevant technological issues.[220] This is likely at least in part because

---

[219] Interventions on behalf of criminal defendants in the cases cited in Parts II(a) and (b) were sparse. ISP Subscriber Information Cases: *Ward* & *Cuttell* (The appeals were heard together. No intervener at trial but the Canadian Civil Liberties Association intervened at the Court of Appeal:); *Spencer* (not at trial or Court of Appeal but the Privacy Commissioner of Canada, Canadian Civil Liberties Association, and Criminal Lawyers' Association of Ontario intervened at the Supreme Court of Canada:); *Trapp* (not at trial or Court of Appeal); *Wilson* (not at trial); *Friers* (not at trial); *McNeice* (not at trial or Court of Appeal); *Brousseau* (not at trial); *Smith* (not at trial); *Re C.(S.)* (not at trial); *Kwok* (not at trial). Cell Phone Searches Incident to Arrest: *Manley* (not at trial or Court of Appeal); *Fearon* (not at trial but the Criminal Lawyers' Association and Canadian Civil Liberties Association intervened at the Court of Appeal and were joined by the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, British Columbia Civil Liberties Association, Criminal Trial Lawyers' Association [Alberta] at the Supreme Court); *Hiscoe* (not at trial or Court of Appeal); *Cater* (not at trial or Court of Appeal); *Liew* (not at trial or Court of Appeal); *Polius* (not at trial); *Finnikin* (not at trial); *R v Otchere-Badu* (not at trial); *Giles* (not at trial); *Mann* (not at trial but BCCLA on appeal); *Dhillon* (not at trial); *Young* (not at trial); *Howell* (not at trial); *Franko* (not at trial).

[220] Unless stated otherwise, the following factums were retrieved from the Supreme Court of Canada's website, online: <https://www.scc-csc.ca/case-dossier/info/search-recherche-eng.aspx?cas=35298>.

(1) Spencer: (a) *Privacy Commissioner*: The author generally observes in his brief analysis from of five paragraphs (17-21) that much can be revealed with an IP address. However, she does not provide much by way of an outline of how this occurs, or more importantly, how this may be limited as I discuss above; (b) *Ontario Crown*: In two paragraphs (9-10) categorically denies that anything can be revealed with such searches; (c) *Alberta Crown*: says nothing about the issues raised here; (d) *Federal Crown*: emphasizes "one moment of time" being revealed at paras 2, 27 without an explanation as to why this is so. The author also broadly rejects Westin's anonymity aspect of privacy extending to the internet. See paras 16-29. The analogies used do not engage in a meaningful way with the qualitative and quantitative differences between the digital and physical worlds outlined in *Vu*, *supra* note 18; (e) *Criminal Lawyers' Association of Ontario*: at para 2 rightly observes that IP address information can be used for such purposes. However, does not explain why it need not be used this way; (f) *Canadian Civil Liberties Association*: asserts without explaining that these searches allow for much to be discerned about internet activity (see para 5).

(2) Fearon (SCC): (a) *Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic*: notes at para 15 that "powering down a device or removing its battery (at least until officers return to the station) will typically address any risk of remote deletion of evidence hosted on the device itself" and observes that faraday bags can block transmissions. The technologies frailties as explained above are not discussed. At para 21 the author also erroneously says that data will be safe by merely seizing the device; (b) *Canadian Association of Chiefs of Police*: Asserts that evidence is is lost when deleted but does not describe forensic recovery (see para 24-25); (c) *Canadian Civil Liberties Association*: asserts in one paragraph that removing the battery or placing it in a Faraday bag would prevent loss of evidence (see para 19). Does not discuss frailties of these techniques; (d) *British Columbia Civil Liberties Association*: notes deleted texts can be recovered but appears to later suggest that messages can always be recovered (see paras 4, 24); (e) *Criminal Lawyers' Association*: argues that this is an "intercept" governed by Part VI; (f) *Director of Public Prosecutions*: draws a distinction between a manual and forensic search (see para 2). Although a manual search could not as effectively "troll" or "scan" the device, the distinction drawn ignores the vast amount of information that would still be found by conducting a manual search. The author does, however, correctly note that significant amounts of data after deleted will still be forensically recoverable (see para 16); (g) *Alberta Crown*: does not discuss technological capacity; (h) *Criminal Trial Lawyers' Association of Alberta*: argues that there are many ways to ensure phones cannot be remotely wiped but does not consider logic bombs or what happens to evidence stored on RAM (see para 11).

(3) Fearon (ONCA): the following were found via google: (a) *Canadian Civil Liberties Association*: They boldly assert at para 13 that "[o]nce seized, an electronic device poses no threat to police or public, and police can easily take steps to ensure that any potential evidence cannot be destroyed." Later the author briefly hints at the use of faraday

institutions that defend privacy, such as civil liberties associations, are not able to expend necessary resources due to their limited funding being divided between numerous civil rights issues.[221] It may also be attributed to restrictions on interveners, as their factums are generally limited to ten pages, and the time allotted for oral argument to fifteen minutes.[222] Even though interveners often raised relevant arguments, it was impossible with such restrictions to describe the technology in adequate detail, outline potential frailties in the evidentiary record, and respond to counter-arguments by opposing counsel.[223] Without such submissions, it is unreasonable to expect interveners to assist appellate courts in developing precise and coherent rules.

Conclusion

The review of Canadian digital privacy jurisprudence confirms that judges operating within the adversarial system have significant difficulties building adequate factual records and rendering timely decisions with respect to digital technologies. There are at least three reasons courts face these problems. First, there is evidence that criminal defendants do not have sufficient resources to call adequate evidence. Second, judicial comprehension of digital technologies at times causes judges to render misinformed decisions. Finally, traditional adjustments to the adversarial process such as calling experts or relying on intervener factums have proven unreliable in correcting factual records. Whether these constraints are more restrictive than those facing Parliament when enacting

bags and battery removal as options to prevent destruction of evidence; (b) *Criminal Lawyers' Association*: this factum could not be found.

[221] See Erin Murphy, "The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions" (2013) 111 Michigan Law Review 485 at 505-06.

[222] See *Rules of the Supreme Court of Canada*, SOR/2002-156, s 42(5)(a), s 42(5)(b). The factums cited *supra* note 220 are exemplary. It is notable, however, that there is limited discretion to increase the pages allotted to interveners. It is unclear how often this discretion is exercised.

[223] Battery removal and the operation of Faraday bags provide good examples. Contrast the discussion in the cell phone search intervener factums *supra* note 220 with the more detailed discussion in Part II(a) above.

digital privacy legislation requires in depth study of Parliament's legislative record, a study to which the next Chapter turns.

Chapter Three

Parliamentary Capacity to Govern Digital Privacy

Introduction

Although Canadian courts have experienced significant problems when creating rules to govern digital technologies, only limited scholarship has explored the relative institutional capacity of Canadian legislatures to create digital privacy rules.[1] These authors generally conclude that Parliament has risen to the challenge of governing privacy in the digital age.[2] Their conclusions, however, derive from Parliament's first few legislative responses to complex technological issues that arose from litigation under section 8 of the *Canadian Charter of Rights and Freedoms*.[3] As more difficult challenges have arisen since these initial legislative responses, more sustained study of Parliamentary capacity to respond to the unique challenges of governing digital privacy is necessary.

---

[1] Professor Steven Penney has addressed this question most extensively in his article "Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach" (2007) 97 Journal of Criminal Law and Criminology 477 at 503-05. See also Michal Fairburn, "Twenty-Five Years in Search of a Reasonable Approach" (2008) 40 Supreme Court Law Review 55; Daniel Scanlan, "Issues in Digital Evidence and Privacy: Enhanced Expectations of Privacy and Appellate Lag Times" (2012) 16 Canadian Criminal Law Review 301 at 311-12.

[2] *Ibid*.

[3] Part I of the *Constitution Act, 1982*, being schedule B to the Canada Act 1982 (UK), 1982, c11. The limited scholarship is outlined *supra* note 1.

In this Chapter, I contend that the initial academic optimism about the capacity of Parliament to address the unique challenges of governing digital privacy was unwarranted. Parliament often passes digital privacy laws which are broad and indeterminate, leaving it to the courts to develop a framework for governing digital privacy intrusions. When Parliament enacts laws tailored to address a narrow aspect of digital privacy, these laws often become stagnant and/or incoherent. As courts are struggling to create informed rules within the adversarial framework, either Parliament must devote significantly more resources to updating its legislation in an efficient and coherent manner, or it must provide courts with better tools to decide issues relating to complex technologies.

The Chapter is divided into three parts. In Part I, I outline my methodology for exploring the institutional capacity of legislatures to govern digital privacy vis-à-vis courts. In Part II, I then critically review Parliament's legislation governing complex and rapidly-shifting technologies. I do so by asking whether its legislation tends to respond quickly to technological change, does so coherently, and without undue influence. I conclude that Parliament has similar difficulties enacting efficient and coherent digital privacy rules as its American counterpart,[4] although concerns relating to lobbyist and majoritarian influence are significantly attenuated.

I. Methodology

Although my study primarily focuses on Parliament's legislative responses to digital technologies, other complex and rapidly developing technologies raise similar governance concerns and therefore will also be appropriate objects of study.[5] As I explain in Part II, Parliament's legislative responses to novel technologies have been piecemeal over the last several

[4] See the review discussed in Chapter 1.
[5] Parliament's first response to radio-based communications devices is one of several examples discussed below in Part II.

decades. This time-period—beginning from the mid-1970s to the present—provides ample opportunity to test Parliamentary capacity to respond to digital privacy concerns.

My aim is to answer three central questions. First, I ask whether Parliament has reacted efficiently relative to technological change. As observed in Chapter Two, this is one of the main weaknesses of allowing courts to create rules with respect to digital technologies. Judges operating within the adversarial system cannot address issues until criminals or police start using a technology in a legally relevant way.[6] Even after a technology appears in the courts, the appeals process will delay confirmation of any rule rendered at trial.[7] This delay makes judicial rules highly susceptible to being rendered redundant by advances in technology. If Parliament reacts no more quickly than courts, this consideration will hold little sway in determining who is better capable of governing digital privacy.

Second, I will assess whether Parliament's responses have led to incoherent or unintended results. As seen in Chapter Two, this is also a main critique of allowing courts to govern digital technologies. Courts not only face time constraints when rendering decisions, they are also limited to consideration of the evidence submitted at trial. As the adversarial system tends to provide inadequate evidence of the operation of digital technologies, courts are prone to render decisions without vital information.[8] If Parliament does not receive adequate evidence, conducts insufficient study, or passes laws in haste, it is likely that oversights and errors will also be found in its statutory schemes. If true, its relative institutional competence will be undermined.

---

[6] See Scanlan, "Issues", *supra* note 1 at 312 ("[w]hen the subject of the decision is technology, the time between when the technology first appears, some criminal use is made of it, police investigations occur, trials are held, and appeals are heard can be many years. When dealing with a relatively stable technology like DNA analysis, no harm occurs. When the process occurs in relation to a specific digital technology or software, the result may well be an appellate pronouncement of historical interest only").

[7] *Ibid*. See also Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution" (2004) 102 Michigan Law Review 801 at 868-69.

[8] See Kerr, "Fourth Amendment", *supra* note 7 at 875-76.

Finally, it is necessary to ask whether Parliament is subject to undue influence by special interest groups or ignores privacy interests to appeal to majoritarian bias. This is an important question in the context of search and seizure law, as prominent academics have questioned whether such concerns arise at all in the criminal law context.[9] Even if these concerns do arise, scholars query whether they apply to novel search technologies, which some claim are disproportionately owned by classes that have few encounters with the criminal law.[10] If these predictions prove incorrect, and Parliament is unduly influenced, the independence brought by courts will weigh heavily in favour of tailoring better judicial responses to governing digital privacy.

I undertake the latter inquiry with the aid of two theoretical lenses. The first, majoritarianism, posits that the democratic process will frequently result in laws which favour majority interests at the expense of minority groups.[11] As John Hart Ely explained, "a majority with untrammeled power to set governmental policy is in a position to deal itself benefits at the expense of the remaining minority even when there is no relevant difference between the two groups."[12] As the criminal law provides a means for majorities to perpetuate existing social inequality,[13] it is necessary to consider whether police powers to search digital devices are undermining vulnerable parties' interests.

---

[9] *Ibid* at 885-87. Kerr maintains that there is only "sparse" support for the argument that majorities impose their will on vulnerable minorities. Alternatively, even if such concerns arise in criminal procedure generally, Kerr contends that majoritarian concerns are unlikely to arise with respect to new technologies as such devices are predominantly owned by politically powerful groups.

[10] *Ibid*. See also Penney, "Reasonable Expectations", *supra* note 1 at 503-04.

[11] This rationale was famously articulated in footnote four of *United States v Carolene Products Company*, 304 US 144 (1938). Justice Stone, although refusing to continue strictly reviewing economic legislation, added footnote four to explain that strict scrutiny would still be used to assess the impact of state action on individual rights, especially where government regulations adversely affect "discrete and insular minorities".

[12] John Hart Ely, *Democracy and Distrust* (Cambridge: Harvard University Press, 1980) at 7.

[13] As Kent Roach observes, "[p]eople accused of crime are emblematic of the powerless, the unpopular, and the disenfranchised." See Kent Roach, "Dialogue or Defiance: Legislative Reversals of Supreme Court Decisions in Canada and the United States" (2006) 4 International Journal of Constitutional Law 347 at 351 citing Ely, *Democracy*, *supra* note 12; Donald Dripps, "Constitutional Theory for Criminal Procedure: *Dickerson*, *Miranda*, and the Continuing Quest for Broad-but-Shallow" (2001) 43 William and Mary Law Review 1. See also Kent Roach, *The Supreme Court on Trial: Judicial Activism or Democratic Dialogue* (Toronto: Irwin Law, 2001).

The second theoretical lens is public choice theory. It applies micro-economic theory to political decision making. Its broad contribution illustrates how the rational actor model applies to political actors.[14] Public choice theorists reject the assumption that political actors always act in the public interest and seek to explain political behaviour by viewing political actors as "egoistic, rational, utility maximizer[s]."[15] Public choice theory is frequently used to explain inaction[16] and anomalous action (often caused by lobbyist influence)[17] by legislatures. Applying these theoretical frameworks will allow for a more focused conclusion concerning why Parliament reacts in the manner it does with respect to complex search technologies.

II. Parliament's Legislative Responses

To assess Parliament's ability to govern digital privacy, I divide my analysis into three sections. The first considers whether Parliament responds quickly to a technology which arises in the jurisprudence or is widely used by the public. Whether the response was intelligible or had significant gaps will be the subject of the second inquiry. The third inquiry assesses whether majoritarian or public choice concerns arise when Parliament passes digital privacy laws. I offer institutional explanations for Parliament's successes and failures at each interval.

(a) Speed of Response

[14] See generally Philip Frickey and Daniel Farber, *Law and Public Choice: A Critical Introduction* (Chicago: University of Chicago Press, 1992).
[15] See Denis Mueller, *Public Choice III* (Cambridge: Cambridge University Press, 2003) at 1-2.
[16] As Anthony Downs explains in *An Economic Theory of Democracy* (New York: Harper, 1957), the limited resources citizens possess to investigate complex political issues results in few issues defining an election. As a result, even extreme instances of privacy infringements (e.g. Snowden) have failed to significantly impact elections. Other more common privacy infringements—such as corporate collection and dissemination of data—rarely constitutes more than a nuisance, again making these issues relatively unimportant. As such, it is often (but certainly not always) the case that political actors do not make privacy protections a major election issue. See also David Mayhew, *Congress: The Electoral Connection* (New Haven: Yale University Press, 1974) and Neil Komesar, *Imperfect Alternatives: Choosing Institutions in Law, Economics, and Public Policy* (Chicago: University of Chicago Press, 1994) at 56.
[17] See Erin Murphy, "The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions" (2013) 111 Michigan Law Review 485 at 504; Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books, 2006) at 323.

The adoption of the *Charter* resulted in a series of assertive decisions interpreting the scope of section 8 of the *Charter*. Perhaps unsurprisingly, Parliament's response to novel technologies was somewhat lagging in the first decade, as it also had to respond to a plethora of other *Charter* decisions. Despite the challenge of responding to the judicial interpretation of a new bill of rights, Parliament initially reacted quickly to fill gaps in the law on several occasions. In later years, however, institutional limitations prevented timely, or even any, legislative response.

(i) 1974-1993

Before the *Protection of Privacy Act*[18] introduced what is now Part VI of the *Criminal Code*,[19] electronic surveillance was largely unregulated in Canada.[20] By passing the *PPA* in 1974, Parliament followed in the footsteps of the United States and provided a comprehensive scheme for governing interceptions of private communications.[21] It defined "private communications" as "any oral communication or any telecommunication made under circumstances in which it is reasonable for the originator thereof to expect that it will not be intercepted by any person other than the person intended by the originator thereof to receive it."[22] The original scope of Part VI therefore applied only to telephone wiretaps and other audio intercepts.[23] However, with the onset of communications technologies, the limitations of Part VI's ability to respond to privacy and law enforcement concerns were repeatedly exposed.[24]

---

[18] SC 1973-74, c 50 [*PPA*].
[19] RSC 1985, c C-46.
[20] See Robert Hubbard, Peter Brauti, and Scott Fenton, *Wiretapping and other Electronic Surveillance: Law and Procedure*, looseleaf (Aurora: Canada Law Book Inc, 2005) at Chapters 12, 17.
[21] See the *Wiretap Act*, 18 US Code §§ 2510-22 (1968). This legislation will be discussed in significant detail in the next Chapter.
[22] See section 183 of the *Criminal Code*. It is notable that the definition "telecommunication" derives from the *Interpretation Act*, RSC 1985, c I-21, s 35(1) ("'telecommunications' means the emission, transmission or reception of signs, signals, writing, images, sounds or intelligence of any nature by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system").
[23] *Ibid*.
[24] See Steven Penney, "Updating Canada's Communications Surveillance Laws: Privacy and Security in the Digital Age" (2008) 12 Canadian Criminal Law Review 115 at 121.

One of the first challenges posed to the scope of Part VI arose from its application to analog voice pagers.[25] These devices send recorded messages to a recipient which is then broadcast over the device's speaker.[26] At least two courts concluded that these technologies did not attract a "reasonable expectation of privacy" thereby foregoing the need for an intercept warrant.[27] Two reasons underpinned this conclusion. First, it was possible that a third party would overhear the recorded messages when played back on the pagers' speakers.[28] Second, it was also possible for third-party pagers to access recorded messages by tuning into the same frequency as the receiving party's receiver.[29] Despite the fact that the volume of a speaker may be controlled,[30] courts refused to recognize a reasonable expectation of privacy in the devices.

Similar difficulties arose from public use of cell phones.[31] The analog signals sent were unencrypted and available over publicly accessible parts of the radio spectrum, thereby giving rise to the question of whether they attracted a reasonable expectation of privacy.[32] In *R c Solomon*,[33] the Court concluded that no reasonable expectation of privacy existed for this reason. In *R v Cheung*,[34] the Court undertook a more detailed assessment of telephony. Because of the many frequencies and transmission towers from which information is transferred over wireless networks used by some phones,[35] the Court concluded that it would be rare to intercept any communications

---

[25] *Ibid* at 122.
[26] See *R v Nin* (1985), 34 CCC (3d) 89, 1985 CarswellQue 278 (Que CSP); *R v Lubovac* (1989), 101 AR 119, 52 CCC (3d) 551 (ABCA) leave to appeal refused [1989] SCCA No 463.
[27] *Ibid*. Before the *Charter*, the "reasonable expectation of privacy" test was synonymous with "private communication."
[28] *Ibid*.
[29] See *Lubovac*, *supra* note 26 at 558-59.
[30] See Penney, "Updating", *supra* note 24 at 122 citing Hubbard, Brauti, and Fenton, *Wiretapping*, *supra* note 20 at para 6.5.3.
[31] See Penney, "Updating", *supra* note 24 at 122-23.
[32] *Ibid*.
[33] (1992), 77 CCC (3d) 264, 16 CR (4th) 193 (QC Mun Crt).
[34] 100 CCC (3d) 441, 1995 CarswellBC627 (BCSC).
[35] The different types of phones will be discussed in the section discussing coherence of Parliament's response.

from these mobile phones.[36] As a result, the Court found the user's expectation of privacy to be reasonable.[37]

In the late 1980s, a further issue arose with respect to whether the consent of one party to covertly record a conversation expunged the other party's reasonable expectation of privacy. As this issue was not covered by Part VI, the police could only rely upon the evidence obtained if the accused's expectation of privacy was unreasonable.[38] As the consenting party could repeat the words to the police or in court, there was a basis to conclude that the accused gave up any reasonable expectation of privacy.[39] In *R v Duarte*,[40] the Court rejected this argument. As Justice La Forest wrote, "[a] society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning."[41] Given the "wholly unacceptable" danger to privacy brought on by such new technologies, the Court concluded that prior judicial authorization was required.[42]

Shortly after *Duarte*, the Court in *R v Wong*[43] considered whether Part VI applied to video recordings. As outlined above, Part VI only covered oral or voice communications when it was first enacted. It therefore did not apply to non-audio-based video recordings. A few years earlier, the Law Reform Commission of Canada had explicitly concluded that this gap in the legislation would not lead to "unjustifiable privacy intrusions."[44] As a result, the police had taken advantage of this loophole and planted a non-audio-equipped video camera in the accused's hotel room. The

---

[36] See *Cheung*, *supra* note 34 at paras 12-15.
[37] *Ibid*.
[38] It would not be a "search" for constitutional purposes. See *R v Collins*, [1987] 1 SCR 265, 38 DLR (4th) 508.
[39] This was in fact the conclusion of the United States Supreme Court in *Lopez v United States*, 373 US 427 (1963).
[40] [1990] 1 SCR 30, 71 OR (2d) 575.
[41] *Ibid* at 11.
[42] *Ibid* at 13-14.
[43] [1990] 3 SCR 36, 120 NR 34.
[44] See Law Reform Commission of Canada, *Electronic Surveillance*, Working Paper No 47 (Ottawa: 1986) at 21.

Court ultimately found a breach of section 8 of the *Charter* as the accused had a reasonable expectation of privacy in his hotel room.[45] As Part VI did not provide for a warrant power, it was again unable to serve legitimate law enforcement interests.

Around the time *Duarte* and *Wong* were decided, courts were also considering the legality of using digital number recorders to record outgoing and incoming calls being dialled from a phone.[46] In *R v Fegan*,[47] the Ontario Court of Appeal found that no warrant was required to use digital number recorders because the service provider was not acting on behalf of the state. Had such activity occurred at the behest of the state, preauthorization would have been required.[48] This conclusion derived from the then-recent decision in *R v Wise*,[49] where the Court considered whether police installation of a tracking device on a motor vehicle required prior judicial authorization. Even though the "beeper" device at issue was unsophisticated,[50] the Court found that its use infringed the occupant's reasonable expectation of privacy. If such a minimal infringement required pre-authorization, then it was likely (contrary to an earlier appellate

[45] *Ibid*.
[46] The Quebec and Ontario Courts of Appeal have both described digital number recorders as follows: "[a] digital number recorder (DNR) is activated when the subscriber's telephone is taken 'off the hook'. Electronic impulses emitted from the monitored telephone are recorded on a computer printout tape which discloses the telephone number dialled when an outgoing call is placed. The DNR does not record whether the receiving telephone was answered nor the fact or substance of the conversation, if any, which then ensues. When an incoming call is made to the monitored telephone, the DNR records only that the monitored telephone is 'off the hook' when answered and the length of time during which the monitored telephone is in that position." See *R v Cody*, 2007 QCCA 1276 at para 11, 228 CCC (3d) 331 and *R v Fegan* (1993), 13 OR (3d) 88 at 363-64, 80 CCC (3d) 356 (ONCA). DNRs replaced their analog equivalents known as pen registers and trap and trace devices. The former recorded outgoing phone calls dialled on a landline telephone, while the latter captures incoming calls to a specific number.
[47] *Supra* note 46.
[48] *Ibid*. See also *R v Griffith* (1988), 44 CCC (3d) 63, 49 CRR 323 (Ont Dist Crt); *R v Khiamal* (1990), 83 Alta LR (2d) 359, 106 AR 246 (ABQB).
[49] [1992] 1 SCR 527, 70 CCC (3d) 193.
[50] *Ibid*. The device was a low power radio transmitter that could provide a general location for the thing being tracked.

opinion)[51] that a digital number recorder would also require pre-authorization.[52] As the *Criminal Code* provided neither powers, such searches violated section 8 of the *Charter*.[53]

Parliament addressed many of these concerns in 1993 with Bill C-109.[54] To address the inapplicability of Part VI to wireless phone communications, Parliament amended the definition of "private communication". It did so by including within that definition any "radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it."[55] This ensured that *some* wireless telephone communications would require the state to meet the higher requirements for a Part VI intercept warrant.[56]

Parliament's enactment of section 184.2 of the *Criminal Code* further provided a warrant provision to allow for consensual intercepts of communications. This addressed the concerns raised in *Duarte*. In addition, Parliament enacted provisions which permitted warrantless interceptions where bodily or imminent harm is reasonably foreseeable.[57] Although the requirements now found in section 184.2 do not provide the added protections of other Part VI warrants,[58] the courts have found the lower standard to be constitutional as the third-party privacy concerns raised by traditional intercepts are not engaged.[59] As Justice Watt observed in *R v*

---

[51] See *R v Samson* (1983), 45 Nfld & PEIR 32, 132 APR 32 (Nfld CA).
[52] See the last two paragraphs in *Fegan*, *supra* note 46.
[53] For a search to be reasonable under section 8 of the *Charter*, it must be "authorized by law". See *Collins*, *supra* note 38 at 278. No law authorized the technique used in either *Fegan* or *Wise*.
[54] See *An Act to amend the Criminal Code, the Crown Liability and Proceedings Act and the Radiocommunication Act (Bill C-109)*, 1993, c 40.
[55] See Penney, "Updating", *supra* note 24 at 123-24. Parliament also explicitly subjected wireless telecommunications to the wiretap warrant procedures. See sections 184.5 and 184.6 of the *Criminal Code*.
[56] I explain under the coherence of response section below why the amendments were not comprehensive.
[57] See sections 184.1 and 184.4.
[58] Most notable is the absence of an investigative necessity requirement. For additional requirements, see section 487.01(5). For a review of the investigative necessity requirement, see *R v Araujo*, 2000 SCC 65 at para 29, [2000] 2 SCR 292.
[59] Constitutional challenges to section 184.2 have been unsuccessful. See *R c Bordage*, 146 CCC (3d) 549, [2000] JQ No 2045 (QBCA); *R v Largie*, 2010 ONCA 548, 101 OR (3d) 561 leave to appeal refused [2010] SCCA No 460.

Largie,[60] "[p]articipant surveillance is generally more focused than third-party surveillance, targeting specific conversations with specific individuals."[61] This not only makes capture of third-party communicants less likely, the state agent's control over the conversation also reduces the risk of accidentally receiving irrelevant but private information.[62]

To address the gap revealed in *Wong*, Parliament enacted the general warrant provision under section 487.01. This broad provision provided a means for police to seek a warrant where no other legislative enactment provided a suitable power. It also specifically included sections 487.01(4) and (5) which applies Part VI requirements to any observation "by means of a television camera or other similar electronic device" of "any person who is engaged in activity in circumstances in which the person has a reasonable expectation of privacy."[63] Thus, Parliament not only provided police with a means to lawfully conduct non-audio-based video recordings, it also gave police a provision to apply for search warrants where no specific *Criminal Code* provision applied.

Finally, in response to *Wise* and *Fegan*, Parliament enacted sections 492.1 and 492.2 of the *Criminal Code*. The former allowed tracking warrants to issue if the police had reasonable grounds to suspect an offence had been or would be committed and that information relevant to the offence could be obtained by using a tracking device. The latter allowed for the use of digital number recorders if police had reasonable grounds to suspect information related to an accused's telephone calls would aid in an investigation. This lower standard of reasonable suspicion was borrowed from the Court's decision in *Wise* where it concluded that any Parliamentary response could allow

[60] *Supra* note 59.
[61] *Ibid* at para 56.
[62] *Ibid*.
[63] See section 487.01(4).

for authorization on a lower standard given the lower privacy interests inherent in the information revealed by some searches.[64]

(ii) 1994-1997

The next Parliamentary response to digital privacy was less comprehensive, but no less important as it updated the main warrant powers under section 487 of the *Criminal Code*. This provision's scope extended only to "things" found in buildings, places, or receptacles. The problem raised by digital technologies was aptly queried by Susan Magotiaux:

> Is a computer a thing? Is the data on it a thing? Is the string of binary code sent through satellites in pieces and reassembled at some other machine a thing? Is it the same 'thing' when it lands as it is when it travels in pieces? And what of the places? Police can't knock and announce their presence at the door of satellites and clouds and mobile servers. Yet without particularity of place, current tools may be unavailable.[65]

To ensure police could seek warrants for digital "things", Parliament added subsections 487 (2.1) and (2.2) to the *Criminal Code* to ensure police may apply to access and use computer systems found in the place of a search.[66] These broad provisions provide that a police officer may "use or cause to be used any computer system at the building or place to search any data contained in or available to the computer system."

(iii) 1998-2013

During this period, Parliament passed what would be its first production order scheme.[67] Production orders allow police to compel third parties who are not under investigation for any offence to produce data or documents that may be relevant to the commission of an offence by another person.[68] The impetus to pass this scheme arose from Canada's 2001 signing of the Council

---

[64] See *Wise*, *supra* note 49 at 229.
[65] See Susan Magotiaux, "Out of Sync: Section 8 and Technological Advancements in Supreme Court Jurisprudence" (2015) 71 Supreme Court Law Review 501 at 510. See also James Fontana and David Keeshan, *The Law of Search & Seizure in Canada*, 8th ed (Markham: Lexis Nexis, 2010) at 1181-82.
[66] *Ibid*.
[67] See Bill C-13, *An Act to amend the Criminal Code (capital markets fraud and evidence gathering)*, SC, 2004, c 3.
[68] See Fontana and Keeshan, *Search and Seizure*, *supra* note 65 at 494.

of Europe's *Convention on Cybercrime*.[69] The Convention requires that all signatories criminalize certain offences commonly committed on computers and improve investigative techniques for detecting online crime. By so doing, the signatories aimed to facilitate increased cooperation between countries investigating cybercrime.[70]

Parliament furthered these goals by providing police with two types of production orders: a general production order issuable on reasonable grounds to believe an offence occurred and a specific order relating to financial or commercial data issuable on reasonable suspicion.[71] Subsequent attempts in 2005,[72] 2009,[73] 2010,[74] and 2012[75] to bring in more narrowly tailored production orders,[76] as well as provide a variety of other police powers necessary to ratify the Cybercrime Convention,[77] were unsuccessful. The Conservative government either received limited opposition party support when in a minority position, an election was called causing the

[69] Council of Europe, "Details of Treaty No 185: Convention on Cybercrime", ETS No 185 (23 November 2001), online: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>. Canada signed the Treaty on 23 November 2001.
[70] *Ibid*.
[71] See previous sections 487.011-017. The difference between the two standards was described by the Court in *R v Chehil*, 2013 SCC 49 at para 27, [2013] 3 SCR 220 ("while reasonable grounds to suspect and reasonable and probable grounds to believe are similar in that they both must be grounded in objective facts, reasonable suspicion is a lower standard, as it engages the reasonable possibility, rather than probability, of crime").
[72] Bill C-74, "An Act regulating telecommunications facilities to facilitate the lawful interception of information transmitted by means of those facilities and respecting the provision of telecommunications subscriber information", 1st Sess, 38th Parl, 2005.
[73] Bill C-46, "An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act", 40th Parl, 2nd Sess, 2009; Bill C-47, "An Act regulating telecommunications facilities to support investigations", 40th Parl, 2nd Sess, 2009.
[74] Bill C-50, "An Act to amend the Criminal Code (interception of private communications and related warrants and orders)", 40th Parl, 3rd Sess, 2010; Bill C-51, "An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act", 40th Parl, 3rd Sess, 2010; and Bill C-52, "An Act regulating telecommunications facilities to support investigations", 40th Parl, 3rd Sess, 2010.
[75] Bill C-30, "An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts", 41st Parl, 1st Sess, 2012.
[76] Most notably was a production order to allow police to demand ISP service providers provide internet subscriber information to police.
[77] *Supra* note 69. The police powers passed by Parliament discussed in the next subsection were required to ratify the Convention.

proposals to die on the order table, or, as discussed in detail below, public backlash caused government to retract its proposal.[78]

Parliament also made one further amendment to the intercept provisions of the *Criminal Code* during this period.[79] This amendment was in direct response to the Supreme Court of Canada's decision in *R v Tse*.[80] Although the Court concluded that allowing police to intercept communications without prior authorization in exigent circumstances was constitutional, the absence of a requirement to notify the subject of the interception that an intercept had been conducted was found to violate the *Charter*.[81] Parliament responded quickly by providing such a requirement.[82]

In addition to the above amendments, Parliament also created a variety of new criminal offence provisions or amended old ones. As computer technologies became more prevalent, the way in which a diverse number of crimes were committed was fundamentally transformed.[83] Unfortunately, the wording of many criminal offences did not capture acts committed with computer technologies, while other offences now prevalent in the digital age had not received any criminal prohibition. Parliament spent much of this period attempting to fill these legislative gaps.

Parliament's main concern was the sexual exploitation of minors. Digital technologies provided new and difficult to trace means of possessing and distributing child pornography.[84] The

---

[78] See Part II (c).
[79] Section 183 was "consequentially amended" in Bill C-19, 2000, c 24. An exemption for intercepting private communication was established in now section 184(3) in Bill C-14, 2004, c 12; section 186 received the following addition: "(5.1) For greater certainty, an authorization that permits interception by means of an electro-magnetic, acoustic, mechanical or other device includes the authority to install, maintain or remove the device covertly."
[80] 2012 SCC 16, [2012] 1 SCR 531.
[81] *Ibid*.
[82] See *Response to the Supreme Court of Canada Decision in R. v. Tse Act*, SC 2013, c. 8.
[83] See James Fontana and David Keeshan, *The Law of Search & Seizure in Canada*, 9th ed (Toronto: Lexis Nexis, 2015) at 782 citing offences such as "fraud, money-laundering, distribution of child pornography, invasion of privacy, and production of counterfeit cheques, identification and bills of exchange", as well as other nefarious uses of computers.
[84] *Ibid* at 779.

typical means of "possession" in the physical sense applied to those who downloaded child pornography.[85] However, whether accessing an image on an internet website constituted "possessing" the data provided conceptual difficulties.[86] Although evidence stored in the cache *may* provide sufficient evidence of knowledge and control, these core elements of possession will often be difficult to prove with such evidence.[87] Equally concerning, the definition of distributing child pornography did not extend to digital means of distribution, which had become increasingly common at the turn of the century.[88]

In response to these issues, Parliament enacted Bill C-15A in 2002.[89] This Bill created the "accessing" child pornography offence now found in section 163.1(4.1) and (4.2) of the *Criminal Code*.[90] Parliament's purpose in so doing was to "capture those who intentionally view child pornography on the net but where the legal notion of possession may be problematic."[91] Bill C-15A also amended the distribution of child pornography offence found in section 163.1(3) to include "transmission" and "making available" within the scope of the offence. This had the effect of ensuring that the "offence extends to distribution of child pornography in electronic form on the Internet by such means as e-mail and posting items to websites."[92] Parliament further passed section 164.1 which allowed for courts to order the removal and destruction of child pornography on the internet.[93]

---

[85] See *R v Morelli*, 2010 SCC 8, [2010] 1 SCR 253.
[86] *Ibid* at paras 34-37. See also *R v Weir*, 2001 ABCA 2001 at paras 22-24, 281 AR 333; *R v Daniels*, 2004 NLCA 73 at paras 11-12, 242 Nfld & PEIR 290; *R v Panko*, 52 CR (6th) 378 at paras 57-72, [2007] OJ No 3826 rev'd 2010 ONCA 660, 276 OAC 49.
[87] See *Morelli*, *supra* note 85 at paras 34-37.
[88] *Ibid*.
[89] Bill C-15A, *An Act to Amend the Criminal Code and to Amend Other Acts*, 2002, c 13.
[90] *Ibid*, s 5.
[91] See "Bill C-15A, An Act to amend the Criminal Code and to amend other Acts", *House of Commons Debates*, 37th Parl, 1st Sess, No 137 (3 May 2001) at 3581.
[92] David Goetz and Gérald Lafrenière, "Legislative History of Bill C-15A" (30 September 2002), online: <http://publications.gc.ca/Collection-R/LoPBdP/LS/371/371c15a-e.htm>. This Bill also permitted courts to order the destruction of online child pornography. See Bill C-15A, *supra* note 84, s 7.
[93] Bill C-15A, *supra* note 89, s 7.

Bill C-15A further provided an offence for child luring via a "telecommunication".[94] The internet made such a practice much more prevalent, and as such received prohibition tailored at digital commission of such crimes.[95] Similarly, voyeurism offences had become increasingly prevalent with increased technological capacity. Parliament responded with a specific prohibition against recording people in private circumstances.[96] These and the child pornography provisions would not require any further substantive amendments during this time period.

Parliament also brought several other less common offences up to date. For instance, the illegal gambling provisions in section 202(1)(j) were amended in 2008 to include digital means for promoting or facilitating betting.[97] Section 342.01 was amended to include copying of "credit card data" as opposed to prohibiting only "forging or falsifying" credit cards, as the latter definition did not apply to the mere possession or use of a credit card's data.[98] Finally, Parliament provided a criminal prohibition for using recording technology (i.e. small cameras) to record private productions such as movies on display in a theatre.[99]

(v) 2014-Present

The advent of email and text messaging posed novel challenges for Part VI intercepts. Under section 183, "intercept" includes "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof." As discussed in Chapter Two, courts and academics debated whether inclusion of the word "acquire" made it necessary to apply for a Part VI warrant

---

[94] *Ibid*, s 8. "Telecommunication" is defined as an "emission, transmission or reception" of communicative content "by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system".
[95] See section 172.1 of the *Criminal Code*.
[96] See Bill C-2, *An Act to Amend the Criminal Code and the Make Consequential Amendments to Other Acts*, 2005, c 32, s 6, which enacted the current section 162 prohibition.
[97] See Bill C-13, *An Act to Amend the Criminal Code (criminal procedure, language of the accused, sentencing and other amendments)*, 2008, c 18. The previous version of the offence applied only to "radio, telegraph, telephone, mail or express" forms of information transmission.
[98] See Bill C-27, *An Act to amend the Criminal Code (identity theft and related misconduct)*, SC, 2009, c 28.
[99] See Bill C-59, *An Act to amend the Criminal Code (unauthorized recording of a movie)*, SC, 2007, c 28. The offence now exists under section 432 of the *Criminal Code*.

to access retrospective email and text messages. Although this issue is now (mostly) settled,[100] it is notable that Parliament failed to update its legislation despite these ambiguities being known to the federal government for well over a decade.[101]

The use of peer-to-peer file sharing networks in the context of child pornography investigations also provided difficulties for police investigations. As discussed in Chapter Two, the accused in *R v Spencer*[102] successfully argued that he had a reasonable expectation of privacy in his subscriber information.[103] The Court therefore concluded that state requests for ISP subscriber information qualify as a search under section 8 of the *Charter*, thereby requiring lawful authority to conduct the search. Despite frequent calls from police to provide a legislative response to *Spencer*, Parliament has remained silent.[104]

The Court was also presented with the issue of whether searching cell phones incident to arrest is constitutional.[105] This issue has especially important implications for digital privacy as searches incident to arrest occur approximately forty times more often than warranted searches.[106] As seen in Chapter Two, the Court's decision to allow warrantless searches incident to arrest of cell phones was controversial.[107] Anticipating its institutional shortcomings to develop a

---

[100] See the discussion in Chapter Two with respect to *R v Telus Communications Co*., 2013 SCC 16, [2013] 2 SCR 3; *R v Jones*, 2017 SCC 60, [2017] 2 SCR 696.

[101] See Dominique Valiquet, "Bill C-74: Modernization of Investigative Techniques Act: Backgrounder" (21 December 2005), online: <https://lop.parl.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?lang=F&ls=c74&Parl=38&Ses=1&source=library_prb> at D(5).

[102] 2014 SCC 43, [2014] 2 SCR 212.

[103] *Ibid* at para 51.

[104] See Patricia Joseph, "A TheCourt.ca Exclusive Interview: R v Spencer One Year Later" *TheCourt.ca* (24 September 2015), online: <http://www.thecourt.ca/a-thecourt-ca-exclusive-interview-r-v-spencer-one-year-later/>. Although production orders are available for acquiring such information, the significant resources it takes to apply and acquire such an order has had negative effects on law enforcement's ability to prosecute digital crimes, most notably child pornography offences. See the discussion on this point in Chapter Two.

[105] See *R v Fearon*, 2014 SCC 77, [2014] 3 SCR 621.

[106] See Don Stuart, *Charter Justice in Canadian Criminal Law*, 6th ed (Toronto: Carswell, 2014) at 283.

[107] See the discussion in Part II(a) of Chapter Two.

comprehensive rule, the majority invited Parliament to pass legislation governing when police may conduct such searches.[108] This invitation has so far received no response.

The intrusiveness of tracking warrants had also been affected by technological change. Tracking warrants are frequently attached to things, such as vehicles, but now are also available to monitor mobile devices frequently carried on the person. The ability to track a person's precise location with Global Positioning System (GPS) technology as opposed to the unsophisticated methods at issue in *Wise* raise significantly more serious threats to privacy. It was therefore questionable whether tracking a person based on "reasonable suspicion" still struck an appropriate balance between privacy and law enforcement interests.[109]

The utility of digital number recorders was also impacted by technological developments. Section 492.2 originally conferred that a "number recorder" was "any device that could be used to record or identify the telephone number or location of the telephone from which a telephone call originates, or at which it is received or is intended to be received".[110] As people now frequently communicate with other media such as email and text, it was necessary to create a broader framework for the capture of metadata with respect to such communications.[111] It was also unclear if the retrievable data under section 492.2 included the place at which the call was made and received. Arguably this would also be constitutional, but the legislation needed to explicitly allow for such a search.[112]

---

[108] See *Fearon*, *supra* note 105 at para 84.
[109] See *R v Grandison*, 2016 BCSC 1712, [2016] BCWLD 6850; *R v Brown*, 2014 ONSC 6323, [2014] OJ No 5314.
[110] See previous section 492.2.
[111] Although not a perfect analogy, metadata may be thought of as the data typically found on the outside of an unopened letter. Importantly, such information reveals nothing about the *content* of the letter. With respect to an email, for instance, such data includes the "to" and "from," time codes, and routing information, but excludes the subject line. See Orin Kerr, "Internet Surveillance Law After the USA Patriot Act: The Big Brother that Isn't" (2003) 97 Northwestern University Law Review 607 at 611.
[112] See Penney, "Updating", *supra* note 24 at 150-51.

Parliament addressed some of these concerns in 2014 with Bill C-13.[113] First, it passed legislation creating a more robust production/preservation order scheme.[114] Three main production orders were added, all issuable upon reasonable suspicion an offence has been or will be committed. Sections 487.015 and 487.016 were added to allow police to trace and have third parties produce "transmission data."[115] Transmission data is effectively metadata, that is, the contextual information surrounding a communication.[116] Acquiring such data allows police to trace the origin of any telecommunication.[117] Section 487.017 allows police to apply for "tracking data", being data that "relates to the location of a transaction, individual or thing." The amendments also provided police with the ability to compel third parties to preserve documents in their possession for a prescribed period. As such information is routinely destroyed—sometimes intentionally but often inadvertently—this provision was necessary to preserve evidence for crimes committed with digital technologies.[118]

Parliament further responded to concern over the constitutionality of tracking device warrants available under section 492.1 of the *Criminal Code* by raising the standard from reasonable suspicion to reasonable grounds to believe an offence has been committed when the device being tracked is commonly found on the person.[119] Parliament simultaneously updated the digital number recorder provision to include the broader term "transmission data."[120] This allowed

[113] Bill C-13, *Protecting Canadians from Online Crime Act*, SC 2014, c 31.
[114] *Ibid*.
[115] *Ibid*, s 20.
[116] Such "data about data" includes the time and duration of a communication, the device used, its number, and the numbers it called, and its location.
[117] See Julia Nicol and Dominique Valiquet, *Legislative Summary of Bill C-13: An Act to Amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act* (28 August 2014), online: <https://lop.parl.ca/Content/LOP/LegislativeSummaries/41/2/c13-e.pdf>.
[118] *Ibid* at 11. For instance, telecommunications companies frequently destroy communications information after a prescribed period.
[119] See Bill C-13, *supra* note 113.
[120] Defined in sections 492.2(6)(a-c).

police to obtain data indicating the origin and intended recipient of internet and text communications, not just telephone communications.[121] In so doing, the revised definition also clarified that location data during the transmission of a call may be obtained by police, a question left open by the previous provisions.[122] The fact that it took until 2014 to update these provisions is evidence of Parliament's difficulty keeping pace with digital technologies.

Finally, Bill C-13 updated the *Criminal Code* by providing an offence for what has come to be known as "cyberbullying".[123] A legislative gap arose because digital technologies made it easy for young persons to distribute sexually explicit photos of their peers. As charging youth with distribution of child pornography was too harsh a sanction,[124] Parliament passed section 162.1(1) of the *Criminal Code*. Although the section in many ways mirrored the existing child pornography offences, it provided prosecutors with more moderate sentencing options for prosecuting youth and young adults than the child pornography provisions.[125]

(v) Summary

Several conclusions may be drawn from the above review.[126] Parliament's first few responses to gaps or constitutional issues with its legislative framework governing complex technologies were relatively quick.[127] At the turn of the century, however, Parliament became much less efficient. Despite having undertaken to provide a comprehensive lawful access scheme

---

[121] See Fontana and Keeshan, *Search and Seizure*, *supra* note 65 at 563.
[122] See Penney, "Updating", *supra* note 24 at 149. The new section contains a broad reference to the "origin" of any transmission data. See section 492.2(6).
[123] This term refers to "the use of information and communication technologies to support deliberate, repeated and hostile behaviour by an individual or group that is intended to harm others." The term was coined in Bill Belsey, "Cyberbullying: A Real and Growing Threat" *ATA Magazine* (Fall 2007) 14 at 15.
[124] Section 163.1(3) proscribes a mandatory minimum penalty of one-year imprisonment.
[125] See Nicol and Valiquet, *Bill C-13*, *supra* note 117 at 4. It is also notable that section 164.1(1) provides for a warrant of seizure for such material to prevent further distribution on the internet.
[126] These conclusions are summarized in Appendix A.
[127] Parliament's initial response received some judicial praise. See *R v Backhouse* (2005), 194 CCC (3d) 1 at para 110, 28 CR (6th) 31 ("Parliament has moved quickly to fill in gaps in the legislative scheme of search and seizure to provide the police with the necessary tools to investigate crime while ensuring that the public and individual interests in privacy are adequately protected").

in 2001, Parliament's legislation was patchwork and slow. It did, however, manage to meet the requirements of the *Convention on Cybercrime* fourteen years after it adopted it.[128] In the interim, the Crown pursued drawn out litigation in the courts trying to find lawful access provisions where none existed.[129]

Disputes surrounding Part VI warrants fared no better as Parliament's refusal and/or inability to address the confusion surrounding the definition of "private communication" and "intercept" was ultimately left to the courts.[130] Although the digital number recorder warrant was eventually updated, the provision was inapplicable to many of the most common mediums of communication for over two decades. Other issues with significant digital privacy implications, such as searches of cell phones incident to arrest, legislation governing acquisition of ISP subscriber information, and guidelines for searching computers under subsections 487 (2.1) and (2.2), have so far received no response from Parliament.[131]

Parliament fared better in a domain where it could not rely on courts to fill in legislative gaps: defining offences. Several offences were modified in the early-to-mid-2000s to allow prosecution of new ways of committing crime brought on by digital technologies. Parliament's record with respect to updating offences, however, is not perfect. As Peter McKay observed, given the seriousness of the child pornography offence, the delay in updating these provisions was

---

[128] Government of Canada, "Canada Completes Ratification of Convention on Cybercrime" (8 July 2015), online: <https://www.canada.ca/en/news/archive/2015/07/canada-completes-ratification-convention-cybercrime.html>.

[129] See *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212 and its discussion of section 7(3) of the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*]. As discussed in Chapter Two, the Crown repeatedly argued that s 7(3)(c.1)(ii) of *PIPEDA* provided for such a power. However, whether this section provided actual authority to make the request was doubtful as it requires that the state actor identify its "lawful authority" for making the impugned request. The police were relying on the section as *the* authority to make the request. This reasoning was rightly found to be circular. See *Spencer*, *supra* note 129 at paras 62-63.

[130] See *Telus*, *supra* note 100; *Jones*, *supra* note 100.

[131] It is notable some authors believe that the reason there was less legislation from Parliament was because of the Court's proactive approach to governing privacy. See Steven Penney, Vincenzo Rondinelli, and James Stribopoulos, *Criminal Procedure in Canada* (Toronto: Lexis Nexis, 2018) at 224-25 (footnote 572). Although this may generally be true with other privacy laws, I see little evidence of this in the context of governing complex and rapidly shifting search technologies.

"virtually inexcusable".[132] The well-known practice of cyberbullying had also been an issue many years before Parliament passed its legislation. The legislative response was more than anything a reaction to high profile teenage suicides.[133] Moreover, other needed offences such as a criminal prohibition for accessing and stealing historical data has still not received criminal sanction.[134] Overall, although Parliament has responded reasonably quickly when updating offences, its record has blemishes.[135]

Any attempt at explaining Parliament's slow response time will to some extent be guess work. However, it is not unreasonable to at least partially explain significant delays by observing that Canadian governments are often (at least of late) in a minority position. This was the case from 2004-2011, a period where controversial privacy issues such as "lawful access" were repeatedly stifled.[136] A great deal more criminal law legislation governing digital privacy was passed in the previous and following years which witnessed Liberal and Conservative majority governments.

A majority government may nevertheless face significant restrictions in passing digital privacy laws. Before a federal bill becomes law, it must pass through many stages, including three readings in the House of Commons and approval by the Senate.[137] This says nothing about the preliminary process of proposing and drafting the bill, often done by assigning a legislative

---

[132] "Bill C-15A, An Act to Amend the Criminal Code and to Amend other Acts", *House of Commons Debates*, 37th Parl, 1st Sess, No 97 (18 October 2001) at paras 1520-25.
[133] The suicides of Rehtaeh Parsons and Amanda Todd were often cited in legislative debate and public discourse.
[134] As Penney, "Updating", *supra* note 24 at 137-43 explains, traditional crimes such as theft and mischief do not catch this conduct. Moreover, given the low likelihood of getting caught and sued, it is unlikely that this activity will be deterred. As such, it is necessary for the stigma of criminal conviction to raise deterrence to a sufficient level.
[135] This was found to result in an inability to bring charges in several cases. See "Bill C-46, An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act", *House of Commons* Debates, 40th Parl, 2nd Sess, No 100 (26 October 2009; 27 October 2009) at 1815-20.
[136] See notes 72-75, *supra*. I will discuss the lawful access experience in detail below.
[137] See House of Commons, "Legislative Process", Government of Canada, online: <https://www.ourcommons.ca/About/Compendium/LegislativeProcess/c_g_legislativeprocess-e.htm>.

committee to undertake the necessary research and writing to develop the bill.[138] If a bill does not make it through this onerous process by the end of a session of Parliament it will die on the order table.[139] Although the bill may be revived the following session, governments tend to see no more than two sessions before Parliament is dissolved for an election.[140] Several of the bills discussed above failed precisely for this reason.[141]

(b) Coherence of Response

The coherence of Parliament's responses to complex and rapidly advancing search technologies also illustrates its relative institutional capacity to govern digital privacy. As will be seen, both privacy advocates and law enforcement have identified significant deficiencies with Parliament's legislative responses. Many of the technological developments were not anticipated by Parliament. Other anomalous results arose from unclear legislative drafting which may be attributed to a failure to fully comprehend digital technologies. Still other responses relied on highly questionable determinations by Parliament that the technology at issue did not attract a reasonable expectation of privacy.

(i) Wireless Phones

Parliament's 1993 amendment to the definition of "private communication" ensured that all encrypted digital signals sent via wireless phones came within its ambit. However, the technologies used by different generations of cordless landline and mobile phones resulted in many then-current technologies falling outside of the amended definition of private communication. First generation cordless phones, which at the time of the amendments were used by 95 percent of

[138] *Ibid*.
[139] *Ibid*.
[140] *Ibid*.
[141] For instance, see the lawful access legislation proposed in 2005, 2009, and 2010 *supra* notes 72-74.

telephone users,[142] were susceptible to interception by simple scanner devices.[143] As a result, some courts held that communications via these phones did not attract a reasonable expectation of privacy.[144] These phones, like their analog pager predecessors, could therefore be tapped by anyone, including police, at will.

Others courts, in line with modern jurisprudence on section 8 of the *Charter*, concluded that reliance on the technical capabilities of a technology should not be the only factor considered.[145] To exclude 95 percent of then-current cordless phone users was arguably inconsistent with the privacy expectations of the average consumer, as it is unlikely that anyone other than the police were frequently trying to intercept phone calls.[146] Moreover, placing emphasis on the type of phone one owns allows those who can afford to purchase newly available technologies to have greater privacy protections.[147] Although new technologies are generally made broadly available, it is common for lower income households to have to wait several years before they can update their communications technologies.[148] Parliament, then, arguably drew an arbitrary and unfair distinction in its first amendment to the definition of "private communication".

(ii) Tracking Device Warrants

---

[142] See *R v Penna*, 36 WCB (2d) 483 at para 13, [1997] BCJ No 3014.
[143] *Ibid* at paras 13-18. See also *R v Watts*, 2000 BCPC 191 at paras 6-12, [2000] BCJ No 2721. Second generation phones send encrypted signals, making interception of a communication generally unintelligible. Third generation phones, in addition to sending encrypted messages, also frequently change the frequency with which the signal was sent making it extremely unlikely that the message could be intercepted, let alone made intelligible.
[144] See *Penna*, *supra* note 142 at paras 13-18; *Watts*, *supra* note 143 at para 12 (though note that the judge came to this conclusion "reluctantly").
[145] See *Watts*, *supra* note 143 at paras 8, 11. The Court in *Fearon*, *supra* note 105 at paras 52, 161, concluded that distinguishing between the capacities of dumb and smart phones was ill advised when developing the legal framework for searching cell phones incident to arrest. See also *Telus*, *supra* note 100 at para 5 ("[t]echnical differences inherent in new technology should not determine the scope of protection afforded to private communications").
[146] *Ibid*.
[147] As Member Derek Lee observed, "[a]pparently the only people . . . who are protected under the new bill [C-109] . . . are the ministers of the government, all of whom have encrypted conversation facilities. Government ministers are protected under the bill but ordinary Canadians are not." See "Bill C-109, An Act to amend the Criminal Code, the Crown Liability and Proceedings Act and the Radiocommunication Act", *House of Commons Debates*, 34th Parl, 3rd Sess, No 14 (30 April 1993) at 18,768.
[148] *Ibid*.

In its 2014 amendments, Parliament elevated the grounds necessary to receive a tracking device warrant if the device is commonly found on the person. Given the onset of GPS tracking, this sounds like a reasonable approach. However, it may unduly limit police depending on what technique is used to track a device. Tracking a cell phone, for instance, may involve police using a common tactic known as "pinging". This practice tells police with which cell phone tower a cell phone is exchanging signals. In *R v Grandison*,[149] the expert testimony revealed that the information gained from this tactic told police that the accused was anywhere from a 50 - 4894 metre radius from a tower.[150] The court also noted that pinging does not involve constant tracking of the subject, but instead requires that police make specific requests to the telecommunication service provider to determine the subject's approximate location at any given time.[151] This differs from GPS tracking which can allow police to determine an accused's location at any time.[152]

With a fuller understanding of the technology used for tracking cell phones, the court rejected the accused's contention that using the previous reasonable grounds to suspect standard was unconstitutional.[153] It came to this conclusion despite the amendments raising the relevant burden of proof having been implemented between the time the charge arose and when the court rendered its decision. Although the technique at issue was somewhat more sophisticated than the vehicle tracker used in *Wise*, the court concluded that the information revealed did not significantly touch on the biographical core of personal information required to constitutionally impose the higher reasonable and probable grounds standard.[154] Parliament's amendment, although well intended, inadvertently prevented police from using other reasonable and less invasive methods of

[149] See *Grandison*, *supra* note 109 at paras 64-65.
[150] *Ibid*.
[151] *Ibid* at para 66
[152] *Ibid* at paras 66-69. For an example where the state employed GPS technology under section 492.1, see *R v T & T Fisheries*, [2005] PEIJ No 74 at para 5, 2005 CarswellPEI 71.
[153] See *Grandison*, *supra* note 109 at para 74.
[154] *Ibid* at para 73.

cell phone tracking. By focusing on the capacity of a tracking device, and not the place of the thing being tracked, Parliament could have drawn a principled distinction between GPS technologies and other more non-invasive search technologies.

I do not wish to be understood as saying that the revised tracking device warrants constitute poor policy. The law is defendable in the vast majority of cases wherein police are able to monitor the exact whereabouts of a cell phone by tapping into its GPS locator. Parliament reasonably concluded that such a search will frequently reveal the location of the user as citizens commonly carry their cell phones on their person. This does not take away from the fact that judges could have drawn a more nuanced distinction and found that section 8 of the *Charter* required higher grounds only in instances where non-pinging tracking tactics were employed.

(iii) Digital Number/Transmission Data Recorders

As noted in the preceding section, the initial language of section 492.2 ("digital number recorder") was not broad enough to encompass metadata relating to technologies other than telephone calls. This had the effect of leaving metadata related to technologies such as email and text to be sought under the general warrant or production order provisions.[155] As these provisions require reasonable grounds to believe a crime has been committed before they will issue, they raised the grounds for receiving what is effectively the same information[156] from the lower reasonable suspicion standard required under section 492.2.[157] This was undesirable from a law

[155] See Penney, "Updating", *supra* note 24 at 144.

[156] As noted *supra* note 111, metadata is the data typically found on the outside of an unopened letter. With respect to an email, for instance, such data includes the "to" and "from," time codes, and routing information, but excludes the subject line. The metadata from a telephone conversation would include the numbers involved in the conversation and the duration of the call.

[157] It is notable that use of the reasonable suspicion standard has generally withstood constitutional challenge. See *R v Whitman-Langille*, [2004] QJ No 14164 aff'd in *Cody*, *supra* note 46; *R v Croft*, 2013 ABQB 640, 573 AR 339; *Grandison*, *supra* note 109, all refusing to follow two lower court decisions that earlier decided reasonable suspicion was not a suitable standard for such searches. See *R v Nguyen*, 2004 BCSC 76, [2004] BCWLD 462; *R v Hackert*, [1997] OJ No 6384 (ONCJ) aff'd [2000] OJ No 3495, 2000 CarswellOnt 3325 (ONCA). The contention that use of a

enforcement perspective as metadata data is often used early on to further an investigation and therefore is needed *to make out* reasonable and probable grounds for a warrant.[158] Although the 2014 amendments referenced earlier corrected this mistake, it persisted in the *Criminal Code* for twenty-one years.

(iv) General Warrants

Parliament passed the general warrant provision found in section 487.01 to allow courts to issue warrants permitting police to "use any device or investigative technique or procedure or do any thing described in the warrant that would, if not authorized, constitute an unreasonable search or seizure."[159] Although section 487.01 provides police with a flexible law enforcement tool,[160] it also abdicates authority for governing many novel search technologies to the courts. For instance, the following investigative techniques have all been (or can reasonably be anticipated to be) governed under section 487.01: Forward Looking Infrared (FLIR) thermal imaging,[161] installation of "amp meters" to measure electricity usage,[162] making electronic copies of data on a computer

---

dial number recorder qualified as a Part VI intercept has also failed. See *Fegan*, *supra* note 46. The term "intercept" contemplates communication *content* being exchanged.

[158] See Penney, "Updating", *supra* note 24 at 146-47.

[159] See section 487.01(1)(a-c).

[160] It is notable that such a broad discretion to allow courts to issue warrants for police tactics that Parliament had not contemplated has received significant criticism. See Steven Coughlan, *Criminal Procedure*, 2nd ed (Toronto: Irwin Law, 2012) at 133-34. However, constitutional challenges to the provision have been rejected. See *R v Lucas*, 2014 ONCA 561 at paras 104-26, 121 OR (3d) 303 leave to appeal ref'd 2015 CarswellOnt 639; *R v Kuitenen*, 2001 BCSC 677, 45 CR (5th) 131.

[161] The Court found in *R v Tessling*, 2004 SCC 67 at para 55, [2004] 2 SCR 432 that thermal imaging did not constitute a search but left open the possibility that technological advancement could lead to the opposite conclusion. Contrast this with the United States Supreme Court decision in *Kyllo v United States*, 533 US 27 (2001) wherein FLIR technology was generally found to invade a reasonable expectation of privacy. As radio frequency identification chips are now able to go "through the wall" (Fontana and Keeshan, *Search and Seizure*, *supra* note 65 at 572) and see actual activity going on inside the home, the courts will almost certainly have to revisit *Tessling*. To keep pace with developments in technology, some authors recommended that Parliament adopt FLIR warrants based on reasonable suspicion. See Steve Coughlan and Marc Corbet, "Nothing Plus Nothing Equals . . . Something? A Proposal for FLIR Warrants on Reasonable Suspicion" (2005) 23 CR (6th) 239.

[162] Although the Court in *R v Plant*, [1993] 3 SCR 281, 145 AR 104, initially determined that electrical consumption billing records did not constitute a search, the Court's more recent decision in *R v Gomboc*, 2010 SCC 55, [2010] 3 SCR 211, wherein the police installed a digital recording ammeter to the powerline connected to the house, turned on the terms and conditions of the contract issued for electrical services. But for the accused not having chosen to prevent warrantless disclosure to police, a majority of the Court would have found a reasonable expectation of privacy, which

system,[163] review of third party forensic files,[164] the ability to program failures into a criminal suspect's computer hardware,[165] use of forensic fluorescent light technologies to covertly search for bloodstains,[166] and the ability to perform phallometric testing.[167] As Daniel Scanlan posits, the general warrant "will [continue to] have broad application to the investigation of offences involving computers and the capture of data."[168] If true, the list of searches governed by the general warrant provision can reasonably be anticipated to continue growing.

My point in raising gaps in police powers which have been filled under section 487.01 is again not to suggest that the provision is poor policy. As Parliament recognized that it will be difficult to keep up with digital technologies, it is reasonable to allow courts to develop necessary police powers on a case-by-case basis. Although courts are likely to make mistakes when crafting such rules,[169] the general warrant provision at least allows for a discussion on whether a variety of police powers ought to exist. The general warrant provision therefore allows for the continuation of important dialogue on the appropriate scope of police power.[170] The fact that Parliament deferred this much authority to courts is nevertheless an implicit admission of its inability to craft efficient and coherent digital privacy rules.

---

would in turn have required a 487.01 warrant. See for instance *R v Christensen*, 2001 ABPC 227, 304 AR 148; *R v Nguyen*, 2005 ABQB 403, 379 AR 202.

[163] See *Keating v Nova Scotia (Attorney General)*, 2001 NSSC 85 at para 26, 194 NSR (2d) 290.

[164] See Scott Hutchinson & Michael Bury, *Search and Seizure Law in Canada*, looseleaf (updated 1 January 2018) at 16-39. The authors cite information personally received from the Attorney General in Ontario.

[165] *Ibid*.

[166] See *Application for a General Warrant pursuant to S.487.01 of the Criminal Code, Re*, 2002 SKPC 11, 52 WCB (2d) 517.

[167] See *R v Rayworth*, [1999] OJ No 5289, 45 WCB (2d) 291. It is possible that such a procedure would not satisfy the requirement that a general warrant not issue if it interferes with an accused's bodily integrity. As the Court recently observed in *R v Saeed*, 2016 SCC 24 at para 70, [2016] 1 SCR 518, the meaning of bodily integrity in section 487.01 is unclear. Lower courts have nevertheless upheld the photographing of anal and genital areas, which involves touching and manipulating the subject's genitalia. See *R v TGH*, 2014 ONCA 460, 120 OR (3d) 581; *R v HG*, 2005 QCCA 1160, [2005] JQ No 17665. Although phallometric testing does not require such physical contact, it is highly invasive in other obvious ways and may therefore not be issuable under the general warrant provision.

[168] See Daniel Scanlan, *Digital Evidence in Criminal Law* (Aurora: Canada Law Book, 2011) at 100.

[169] See the discussion in Chapter Two.

[170] See Peter Hogg and Allison Bushell, "The Charter Dialogue between Courts and Legislatures (Or Perhaps the Charter of Rights Isn't Such a Bad Thing after All)" (1997) 35 Osgoode Hall Law Journal 75.

(v) Computer Searches

The addition of subsections 487 (2.1) and (2.2) of the *Criminal Code* allow police to use "any computer system" to search for "any data" available to the computer system.[171] As Susan Magotiaux observes, the scope of these subsections is potentially boundless. "Depending on the configurations and active connections of a given device, there could be data accessible to the device from other people, other networks, other countries, or other businesses."[172] The privacy interests implicated by such computer searches were aptly summarized by Justice Fish. As he wrote in *R v Morelli*,[173] "[i]t is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer".[174] The need to ensure such searches respect privacy interests is therefore of the utmost importance.

Unfortunately, Parliament has not elaborated upon the process for searching computers. Indeed, until 2013 the Crown maintained that special authorizations for computer searches were unnecessary as computers are no different than filing cabinets or cupboards.[175] Although the Court unanimously rejected these analogies,[176] by far the more difficult question requires asking *how* computer searches must be conducted.[177] This concern prompted the Court in *R v Vu*[178] to suggest that the broad scope of computer searches may require Parliament or the courts to devise search protocols.[179] By enacting sections 487 (2.1) and (2.2), and then refusing to update these sections

[171] "Computer system" is defined in section 342.1(2).
[172] See Magotiaux, "Out of Sync", *supra* note 65 at 510-11. The courts have confirmed the breadth of this section includes data held on computers in other physical locations. See *R v Edwards* (ONSC), [1999] OJ No 3819, 44 WCB (2d) 45.
[173] *Supra* note 85.
[174] *Ibid* at para 2.
[175] See *R v Vu*, 2013 SCC 60 at para 24, [2013] 3 SCR 657.
[176] *Ibid*.
[177] See Gerald Chan, "Life After Vu: Manner of Computer Searches and Search Protocols" (2014) 67 Supreme Court Law Review 433 at 435.
[178] *Supra* note 175. The Court considered whether police were required to specifically state in a warrant that they were seeking to search computers found in the place searched. It answered this question in the affirmative.
[179] *Ibid* at paras 56, 62.

in response to the Court's decision in *Vu*, Parliament has again left it to the courts to determine the rules with respect to a complex search technology.[180]

Although some commentators believe that developing computer search protocols is not possible,[181] others have proposed ways forward.[182] The capacity and functionality of modern computers give rise to several basic questions.[183] Should police be able to look through every file and folder on a computer?[184] Does the type of crime investigated limit police to reviewing certain types of files? Should police searches be restricted to use of certain keywords? How does the plain view doctrine operate within computer searches?[185]

The need to explore the answers to these and related questions is important, as to leave computer searches to *ex post* review is inconsistent with the purpose of section 8 of the *Charter*: *preventing* unreasonable searches and seizures.[186] This is especially important as the case law is

---

[180] The courts have discussed and imposed search protocols in several cases before and after *Vu* was decided. See for instance *R v Jones*, 2011 ONCA 642 at para 42, 107 OR (3d) 241 (search must be related to legitimate targets of the warrant); *R v Beitel*, 2011 ONSC 5394 at paras 25-31, 243 CRR (2d) 296 (same;); *R c Boudreau-Fontaine*, 2010 QCCA 1108 at para 53, [2010] QJ 5399 (same; suggesting that a search from most to least obvious location should be followed); *R v Braudy*, [2009] OJ No 347, 81 WCB (2d) 561 (same); *A (Re)*, 2017 SKPC 90, 142 WCB (2d) 685 (same); *Ontario (Ministry of the Attorney General) v Law Society of Upper Canada*, [2010] OJ No 2975 (ONSC) at paras 2-4, Appendix A (several protocols implemented, including neutral third-party supervision, so as to ensure privileged information likely on computer would not be revealed to police).

[181] See Magotiaux, "Out of Sync", *supra* note 65 at 508; Orin Kerr, "Ex Ante Regulation of Computer Search and Seizure" (2010) 96 Virginia Law Review 1241 at 1282 (issuing judges "cannot get a sense of the exigencies that will unfold at each stage of the search process").

[182] See Chan, "Life After Vu", *supra* note 177 at 436. The author reviews the Canadian and some American jurisprudence, and in so doing teases out three guiding principles: "(1) The courts should carefully examine the methodology used by the police to determine whether they were faithful to the objectives of the warrant in their execution of the search. (2) The courts should resist categorical claims that every file on a computer must be examined, even if only cursorily, to determine its relevance. (3) The courts should require search protocols to be set out in the warrant in cases involving heightened privacy risks (e.g., searches involving potentially privileged information and confidential intellectual property; searches aimed at networks of computers; and searches targeting innocent parties)."

[183] Chan, "Life After Vu", *supra* note 177 at 436 asks the following questions.

[184] The Crown has argued that officers need to cursorily inspect every file, as file names may be camouflaged. See *R v Sonne*, 2012 ONSC 1463, 100 WCB (2d) 414; *R v Bishop*, 2007 ONCJ 441 at para 47, 75 WCB (2d) 258; *R v Little*, [2009] OJ No 3278 at para 93, 87 WCB (2d) 251.

[185] For an interesting discussion of the applicability of the plain view doctrine in the context of computer searches, see *R v Jones*, 2011 ONCA 632 at paras 59-70, 107 OR (3d) 241. If, for instance, the Crown is successful in arguing that police can "cursorily inspect" every file (*Sonne*, *supra* note 184; *Bishop*, *supra* note 184; *Little*, *supra* note 184), then the plain view doctrine would have nearly unlimited application.

[186] See *Hunter et al. v Southam Inc*., [1984] 2 SCR 145 at 160, 33 Alta LR (2d) 193.

replete with instances where police have grossly overstepped the boundaries of what would qualify as a "reasonable" search.[187] Moreover, new technological developments allow police to search in manners much more respectful of privacy interests.[188] Keeping on top of these developments is unlikely to occur within the current mode of adversarial trials, wherein courts are often limited with the types of information provided to them.[189] Parliament's approach so far has not, however, fared any better.

(vi) The Definition of "Intercept"

Although the Court reconciled the competing interpretations with respect to the meaning of "intercept" in *Telus* and *Jones*,[190] two main issues persist. The first concerns the prospective acquisition of "untransmitted" communications. As Steven Penney observes, the definition of "private communication" should be amended "to include the prospective interception of electronic communications *before* they are transmitted."[191] As the current definition of "private

[187] A good example is found in *Beitel*, *supra* note 180, wherein the officer, who was looking to see if the computer was stolen, began by searching in the recycle bin, and later searched for videos. It was clear that he was looking for child pornography or other nefarious videos. Similarly, see *R v Perkins*, 2013 ONSC 1807, 105 WCB (2d) 694 and *Boudreau-Fontaine*, *supra* note 180. Conducting computer network searches also makes the potential for over seizure much greater. The Canadian case of *United States of America v Equinix Inc*, 2013 ONSC 193, 104 WCB (2d) 848, provides a good example. In assisting the US with its investigation, the Attorney General of Canada was asked to send 32 servers worth of information to the US. The court refused to do so, as this was about 100 full laptops worth of information. It left the parties to "agree" on narrowing the content, but if the parties failed to agree, the court would have had to deal with the order without guidance.

[188] Consider EnCase, a software device that can tell its user if any files on a computer have been altered. This may address Crown arguments that it is necessary to search all documents as criminals may "camouflage" evidence. See *Sonne*, *supra* note 184 at para 66; *Ontario (Minister of the Attorney General) v Law Society of Upper Canada*, [2010] OJ No 2975 at para 19. Similarly, a search tool known as a "file header" can tell police whether, for instance, a video image document has been disguised as a word processing document. See Christina Schuck, "A Search for the Caselaw to Support the Computer Search Guidance in *United States v. Comprehensive Drug Testing*" (2012) 16 Lewis & Clark Law Review 741 at 750. It is also notable that in the context of the most common types of computer search investigations, child pornography, police tend to keep a large database of such videos and their "hash values" (32-digit numbers). Police can simply search for similar videos by searching hash values first, thereby preventing the need to conduct invasive searches. In a case such as *Little*, *supra* note 184, imposing such a search protocol would have prevented the need to cursorily search over 13,000 files. See para 102.

[189] See Scanlan, "Issues", *supra* note 1 at 312. For a review of the types of cases where courts have imposed search protocols, see note 174.

[190] See Part II(c) of Chapter Two.

[191] See Penney, "Updating", *supra* note 24 at 136.

communication" includes only "oral" communications and "telecommunications"—the latter of which requires the "emission, transmission or reception" of communicative content "by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system"—Part VI intercepts are not required to prospectively intercept non-oral communications which do not meet the definition of "telecommunication.[192] This creates at least one gap. Most notably, covertly installed key logger software could be used to record emails, passwords, and other communications before they are sent, but would not be afforded the protections in Part VI despite implicating identical privacy interests.[193]

Second, the result of relying on the prospective/retrospective distinction may cause constitutional issues in other contexts. As explained in Chapter Two, Justice Rowe's concurring opinion in *R v Jones*[194] suggests that the prospective/retrospective distinction may break down in practice, as it leaves the possibility of police applying for a transmission data warrant, and then subsequently applying for production orders to retrieve the stored messages a short time after they receive notice that a particular call or text was made.[195] If the moment of authorization is what matters, then there is nothing in the legislation stopping police from exploiting this loophole.[196] By narrowing the definition of "intercept", the problem with its definition has arguably been shifted to Parliament's production order scheme.[197]

(vii) Cell Phone Subscriber Information

[192] *Ibid* at 137.
[193] *Ibid* citing *United States v Scarfo*, 180 F Supp 2d 572 at 574 (DNJ 2001). I am unaware of any Canadian cases where police attempted to use this technology.
[194] *Supra* note 100.
[195] *Ibid* at paras 83-87.
[196] *Ibid*.
[197] For more in-depth review, see Chapter Two.

In *Re Subscriber Information*,[198] the court considered whether subscriber information to a cell phone could be retrieved by police without a warrant. As the phone in question was internet connected, the court concluded that its subscriber information attracted a reasonable expectation of privacy, even if non-internet connected phones did not.[199] As such, the Crown sought to have the cell phone's subscriber information produced through sections 487.016 and 487.017. To qualify, the information sought must relate to "telecommunication functions of dialling, routing, addressing or signalling" (487.016) or "the location of a transaction, individual or thing" (487.017).

The Crown argued that cell phone subscriber information relates to these functions because it is accumulated and stored to facilitate billing and collection of payment.[200] However, as billing does not relate to the *functioning* of telecommunications as required by these sections, it was held not to fall within the ambit of the provisions.[201] Other cases and legal commentary support this conclusion.[202] Parliament's 2014 amendments therefore created an anomalous result by permitting police to obtain transmission and location data on a lower standard (reasonable suspicion via sections 492.1 and 492.2) than basic subscriber information to internet connected cell phones (reasonable and probable grounds via section 487.014).[203]

---

[198] 2015 ABPC 178, 123 WCB (2d) 553.

[199] This followed on the reasoning of *Spencer*, *supra* note 4. For decisions determining that subscriber information to regular, non-internet connected phones, do not attract a reasonable expectation of privacy see *R v Khan*, 2014 ONSC 5664, 122 WCB (2d) 259; *R v Telus Communications Company*, 2015 ONSC 3964, 122 WCB (2d) 281; *Transmission Data Recorder Warrant, Re*, 2015 ONSC 3072, 254 ACWS (3d) 76.

[200] See *Re Subscriber Information*, *supra* note 198 at para 19.

[201] *Ibid* at paras 30-32.

[202] See *Telus (2015)*, *supra* note 199 at para 53; *Transmission Data Recorder Warrant*, *supra* note 199; Randy Schwartz, "*Criminal Update:* The Online Crime Act (Bill C-13) and New Police Search Powers", (Paper delivered during Webinar presented by Osgoode Hall Law School, May 11, 2015) [unpublished]; Marcy Henschel, "Obtaining Records of Cell Phone Calls and Text Messages" (Paper delivered at the Federation of Law Societies of Canada 42nd National Criminal Law Program, Edmonton Alberta, July 2015) [unpublished].

[203] See *Re Subscriber Information*, *supra* note 198 at para 55. As discussed in Part II(b) of Chapter Two in the context of police ability to obtain ISP subscriber information, basic subscriber information does not engage significant privacy interests given the limited information that can be determined from such requests. As such, it is reasonable for such information to be retrivable on a lower standard.

This omission is particularly egregious as the legislation was passed after the Court released its decision in *R v Spencer*.[204] Parliament's failure to subsequently provide for a police power to obtain ISP subscriber information similarly resulted in police needing to apply for a production order to obtain internet subscriber information. As explained in the previous Chapter, such a standard is far too onerous and could readily be lowered by Parliament. Unfortunately, Parliament has failed to provide a response to *Spencer* six years after it was released. It also failed to draft its 2014 production orders in a manner that would allow police to access subscriber information implicating similar privacy interests as those at issue in *Spencer*.

(viii) Summary

In most of the areas where Parliament has responded to the challenges of governing digital privacy, noticeable gaps and inconsistencies have been revealed via judicial and/or academic review. Again, it is difficult to provide a definitive reason for why holes in Parliament's legislative scheme frequently arise. However, it is reasonable to conclude that in some circumstances Parliament is not availed of the relevant information when passing its laws. It is likely that technology is not presented to legislators with a list of all of its current or possible future applications and all possible interaction effects with other technologies. Even with the advantage of time to study technologies in depth, what is done with the potential embedded in technology is difficult to anticipate.

In other instances, it may be that Parliament is acting in haste or without much interest in protecting privacy. Its response to early wireless phone technology is indicative of a lack of study or outright neglect of privacy interests in early cordless telephones. Parliament's difficulties passing lawful access legislation also witnessed the Conservative government, with its first

[204] 2014 SCC 43, [2014] 2 SCR 212.

majority, take advantage of this position by significantly expediting its legislation. In yet other instances, Parliament has made a deliberate choice to allow courts to create governing frameworks for digital technologies. The general warrant provision in section 487.01, as well as the broad computer search powers found in sections 487(2.1) and (2.2), are illustrative. These responses demonstrate that Parliament often fails to respond adequately or intelligibly to digital privacy challenges despite its theoretical advantage over courts.

(c) Public Choice Theory

Public choice theory cautions that the legislative process may be skewed in favour of powerful interest groups or majoritarian interests. Less fortunate groups will therefore suffer to the benefit of often wealthier, less diverse, and better organized groups.[205] Although Canada is generally less susceptible to the negative influences of lobbying,[206] scholars argue that novel search technologies are immune from majoritarian concerns.[207] The logic underlying these assertions has not, however, been tested in the Canadian digital/criminal procedure context.

(i) The Relevance of Public Choice Theory

In his seminal article on the relative institutional capacities of courts and legislatures to govern complex and rapidly advancing search technologies, Orin Kerr rejects the proposition that public choice considerations impact criminal procedure rules.[208] In his view, law enforcement actors do not seek benefits from government. As Kerr observes, "[i]n most cases, law enforcement does not 'profit' more or less based on how restricted its investigative powers may be, and does

[205] See Penney, "Reasonable Expectations", *supra* note 1 at 503 citing Kent Roach, *Due Process and Victims' Rights: The New Law and Politics of Criminal Justice* (Toronto: University of Toronto Press, 1999); William Stuntz, "The Pathological Politics of Criminal Law" (2001) 100 Michigan Law Review 505 at 553-56.
[206] See Raj Chari, Gary Murphy, and John Hogan, "Regulating Lobbyists: A Comparative Analysis of the United States, Canada, Germany and the European Union" (2007) 78 The Political Quarterly 422; Barrie McKenna, "Corrupt Canada? We're Small Time Compared to the US" *Globe and Mail* (10 October 2010).
[207] See Kerr, "Fourth Amendment", *supra* note 7 at 884-88.
[208] *Ibid.*

not have a clear economic incentive to lobby Congress for less privacy-protecting rules."[209] Although law enforcement does lobby for greater powers with significant success, its view "generally reflects honest (if sometimes myopic) claims of the public interest in solving crimes, and the latter generally reflects legitimate public preferences."[210]

Kerr does, however, recognize that majoritarian concerns are thought by others to be influential on the legislative process.[211] Politicians are vote-seekers, and being "tough on crime" is popular among many voters. Thus, there is an incentive to provide restrictive privacy legislation in the criminal context, and nowadays that means providing police with tools which are invasive of digital privacy.[212] Even if true, Kerr suggests that digital technologies are likely an exception, as they are used disproportionately by the wealthy.[213] These individuals will be able to effectively represent their privacy interests before legislatures, "resulting in a healthy debate and relatively favorable conditions for balanced legislative rules."[214] In such an environment, Kerr maintains, the typical public choice concerns will be significantly mitigated.

There are three reasons to question this position. First, Kerr assumes that because a technology is widespread, people will fight for privacy protections even in the criminal law context.[215] However, this position ignores the popular argument that "[i]f you've got nothing to hide, you've got nothing to fear."[216] This way of thinking can be a powerful tool for justifying

---

[209] *Ibid* at 885.
[210] *Ibid*.
[211] *Ibid* at 886-87 citing Donald Dripps, "Criminal Procedure, Footnote Four, and the Theory of Public Choice; Or, Why Don't Legislatures Give a Damn About the Rights of the Accused?" (1993) 44 Syracuse Law Review 1079. As discussed in Part II (a), these concerns have also appeared in Canada.
[212] *Ibid*.
[213] See Kerr, "Fourth Amendment", *supra* note 7 at 886-87.
[214] *Ibid*.
[215] *Ibid*.
[216] See Daniel Solove, *Nothing to Hide: The False Trade-off between Privacy and Security* (New Haven: Yale University Press, 2011) at 22. This argument focuses on the small harms caused by many privacy invasions when looked at in isolation, and then compares them to big harms caused to public safety by larger threats such as terrorism.

intrusive criminal law policies to majorities. These policies in turn predominantly effect marginalized groups as they are far more likely to be investigated by police.

Second, the digital divide has been significantly mitigated in recent years. Most everyone now has access to smart phones, computers, and the internet,[217] thus increasing the likelihood that fighting crime means invading digital privacy.[218] Although increased availability of a technology might result in more citizens lobbying for privacy protections, the diffuse nature of privacy interests makes organizing efforts much less likely to be succesful.[219]

Finally, the greater capacity of digital technologies may equate to economic benefits for private corporations. The more private corporations have to gain from privacy-invasive legislation, the more likely they will lobby for it. At least in the American context, private corporations have been shown to be influential in the creation of privacy-restrictive criminal procedure rules.[220] It is nevertheless important to observe that many corporations also have incentive to lobby for more privacy-favoring rules.[221] It is currently unknown which of these groups are more successful at influencing the development of criminal procedure rules implicating digital technologies.

---

[217] See Sheena Goodyear, "Digital Divide: Is high-speed internet access a luxury or a right?" *CBC News* (9 February 2016) citing a 2015 survey by Ipsos Reid. The survey found that of the 1250 Canadians questioned 91 percent have the internet at home. From the nine percent that do not, only 30 percent cited cost as a barrier. The remaining 70 percent cited a lack of interest or ability to use the internet.

[218] See Murphy, "Politics of Privacy", *supra* note 17 at 505-06. See also Steven Penney, "Fear the Fearon? Searches of Digital Devices Incident to Arrest" Webcast (6 February 2015) online: <https://ualawccsprod.srv.ualberta.ca/index.php/webcasts/811-fear-the-fearon-searches-of-digital-devices-incident-to-arrest-professor-steven-penney>. Interestingly, Penney observes a difference in privacy protections in cases where upper-class citizens' privacy is implicated (ISP subscriber information) and those where lower-class privacy interests are at issue (searches of cell phones incident to arrest).

[219] See Komesar, *Imperfect Alternatives*, *supra* note 16 at 56 ("[c]onsumers, each of whom bears only a relatively minor cost, do not even have the incentive to understand these negative effects let alone to organize activity to combat them").

[220] See Murphy, "Politics of Privacy", *supra* note 17 at 535-36; David Sklansky, "Two More Ways Not to Think about Privacy and the Fourth Amendment" (2015) 82 The University of Chicago Law Review 223 at 227. The nature of these lobbying activities will be discussed in more detail in the next Chapter.

[221] Companies such as Apple and Google are prime examples. Each company is frequently at odds with law enforcement over whether police may search their customers cell phones and computers. See Steven Penney and Dylan Gibbs, "Law Enforcement Access to Encrypted Data: Legislative Responses and the *Charter*" (2017) 63 McGill Law Journal 201 at 211.

(ii) The Canadian Experience

A review of the legislation discussed above did not reveal significant public choice theory concerns.[222] In some instances, however, elements of undue influence or majoritarianism were directly raised in debates before the House of Commons or in newspaper articles. Beginning with Bill C-109 in 1993, the opposition parties questioned the motivation behind enacting section 184.5 of the *Criminal Code*, which allowed interception of radio-based communications commonly conducted via early models of cordless and cellular phones, but prohibited malicious or profitable disclosure of such communications.[223] The accusation was that telecommunications companies would prosper by having looser privacy protections in the area of radio-based cellular and cordless phone communications, which constituted millions of users at that time.[224] Consumers who value their privacy are much more likely to buy added encryption protection than they would if that protection was provided by law. The opposition parties strongly suggested that banning scanners used to intercept communications was a much more reasonable way of protecting privacy interests.[225] The Conservative government did not, however, see a problem with its legislation being directly aimed at helping telecommunications companies "prosper."[226]

---

[222] See "Bill C-15A, An Act to amend the Criminal Code and to amend other Acts", *House of Commons Debates*, 37th Parl, 1st Sess, No 97 (18 October 2001) at 1315-60 (The Bill was seen as non-controversial by all parties); Bill C-13, 2004 c 3 (the legislation—which was debated under "Bill C-46, An Act to amend the Criminal Code (capital markets fraud and evidence-gathering", *House of Commons Debates*, 37th Parl, 2nd Sess, No 129 (29 September 2003; 8 October 2003; 03 November 2003; 05 November 2003)—concerned the general and financial production orders, but the debate centered on the more contentious issue of insider trading offences that were passed as part of the Bill); Bill C-13, "An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act", 41st Parl, 2nd Sess, No 25 (27 November 2013) (the cyberbullying offence was uncontroversial).

[223] "Bill C-109, An Act to amend the Criminal Code, the Crown Liability and Proceedings Act and the Radiocommunication Act", *House of Commons Debates*, 34th Parl, 3rd Sess, No 13 (26 February 1993) at 16558-60.

[224] *Ibid* at 16559.

[225] *Ibid* at 16558-62. This approach had been taken in the United States.

[226] *Ibid* at 16655. As Mac Harb states in debate, "[o]f course, some people are going to say the purpose of this piece of legislation is to help out the industry and the cellular telephone companies. Well, of course it is. We should be proud of the fact that as legislators we are doing everything we can to help our industry prosper."

Aside from the above isolated example, the lawful access experience provides the most illuminating case study for considering the impact of public choice theory concerns in the digital privacy context. In Parliament's first review of the issues, it consulted more than 300 organizations ranging from police services, telecommunications service providers, civil rights groups, and individual Canadians.[227] As a result of this study, Parliament tabled Bill C-74 in 2005 only to have it die on the order table as a result of an election being called.[228] As mentioned earlier, subsequent attempts to pass lawful access legislation were made in 2009, 2010, and 2012. These proposals did not make it past first reading. The 2014 proposals found in Bill C-13, however, were passed by a majority Conservative government.

The initial proposal in Bill C-74 provided that all internet service providers install infrastructure making them capable of intercepting both transmission data and communications content.[229] This constituted a substantial change, as only telecommunication service providers were previously required to maintain intercept capabilities.[230] Bill C-74 further proposed that designated law enforcement officers be able to demand that internet service providers provide warrantless access to basic subscriber information.[231] Although Bill C-74 required that records of all requests be kept,[232] internal audits by police agencies were the only mandatory review of police requests for subscriber information.[233] The subsequent lawful access proposals in 2009, 2010, and 2012 all included similarly controversial features.[234]

---

[227] See Valiquet, "Backgrounder", *supra* note 101 at C(1).
[228] See Daphne Gilbert, Ian Kerr, and Jena McGill, "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers" (2006) 51 Criminal Law Quarterly 469 at 483.
[229] Dominique Valiquet, "Telecommunications and Lawful Access: I. The Legislative Situation in Canada" (Canada: Library of Parliament, 2006), online: <http://www.parl.gc.ca/Content/LOP/ResearchPublications/prb0565-e.html>.
[230] *Ibid*.
[231] *Ibid*.
[232] *Ibid*.
[233] *Ibid*.
[234] See Dominique Valiquet, *Legislative Summary of Bill C-47: Technical Assistance for Law Enforcement in the 21st Century Act* (28 July 2009), online:

Throughout this experience the federal government justified its lawful access legislation in a variety of ways.[235] Bill C-74 was originally marketed by government as a response to the terrorist attacks of 11 September 2001, as well as a general perception that law enforcement was being technologically outpaced by criminals.[236] After this marketing tactic proved unpersuasive in 2009 and 2010,[237] the government changed its position. In response to criticisms of Bill C-30 in 2012, then-Public Safety Minister Vic Toews infamously responded to critics by saying that people were either with the government or "with the child pornographers."[238] The political backlash from this frivolous statement resulted in the bill being shelved.[239] Bill C-13, the legislation which ultimately passed in 2014, was successfully marketed by a then-majority Conservative government as

<https://lop.parl.ca/About/Parliament/LegislativeSummaries/Bills_ls.asp?language=E&ls=c47&source=library_prb&Parl=40&Ses=2>; Erin Shaw and Dominique Valiquet, *Legislative Summary of Bill C-30: An Act to Enact the Investigating and Preventing Criminal Electronic Communications Act and to Amend the Criminal Code and other Acts* (15 February 2012), online: <https://lop.parl.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?ls=c30&Parl=41&Ses=1&source=library_prb&Language=E>.

[235] See Christopher Parsons, "Stuck on the Agenda: Drawing Lessons from the Stagnation of 'Lawful Access' Legislation in Canada" in Michael Geist, ed, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (Ottawa: University of Ottawa Press, 2015) 257 at 262 citing Department of Justice, "Summary of Submissions to the Lawful Access Consultation", (Ottawa: 7 January 2015), online: <http://www.justice.gc.ca/eng/cons/la-al/sum-res/faq.html>; Jesse Kline, "Vic Toews Draws Line on Lawful Access: You're with Us, or the Child Pornographers" *National Post* (14 February 2012), online: <http://nationalpost.com/opinion/vic-toews-draws-line-on-lawful-access-youre-with-us-or-the-child-pornographers>; Daniel Proussalidis, "Magnotta to be Charged with Criminal Harassment of PM" *Winnipeg Sun* (1 June 2012), online: <http://winnipegsun.com/2012/06/01/internet-snooping-bill-would-be-helpful-in-lin-case-toews/wcm/ad158458-2a17-463f-904d-716cae0de5c6>; Tabatha Southey, "Bill C-13 is about a lot more than Cyberbullying" *Globe and Mail* (6 December 2013), online: <https://www.theglobeandmail.com/opinion/columnists/maybe-one-day-revenge-porn-will-be-have-no-power/article15804000/>.

[236] See CBC News, "Harper Government Should Adopt Liberal Bill on Surveillance: MP" *CBC News* (29 March 2007), online: <http://www.cbc.ca/m/touch/canada/story/1.635923>; Public Safety and Emergency Preparedness Canada, "Legislation to Modernize Investigative Techniques Introduced Today," *Government of Canada* (15 November 2005); Valiquet, "Telecommunications", *supra* note 229.

[237] See "Privacy Watchdog Reiterates Lawful Access Concerns" *CBC News* (27 October 2011), online: <www.cbc.ca/news/technology/privacy-watchdog- reiterates-lawful-access-concerns-1.996304>.

[238] See Kline, "Toews", *supra* note 235. See also Sarah Schmidt and Jason Fekete, "Vic Toews will 'Entertain Amendments' to Online Surveillance Bill" (15 February 2012), online: <https://nationalpost.com/news/canada/protecting-children-from-internet-predators-act-vic-toews> (observing that when the Bill was originally tabled it was called the "Lawful Access Act, but that version was quickly withdrawn and replaced with the Protecting Children from Internet Predators Act").

[239] *Ibid*. Minister Toews was also pressured into apologizing for the comment two days later. See Laura Payton, "Toews Steps Back from Child Pornographers Comment," *CBC News* (16 February 2012), online: <www.cbc.ca/news/politics/ toews-steps-back-from-child-pornographers-comment-1.1127817>.

addressing holes in the legislative scheme relating to cyberbullying, while its lawful access provisions were downplayed.[240]

No matter the underlying rationale for the lawful access proposal, each attempt was consistently met with fierce opposition from civil rights groups, privacy commissioners, academics, opposition parties, and at times internet service providers.[241] Civil rights groups rapidly disseminated information to the public via the media to create opposition to the controversial aspects of each attempt to institute lawful access legislation.[242] In so doing, they questioned (among other aspects of the proposal) the government's lack of explanation for how the proposed police powers would lower crime levels, how such powers could be justified without prior judicial review, and the absence of mandatory oversight of the police's ability to obtain internet subscriber information.[243] Concern was also raised about the desirability of the state effectively soliciting service providers as state agents in fighting crime.[244] The federal and various provincial privacy commissioners raised many of the same concerns both during the initial 2003 consultation process[245] as well as during all succeeding consultations.[246]

---

[240] See Southey, "Bill C-13", *supra* note 235.
[241] See Parsons, "Stuck on the Agenda", *supra* note 235 at 262-63.
[242] *Ibid* at 263.
[243] See "Summary of Submissions to the Lawful Access Consultation" (16 April 2003), online: <http://canada.justice.gc.ca/eng/cons/la-al/sum-res/6.html> at Chapter 6, Part A. For a list of the 14 main civil society groups submitting on lawful access see Appendix D.
[244] *Ibid* at Part B.
[245] *Ibid*, Chapter 5.
[246] See Office of the Privacy Commissioner of Canada, "Response to the Government of Canada's 'Lawful Access' Consultations" (May 2005), online: <http://www.priv.gc.ca/information/research-recherche/sub/sub_la_050505_e.asp>; Jennifer Stoddart et al., "Letter to Public Safety Canada from Canada's Privacy Commissioners and Ombudspersons on the Current 'Lawful Access' proposals" (9 March 2011), online: <http://www.priv.gc.ca/ media/nr-c/2011/let_110309_e.asp>; Office of the Privacy Commissioner of Canada, "Statement from the Privacy Commissioner of Canada regarding Bill C-13" (28 November 2013), online: <http://www.priv.gc.ca/media/nr-c/2013/s-d_131128_e.asp>; Privacy Commissioners of Ontario, Alberta, British Columbia, "RE: Police Chiefs Speak out" *Information and Privacy Commissioner of Ontario* (7 November 2012), online: <http://www.ipc.on.ca/ english/About-Us/Whats-New/Whats-New-Summary/?id=263>.

Academics were also active in criticizing not only the proposed legislation but also the consultation process leading up to the 2009 proposal.[247] With respect to the proposed warrantless access to subscriber information, some authors warned that this development would lead to "a significant alteration in the procedural safeguards against excessive fishing expeditions by law enforcement agencies."[248] The fact that the legislation provided no overview for this practice made the government's proposal even more controversial.[249] When the government neglected to consult with privacy advocates in its 2007 deliberations on lawful access legislation,[250] academics were also quick to criticize the consultation process and called on media outlets to disseminate this information widely.[251] This resulted in the government conducting increased consultations with civil society groups.[252]

Opposition parties also seized on the opportunity to critique the government for ignoring the privacy interests inherent in its lawful access regimes.[253] During the 2009-12 proposals, both the Liberal and New Democratic parties launched campaigns against each successive bill including petitions protesting the Conservative government's lawful access proposals.[254] Each Party accused

---

[247] See e.g. James Stribopoulos, "Peeking in Cyberspace's Backdoor" *Toronto Star* (12 July 2009).
[248] See Gilbert et al., "The Medium", *supra* note 228 at 486. It is notable that the practice at the time allowed law enforcement to receive warrantless access to subscriber information in child exploitation investigations. The new proposals reviewed earlier, however, would allow such information to be available upon demand in all investigations.
[249] See Parsons, "Stuck on the Agenda", *supra* note 235 at 264 citing Philippa Lawson, *Moving towards a Surveillance Society: Proposals to Expand "Lawful Access" in Canada* (Vancouver: British Columbia Civil Liberties Association, 2012).
[250] See Michael Geist, "Public Safety Canada Quietly Launches Lawful Access Consultation" *Michael Geist* (blog), (11 September 2007), online: <www.michael- geist.ca/content/view/2228/99999/>. The consultation process was largely restricted to law enforcement and telecommunication industry representatives.
[251] *Ibid*. See also "Government Moving to Access Personal Info, Sparking Privacy Fears" *CBC News* (12 September 2007), online: <www.cbc.ca/news/technology/govern- ment-moving-to-access-personal-info-sparking-privacy-fears-1.631075>.
[252] *Ibid*.
[253] *Ibid* citing Lindsey Pinto, "NDP Leader Responds to StopSpying.ca Campaign" *OpenMedia* (25 May 2012), online: <https://openmedia.org/en/ndp-leader-responds-stopspyingca-campaign>. A general overview of all the House of Commons debates on the lawful access legislation shows that the NDP and, to a lesser extent, the Liberal Party, were fiercely opposed to many controversial aspects of each proposal.
[254] See Parsons, "Stuck on the Agenda", *supra* note 235 at 267 citing Liberal Party of Canada, "Don't Let Harper Read Your Emails" (2013), online: <http://petition.liberal.ca/online-privacy-surveillance-lawful-access-bill-c30-liberal-amendment/> and a personal interview with Steve Anderson in 2013. See also Lindsey Pinto, "NDP Leader Responds

the government of pandering to majoritarian desires to be "tough on crime" as opposed to drafting a constitutionally compliant lawful access scheme which took seriously the many concerns raised by pro-privacy advocates.[255]

A series of social media campaigns were also highly influential in painting the government's 2009-12 bills as anti-privacy.[256] Online petitions were created by some media outlets to oppose the proposed legislation.[257] News outlets outright mocked the Public Safety Minister, Vic Toews, for his apathetic stance towards privacy.[258] As opposed to writing the Minister with their privacy concerns, various Canadians flooded the Minister's Twitter feed with highly personal information. The "Tell Vic Everything" campaign was directed at illustrating the types of information his proposed warrantless access to subscriber information would frequently reveal about Canadians' online activity.[259] The topic was the most heavily trending in Canada during its peak, and even trended briefly internationally.[260]

Finally, internet service providers questioned the need for broad access powers, and also raised the more self-interested question of who would incur the costs of installing the necessary

---

to StopSpying.ca Campaign" *OpenMedia* (25 May 2012), online: <openmedia.ca/blog/ndp-leader-responds-stopspyingca-campaign>.

[255] See for example "Bill C-46, An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act", *House of Commons Debates*, 40th Parl, 2nd Sess, No 100 (26 October 2009; 27 October 2009) at 1700-05; "Bill C-47, An Act regulating telecommunications facilities to support investigations", *House of Commons Debates*, 40th Parl, 2nd Sess, No 101 (27 October 2009) at 1620-25.

[256] See Jesse Brown, "Slacktivism Defeats Lawful Access" *Maclean's* (21 September 2011), online: <http://www.macleans.ca/society/technology/slacktivism-defeats-lawful-access/>; Laura Stone, "Conservatives Kill Internet Surveillance Bill C-30", *iPOLITICS* (11 February 2013), online: <www.ipolitics.ca/2013/02/11/conservatives-kill-internet-surveillance-bill-c-30>; Laura Payton, "Internet Privacy Experts raise Concerns over Crime Bill" *CBC News* (9 August 2011), online: <http://www.cbc.ca/news/politics/internet-privacy-experts-raise-concerns-over-crime-bill-1.1090482>; Laura Payton, "'Tell Vic Everything Tweets' Protest Online Surveillance" *CBC News* (16 February 2012), online: <http://www.cbc.ca/news/politics/tell-vic-everything-tweets-protest-online-surveillance-1.1187721>.

[257] See "Stop Online Spying" *OpenMedia* (2013), online: <https://openmedia.org/en/ca/look-back-our-stop-spying-campaign-against-canadas-bill-c-30>.

[258] See Payton, "Tell Vic", *supra* note 256.

[259] *Ibid*.

[260] *Ibid*.

infrastructure to provide government access.[261] Perhaps most importantly, service providers successfully forestalled a government proposal to modify the *Solicitor General's Enforcement Standards (SGES) for Lawful Interception of Telecommunications*.[262] This proposal required licensed service providers to replace circuit switched telephony systems with interconnected radio-based transmission facilities.[263] As the service providers representative observed, this change "opens up several additional services to interception requirements, including Internet services, and cable and broadcasting services."[264] Representatives for the service providers objected as this strategy sought to do with regulations what Parliament had been unable to accomplish with its legislation.[265] Even without any response from other privacy advocates,[266] the federal government backed off from this proposed change.[267]

The impact of the aforementioned pro-privacy groups could be seen throughout the government's various proposals. As Parliament admitted in its legislative backgrounder to Bill C-74,[268] any requirement that service providers collect and store information about their customers' internet viewing histories was not included because of the views expressed by pro-privacy

---

[261] See Parsons, "Stuck on the Agenda", *supra* note 235 at 263 citing Dominique Valiquet, "Telecommunications and Lawful Access: I. The Legislative Situation in Canada" (Canada: Library of Parliament, 2006), online: <http://www.parl.gc.ca/Content/LOP/ResearchPublications/prb0565-e.html>; Nestor Arellano, "Small ISPs Foresee Cost Burden in 'Lawful Access' Bills" *ITBusiness* (27 June 2011), online: <https://www.itbusiness.ca/news/small-isps-foresee-cost-burden-in-lawful-access-bills/16419>; Christopher Parsons, "Unpacking the Potential Costs of Bill C-30" (2012) 9:6 Canadian Privacy Law Review 57.

[262] See Parsons, "Stuck on the Agenda", *supra* note 235 at 268-69.

[263] See Canadian Wireless Telecommunications Association, "Re: Consultation on a Licensing Framework for Mobile Broadband Services (MBS) — 700 MHz Band" *Canadian Radio-television Telecommunications Commissioner* (22 June 2012), online: <https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/DGSO-002-12-comments-CWTA-submissions.pdf/$FILE/DGSO-002-12-comments-CWTA-submissions.pdf>. See also Nicholas Kyonka, "Telcos Object to Industry Department's 'Lawful Intercept' Proposal for 700 MHz Band," *Wire Report* (9 July 2012), online: <www. thewirereport.ca/news/2012/07/09/telcos-object-to-industry-department's- 'lawful-intercept'-proposal-for-700-mhz/25496>.

[264] *Ibid*.

[265] *Ibid*.

[266] See Parsons, "Stuck on the Agenda", *supra* note 235 at 268.

[267] *Ibid*.

[268] See Valiquet, "Backgrounder", *supra* note 101.

advocates.[269] This is contrary to numerous regimes in Europe which have such data retention policies.[270] A national database storing names and addresses of customers was also removed from Bill C-74.[271] As was a "know your customer" requirement. The latter would require knowing the identity of who was purchasing a service, which would prevent selling items such as anonymous phone cards.[272] The concerns raised by privacy advocates dissuaded Parliament from trying to implement these anti-privacy policies.[273]

More importantly, the government conceded that any modernization to police powers would not include "the warrantless mandatory disclosure of basic subscriber information or the requirement for telecommunications service providers to build intercept capability within their systems."[274] Bill C-13, which came into force in 2014, upheld this promise. Although it contained significant gaps and inconsistencies,[275] the legislation that passed is much less controversial than when the consultation process began. Overall, then, the lawful access experience is a case study which exemplifies the ability of civil society to mobilize to protect digital privacy interests.

Conclusion

American scholars have entertained a lively debate about the relative institutional capacities of legislatures and courts to govern privacy interests in rapidly evolving and complex

---

[269] *Ibid* at D(1).
[270] See Ann Cavoukian, "Privacy, Transparency, and the Rule of Law: Critical to Preserving Freedom and Liberty" (2005) 19 National Journal of Constitutional Law 193 at 210 citing Robert Wielaard "Data Retention Bill Divides EU Countries" *SFGate.com* (8 September 2005); "U.K. sets out case for data logs to fight terror", *Yahoo News* (*Reuters*) (7 September 2005); and "EU data protection chief warns against anti-terrorism plans", *Mercury News* (26 September 2005); Nicol and Valiquet, "Legislative Summary of Bill C-13", *supra* note 112 at 11.
[271] Law enforcement specifically wanted this addition. See Valiquet, "Backgrounder", *supra* note 101 at subheading "(A)" under the heading "Commentary".
[272] *Ibid* at D(2).
[273] *Ibid*. See also Michael Geist, "Ottawa finds public no pushover in snooping law" *The Toronto Star* (30 October 2006) at EO3.
[274] Laura Payton, "Government Killing Online Surveillance Bill" *CBC News* (11 February 2013), online: <http://www.cbc.ca/news/politics/government-killing-online-surveillance-bill-1.1336384>.
[275] See Parts II(a) and (b) above.

search technologies. Although the Canadian judiciary has encountered similar problems as their American counterparts, a comprehensive study had not been undertaken to assess the potential advantages of having Canadian legislatures govern digital technologies. This Chapter fills this void with respect to the relative institutional capacities of Parliament. After reviewing several decades of its legislation, I conclude that there is little reason to believe that Parliament is quicker or more coherent in its responses to digital technologies than courts. Unlike with the American experience, however, concerns about Parliament being unduly influenced were minor. This may be the result of the relatively stable political climate in Canada, or, as Kerr contends, because the populace is more likely to defend its digital privacy interests given its general importance to the polity. In either event, the preceding review of the institutional capacity of Canadian courts and Parliament to respond to the challenges of governing digital privacy shows that neither have significant advantages over the other.

Chapter Four

Criminal Law & Digital Technologies: The American Experience

Introduction

The Fourth Amendment of the American Constitution provides each citizen with the right to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures".[1] Whether an activity constitutes a search or seizure is governed by the Supreme Court's decision in *Katz v United States*.[2] In rejecting a conception of the Fourth Amendment based exclusively in real property law, the Court famously proclaimed that "the Fourth Amendment protects people, not places."[3] It does so by prohibiting state actions which intrude on an individual's subjective expectation of privacy if society believes such an expectation is objectively reasonable.[4] In these cases, law enforcement will typically require a warrant supported by probable cause to conduct the search or seizure.[5]

[1] The full text of the Fourth Amendment reads as follows: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
[2] 389 US 347 (1967).
[3] *Ibid* at 351.
[4] *Ibid*.
[5] *Ibid*.

The ability of the judicial and legislative branches to adapt the Fourth Amendment to the digital world has come under significant scrutiny.[6] In line with the discussion in the previous Chapters, American scholars have generally questioned the ability of each institution to respond to digital technologies in an efficient, coherent, and even-handed manner.[7] Yet, these scholars' understanding of the evidence relevant to assessing legislative and judicial capacity to craft criminal procedure rules implicating digital technologies varies significantly.[8] The aim of this Chapter is to scrutinize the available evidence and draw my own conclusions with respect to the relative institutional capacities of Congress and the American courts to provide rules governing digital technologies.

The Chapter proceeds as follows. Part I assesses the institutional competence of American courts to craft digital privacy criminal procedure rules. In so doing, I focus less on trial courts as the literature is replete with examples of trial judges misunderstanding digital technologies. Instead, I expand upon the existing literature by exploring the extent to which the Supreme Court has had difficulties understanding digital technologies. Part II then provides a detailed record of Congress' ability to enact efficient, coherent, and balanced rules. This analysis is necessarily more detailed given the significant disagreement on this point between leading scholars. Part III concludes by outlining the main factors contributing to the difficulties Congress and courts have crafting criminal procedure rules implicating digital technologies.

---

[6] See Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution" (2004) 102 Michigan Law Review 801; Orin Kerr, "Congress, the Courts, and New Technologies: A Response to Professor Solove" (2005) 74 Fordham Law Review 779; Daniel Solove, "Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference" (2005) 74 Fordham Law Review 747; Erin Murphy, "The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions" (2013) 111 Michigan Law Review 485**;** David Sklansky, "Two More Ways Not to Think about Privacy and the Fourth Amendment" (2015) 82 The University of Chicago Law Review 223.

[7] *Ibid*.

[8] Each author's views will be discussed throughout this Chapter.

I. Judicial Capacity to Govern Digital Technologies

The early scholarship assessing the American judiciary's ability to respond to the challenges of governing digital technologies provided overwhelming evidence that trial courts have difficulty devising coherent evidentiary records.[9] An overview of trial court decisions would therefore serve little purpose as the reasons inadequate evidence is obtained are similar to those identified in the Canadian adversarial process.[10] The American literature does not, however, seriously consider whether appellate courts have difficulties updating evidentiary records.[11] As I contend below, there is good reason to conclude appellate courts are able to update their evidentiary records. Their governance problem is that they avoid engaging with many digital technologies via employing outdated and ill-fitting legal doctrine.

(a) Early Jurisprudence

The Court's decision in *Katz v United States*[12] marked a break in Fourth Amendment jurisprudence from a property- to a privacy-based conception.[13] Under the property-centric approach, whether a defendant had a right to exclude other people generally dictated the applicability of the Fourth Amendment.[14] The popular understanding is that the Court in *Katz* rejected this view, holding instead that the Fourth Amendment "protects people, not places".[15] It

[9] See especially Kerr, "Fourth Amendment", *supra* note 6. Even Daniel Solove, perhaps the most adamant defender to a judicial approach to governing digital privacy, agrees with Kerr on this point. See Solove, "Fourth Amendment", *supra* note 6 at 751; Daniel Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004) at 42.
[10] See generally Chapter Two.
[11] Kerr provides only three examples of courts of appeals misunderstanding digital technologies. See Kerr, "Response", *supra* note 6 at 785-86 citing *United States v Carey*, 172 F 3d 1268 (10th Circuit 1999); *United States v Maxwell*, 45 MJ 406 (CAAF 1996); *United States v Simons*, 206 F 3d 392 (4th Circuit 2000).
[12] See *Katz*, *supra* note 2.
[13] See Kerr, "Fourth Amendment", *supra* note 6 at 815, 820 citing (among others) Jerold Israel and Wayne Lafave, *Criminal Procedure in a Nutshell*, 5th ed (1993) at 60; Andrew Taslitz and Margaret Paris, *Constitutional Criminal Procedure* (1997) at 95.
[14] See Kerr, "Fourth Amendment", *supra* note 6 at 810-15.
[15] See *Katz*, *supra* note 2 at 347.

does so by answering a normative question of when an expectation of privacy is considered "reasonable".[16]

Despite the popular interpretation of *Katz*, the Court has consistently upheld a property-centric approach to the Fourth Amendment.[17] Post-*Katz*, the Court has affirmed that the Fourth Amendment only applies to houses,[18] cars,[19] and closed containers[20] if the applicant owns or rents the property. The fact that a surveillance technique does not impinge on the "right to exclude others" has also been used to allow police to peer into a home through a window[21] and take photographs of a home from airspace that is of a high enough altitude to be considered "public".[22] Convincing a person with common authority over a home to allow a police search has also been used to negate any reasonable expectation of privacy of other occupants of the home,[23] as has undercover recordings of conversations inside the home.[24] The fact that police had a "right" to be

---

[16] *Ibid* at 351.

[17] See Kerr, "Fourth Amendment", *supra* note 6 at 809, 815. It is notable, however, that there are exceptions such as the "open fields doctrine". As the Court held in *Oliver v United States*, 466 US 170 (1984) at 183-84, "in the case of open fields, the general rights of property protected by the common law of trespass have little or no relevance to the applicability of the Fourth Amendment."

[18] Although the Court recognized Fourth Amendment rights in *Silverman v United States*, 365 US 505, subsequent jurisprudence has used property concepts to narrow the application of the Fourth Amendment in living spaces. See *United States v Botelho*, 360 F Supp 620 at 624 (1973) (concluding that "whether a tenant retained Fourth Amendment rights in a rented apartment depended on whether he had a right to occupy the premises under state property law"); *Stoner v California*, 376 US 483 (1964) at 489 (concluding that the Fourth Amendment applies so long as the renter complies with the rental contract); *United States v Dorais*, 241 F 3d 1124, 1128 (9th Cir 2001) (stating that "a defendant has no reasonable expectation of privacy in a hotel room when the rental period has expired and the hotel has taken affirmative steps to repossess the room").

[19] See *United States v Baker*, 221 F 3d 438 at 442 (3d Cir 2000) determining that those who have consent to borrow a vehicle have a reasonable expectation of privacy in the vehicle. The Fourth Amendment does not, however, apply to those later discovered to have been driving a stolen car (see *United States v Sholola*, 124 F 3d 803 at 815 (7th Cir 1997). Similarly, a person driving a rental car without their name on the contract has no Fourth Amendment rights in the vehicle. See *United States v Wellons*, 32 F 3d 117 at 119 (4th Cir 1994).

[20] See *United States v Ross*, 456 US 798 (1982). See also *United States v Lyons*, 992 F 2d 1029 at 1031 (10th Cir 1993) where the Court concluded that possession of a stolen computer hard drive did not attract a reasonable expectation of privacy because the defendant did not own the hard drive.

[21] See *Kyllo v United States*, 121 S Ct 2038 at 2042 (2001); *California v Ciarolo*, 476 US 207, at 213 (1986). Police have also been allowed to use a flashlight while conducting such searches. See *United States v Dunn*, 480 US 294 at 305 (1987).

[22] See *Florida v Riley*, 488 US 445 at 451 (1989).

[23] See *United States v Matlock*, 415 US 164 at 171 (1974).

[24] See *United States v White*, 401 US 745 at 753-54 (1971).

in the home rendered the Fourth Amendment inapplicable.[25] A similar property-centric understanding of the Fourth Amendment has been used to determine that seizures are not seizures if police only make copies of the original.[26]

This focus on the "right to exclude" led to the adoption of a legal doctrine which has significantly impacted the Court's ability to govern digital technologies: the third-party doctrine. This doctrine holds that when people voluntarily provide information to a third-party, they are no longer able to claim a reasonable expectation of privacy in the information provided.[27] This applies "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[28] As a result, the Court has concluded that there is no reasonable expectation of privacy in personal information surrendered to a bank,[29] phone company records of outgoing calls,[30] or loan applications.[31] Lower courts have also used this rationale to uphold subpoenas issued for records pertaining to medical history,[32] auditors and accountants,[33] and trustees in bankruptcy.[34]

The Court has used similar reasoning in the digital privacy context.[35] In *United States v Knotts*[36] and *United States v Karo*,[37] the Court considered two instances where beepers were surreptitiously planted to track a defendant's movements. In *Knotts*, the container in which the

---

[25] *Ibid*.
[26] See *United States v Thomas*, 613 F 2d 787 at 793 (10th Cir 1980) (concluding that police did not "seize" the defendant's documents when they photocopied them as photocopying does not meaningfully affect the owner's possession of the originals) and *United States v Gorshkov*, No CR00-550C, 2001 (WD Washington, 23 May 2001) (copying electronic data is not a seizure).
[27] See *United States v Miller*, 425 US 435 (1976).
[28] *Ibid* at 443.
[29] See generally *Miller*, *supra* note 27.
[30] See *Smith v Maryland*, 442 US 735 (1979).
[31] See *United States v Payner*, 447 US 727 (1980).
[32] See *Webb v Goldstein*, 117 F Supp 2d 289 (EDNY 2000).
[33] See *Wang v United States*, 947 F 2d 1400, 1403 (9th Cir 1991).
[34] See *In re Kufkin*, 255 BR 204, 211 (Bankr. ED Tenn 2000).
[35] The Court's more recent jurisprudence will be discussed in detail below in Part I(b).
[36] 460 US 276 (1983).
[37] 468 US 705 (1984).

beeper was planted never entered a "constitutionally protected zone" such as a home. As a result, the defendant did not have a reasonable expectation of privacy despite the beeper tracking his vehicles' movements over an extended period of time.[38] In *Karo*, however, the fact that a similarly planted beeper tracked some activity inside a home attracted a reasonable expectation of privacy.[39] The property-based approach again subjugated the normative aspect of the reasonable expectation of privacy test.

The Court employed similar reasoning in *Kyllo v United States*.[40] The police had used a thermal imaging device to detect infrared radiation on the defendant's house. Measuring the infrared radiation emitted by an object allows police to detect the temperature of the surface of an object. The high temperature emitted by the exterior of the house provided necessary grounds to believe that the defendant was operating a marijuana grow-op in his basement.[41] The Court found that the activity qualified as a search because it revealed "information regarding the interior of the home that could not otherwise have been obtained without physical intrusion."[42] As one author explains, "[j]ust as *Knotts* and *Karo* measure the intrusiveness of tracking devices compared to the bench mark of visual surveillance, *Kyllo* measures the intrusiveness of sense-enhancing devices directed at the home compared to the traditional benchmark of physical intrusion."[43]

Although the Court's decision in *Katz* had revolutionary promise, it resulted in courts applying rigid property concepts to a variety of privacy claims, including to new technologies, without focusing on the nature of the privacy inherent in the item searched.[44] As Orin Kerr

---

[38] See *Knotts*, *supra* note 36.
[39] See *Karo*, *supra* note 37.
[40] *Supra* note 21.
[41] *Ibid* at 29.
[42] *Ibid*.
[43] See Kerr, "Fourth Amendment", *supra* note 6 at 835.
[44] *Ibid* at 838. It is notable that at the time Kerr was writing this rationale was also used to negate any reasonable expectation of privacy in stored email records held by Internet Service Providers. See *Guest v Leis*, 255 F 3d 325 at 336 (6th Cir 2001).

maintains, the judicial development and application of the Fourth Amendment suggests that "courts generally do not engage in creative normative inquiries into privacy and technological change when applying the Fourth Amendment to new technologies."[45] He continues, "[f]or better or for worse, courts have tended to apply the same property-based principles…they have applied elsewhere."[46] This in turn brings into question whether the American judiciary is willing to navigate the complex legal terrain of digital privacy.

(b) Recent Jurisprudence

Despite the Court's historical hesitation to use the Fourth Amendment to regulate digital technologies, three of its recent decisions have restricted police powers to use or search digital technologies in the investigative process.[47] In each case, it is evident that the Court fully understood the operation of the relevant digital technology and its privacy implications. As I contend below, it is in part because of a robust intervener process that the Court is able to understand complex digital technologies. Unfortunately, however, the majority of the Court still shows a reluctance to abandon its focus on property concepts which inhibits its ability to provide more determinate and principled rules.

(i) United States v Jones[48]

The police installed a GPS device on the bumper of the defendant's vehicle and monitored the defendant over a four-week period. The Court's earlier decision in *Knotts* had found that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[49] The Court in *Jones* distinguished *Knotts* by

[45] See Kerr, "Fourth Amendment", *supra* note 6 at 831.
[46] *Ibid*.
[47] The following three cases were the first dealing with a major technological tool used by police since 2001. See Murphy, "Politics of Privacy", *supra* note 6 at 490 citing *Kyllo*, *supra* note 21 as the last such case.
[48] 132 S Ct 945 (2012).
[49] See *Knotts*, *supra* note 36 at 281.

observing that Mr. Knotts had unwittingly, but voluntarily, placed a bugged container into his vehicle.[50] In *Jones*, the police physically intruded onto the property of Mr. Jones to attach the GPS device. This intrusion on a property interest automatically engaged the Fourth Amendment.[51] As a strict application of the property-based conception of the Fourth Amendment applied in this case, the majority refused to engage with whether the *Katz* conception of the Fourth Amendment would lead to the same result.[52]

Strong concurring judgments from Justices Sotomayor and Alito recognized that a property-centric approach could not govern many new forms of digital tracking.[53] As such, they contended that the reasonable expectation of privacy test from *Katz* should also be applied to assess whether none-physically intrusive forms of tracking were consistent with the Fourth Amendment.[54] The *Katz* test was more appropriate as it addressed the central concern with use of GPS tracking: whether its inexpensive, precise, and comprehensive tracking capabilities attracted a reasonable expectation of privacy.[55] The *Katz* test also provided a means to oppose the impending argument that GPS records from a telephone service provider were third-party documents for which all reasonable expectation of privacy had been abandoned. Both Justices observed that the application of the third-party doctrine would need to be reconsidered in the digital age given the lack of real choice users have in disclosing information about their use of digital devices.[56]

(ii) Riley v California[57]

[50] See *Jones*, *supra* note 48 at 951-52.
[51] *Ibid*.
[52] *Ibid* at 957.
[53] *Ibid* at 955, 961-64. Justice Sotomayor conceded that the property-centric approach was sufficient to decide the case. However, if the GPS device had been remotely activated, the property centric approach would not apply.
[54] *Ibid* at 955.
[55] *Ibid* at 955-56 citing *United States* v *Cuevas-Perez*, 640 F 3d 272 at 285 (2011).
[56] *Ibid* at 957, 963-64.
[57] 134 S Ct 2473 (2014).

Upon arresting the defendant for possession of concealed and loaded firearms, the police searched his cell phone incident to arrest.[58] The state argued that searching digital data was necessary to ensure officer safety and to preserve evidence.[59] The Court observed that as data on a phone does not directly threaten officer safety, the first rationale for allowing searches incident to arrest was inapplicable.[60] Although arrestees might call for backup, the lack of instances where this occurred resulted in such circumstances being more appropriately governed by the doctrine permitting searches in exigent circumstances.[61] As for the need to preserve evidence, the Court was aware of potential remote or programmed wiping of a phone,[62] as well as the possibility of data becoming encrypted upon the phone being locked.[63] It was also aware that the data will be extraordinarily difficult to access without the cell phone's password.[64] The Court further observed that turning a phone off, removing its battery, and/or placing the phone in a Faraday Bag are potential responses to prevent deletion of data.[65] Although the Court correctly recognized that these techniques do not provide a "complete answer", it concluded that these options provide a "reasonable response" to concerns about preserving evidence.[66]

With respect to the relevant privacy interests, the Court recognized that modern cellular phones implicate privacy concerns in a way that is quantitively and qualitatively different from other physical searches.[67] As the Court observed, comparing a search of a cell phone to other physical containers "is like saying a ride on horseback is materially indistinguishable from a flight

[58] *Ibid* at 2480.
[59] *Ibid* at 2485-86.
[60] *Ibid*.
[61] *Ibid*.
[62] *Ibid* at 2486.
[63] *Ibid*.
[64] *Ibid* at 2486-87.
[65] *Ibid*.
[66] *Ibid*.
[67] *Ibid* at 2488.

to the moon."[68] Although the accused has a reduced expectation of privacy upon arrest, this could not be used to deny the accused all Fourth Amendment protections.[69] Relying upon its previous jurisprudence prohibiting searches of homes incident to arrest, [70] the Court noted that "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house."[71] As a result, the Court prohibited warrantless cell phone searches incident to arrest unless conducted in exigent circumstances.[72]

(iii) Carpenter v United States[73]

The police arrested several men for their involvement in a series of robberies. During the interrogation of one of the arrestees, police received a confession as well as the cell phone number of the petitioner, Mr. Carpenter, who the arrestee claimed was involved in the robberies. The police used his phone number to access Mr. Carpenter's cell site records. As the Court observes, cell phones perform their functions by connecting to and receiving signals from radio antennas known as "cell sites." Every time a phone connects to a cell site—which modern cell phones do multiple times per minute[74]—a time stamped record is generated. These records are typically stored by service providers for business purposes. Depending on the number of cell towers in an area, these time stamps can provide a detailed record of a person's movements. In *Carpenter*, the information accessed allowed the police to receive an average of 101 location notifications per day.[75]

Applying the third-party doctrine, the lower courts concluded that the defendant did not have a reasonable expectation of privacy in cell site information as the petitioner had willingly

[68] *Ibid*.
[69] *Ibid*.
[70] *Ibid* at 2491 citing *United States v Kirschenblatt*, 16 F 2d 202 (1926) at 203.
[71] *Ibid*.
[72] *Ibid* at 2495.
[73] 16 S Ct 402 (2018).
[74] *Ibid*, opinion of Chief Justice Roberts at 17 noting that even the most mundane updates will result in cell site location data being generated.
[75] *Ibid* at 1-4.

given the information over to his service provider.[76] In overturning this ruling, the majority recognized that the digital data at issue did not "fit neatly" into its existing jurisprudence.[77] If bank, medical, and call history records could be accessed by the state because they were revealed to a third party, then why not Mr. Carpenter's cell phone data? The Court distinguished its prior holdings by appealing to the qualitatively different nature of the information revealed.[78] In its view, the evidence suggested that cell phone data tracking could reveal location data analogous to an ankle monitor used on many parolees.[79] It also ensured that the tracking need not start upon police developing any suspicion that the defendant committed a crime.[80] For these reasons, the Court refused to apply the third-party doctrine,[81] although it warned that its ruling would not necessarily apply in other instances such as real-time tracking of cell phones or "tower dumps".[82]

In dissent, Justice Kennedy (Justices Thomas and Alito concurring)[83] extended the third-party doctrine to cell phone site data.[84] They justified this extension because cell phone location data could only reveal, based on current technology, "the location of a cell phone user within an area covering between around a dozen and several hundred city blocks."[85] This number is much less precise in rural areas.[86] Although the majority was aware of the capacity of current technology, it was also aware that the technology was rapidly progressing and would likely be more analogous to GPS tracking in the near future.[87] The minority was not, however, willing to consider any future

[76] See *Carpenter v United States*, 819 F 3d 880 (2016).
[77] See *Carpenter*, *supra* note 73 (Opinion of Chief Justice Roberts at 7).
[78] *Ibid* at 11, 15.
[79] *Ibid* at 13.
[80] *Ibid* at 17-18.
[81] *Ibid*.
[82] *Ibid*. A "tower dump" involves "a download of information on all the devices that connected to a particular cell site during a particular interval."
[83] Each wrote separate opinions but concurred also in Justice Kennedy's decision.
[84] See *Carpenter*, *supra* note 73 at 2 (Opinion of Justice Kennedy).
[85] *Ibid* at 4.
[86] *Ibid*. Justice Kennedy concludes that the information could be up to 40 times less precise.
[87] *Ibid* (majority opinion at 14-15).

development of GPS technology in its decision.[88] The limited insights derived from current cell site data resulted in an insufficient degree of tracking to distinguish the privacy interests from the Court's previous precedents.[89]

(c) Revisiting the Institutional Capacity of Courts

Justice Alito, writing for himself and three others in *Jones*, endorsed Kerr's view that "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."[90] He affirmed this view in *Riley*, adding that "it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment."[91] Justice Sotomayor, writing for herself in *Jones*, took a contrasting position. In her view, it is necessary to guard against "entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse."[92] The divergent views on the bench beg the question: should American courts be entrusted with the complex task of governing digital privacy?

The first consideration inadequately addressed in the literature is whether courts, and in particular the Supreme Court, consistently misunderstands novel and complex technologies. In my view, the existing literature has not proven that appellate courts have significant difficulty understanding complex technologies. Although courts of appeals have at times misunderstood digital technologies,[93] there are many other instances where an appeal court corrected a factual misunderstanding.[94] The above review of the Court's three most recent digital privacy cases also

[88] *Ibid* (reasons of Justice Kennedy at 19) citing *Ontario v Quon*, 560 US 746 at 759 (2010).
[89] *Ibid* at 18-19.
[90] See *Jones*, *supra* note 48 at 964 citing Kerr, "Fourth Amendment", *supra* note 6 at 805-06.
[91] See *Riley*, *supra* note 57 at 2497-98. See also *Carpenter*, *supra* note 72 at 27.
[92] See *Jones*, *supra* note 48 at 956.
[93] See Kerr, "Response", *supra* note 6 at 785-86 citing *Carey*, *supra* note 11; *Maxwell*, *supra* note 11; *Simons*, *supra* note 11.
[94] See Solove, "Fourth Amendment", *supra* note 6 at 772.

shows a general appreciation of the applicable digital technologies which, to my knowledge, has not received cogent academic criticism. This is consistent with the observation that American appellate courts are typically capable of updating gaps in trial court records with respect to digital technologies.[95]

An overview of the records of the three most recent Supreme Court cases provides some insight into the relative competence of the Court to understand digital technologies. Despite suggestions that appellate courts rarely receive intervener briefs,[96] these cases suggest otherwise. In *Carpenter*, for instance, there were fifteen *amicus* briefs in support of the defendant, four in support of the government, and one neutral brief.[97] Including the petitioner and respondent briefs, the Supreme Court was informed by twenty-two separate briefs when making its ruling.[98] In *Riley*, the Court received ten *amicus* briefs in support of the defendant, two in support of the government, and one neutral brief.[99] The Court in *Jones* similarly had twelve *amicus* briefs.[100] In addition to the volume of submissions, it is important to note that interveners tend to write long factums prefaced with lengthy descriptions of the relevant technology. A thirty-page *amicus* brief with ten or more pages devoted to explaining the relevant technology was not an uncommon finding.[101]

The review of the Court's recent jurisprudence nevertheless bolsters the conclusion that strong *stare decisis* norms restrict the Court's ability to respond to digital privacy concerns. Despite calls by various Supreme Court Justices for a reconsideration of the application of the

---

[95] *Ibid*.
[96] See Kerr, "Fourth Amendment", *supra* note 6 at 879.
[97] American Bar Association, "16-402" (26 January 2018), online: <https://www.americanbar.org/groups/public_education/publications/preview_home/2017_2018_briefs/16-402/>.
[98] *Ibid*.
[99] See Electronic Privacy Information Centre, "Riley v California", online: <https://epic.org/amicus/cell-phone/riley/>.
[100] See Electronic Privacy Information Centre, "United States v Jones", online: <https://epic.org/amicus/jones/>.
[101] For a good example, see *Carpenter v United States*, Brief for Electronic Frontier Foundation et al., *supra* note 96. See also Solove, "Fourth Amendment", *supra* note 6 at 772 citing *United States v Bach*, 310 F 3d 1063 (8th Cir 2002).

third-party doctrine to digital technologies,[102] the Court has only moved its position slightly. Although the Court in *Carpenter* imposed a warrant requirement for expansive searches of cell phone site location data, it also cautioned that its decision should be interpreted narrowly.[103] The third-party doctrine will therefore likely continue to apply to significant amounts of digital data. Barring Congress providing increased protections, many of the most common forms of digital communications will therefore go unregulated.

There are at least three possible explanations for why the Court has struggled to adapt the Fourth Amendment to the digital age. The first concerns the scope of the Fourth Amendment. As the dissent in *Carpenter* observes, the text of the Fourth Amendment protects the right of the people to be secure in "*their* persons, houses, papers and effects".[104] Applying the Fourth Amendment to third-party records arguably reads out the word "their".[105] As Justice Alito concludes, there is no evidence that the founders intended the Fourth Amendment to apply to third-party subpoenas to provide evidence.[106] Instead, the Fourth Amendment arose from a general disdain for writs of assistance which permitted searches of virtually any property.[107] The response was to protect particular places and things, "persons, houses, papers, and effects", a response that seems ill-suited to address digital privacy concerns. Although there is room to disagree with this "originalist" understanding of the Fourth Amendment, its influence on the Court has proven to be at least a partial barrier to recognizing privacy rights in many common uses of digital data.

The second reason relates to the structure of the Fourth Amendment. A finding that an activity constitutes a "search or seizure" typically requires the government to obtain a warrant

[102] See *Jones*, *supra* note 48 at 957, 963-64.
[103] See *Carpenter*, *supra* note 73 (opinion of Chief Justice Roberts at 17-18).
[104] *Ibid* (reasons of Justice Thomas at 12; reasons of Justice Alito at 19-20).
[105] *Ibid*.
[106] *Ibid* (reasons of Justice Alito at 11-12).
[107] For a history see William Stuntz, "The Substantive Origins of Criminal Procedure" (1995) 105 Yale Law Journal 393 at 404-09.

based on probable cause. Not only does the warrant requirement provide little flexibility when considering what prerequisites strike an appropriate balance between law enforcement and privacy interests,[108] the judicial remedy following such a breach has historically been all or nothing: exclusion of evidence.[109] It is only reasonable for a court, faced with a relatively non-serious digital privacy breach, to attempt to avoid imposing a high threshold for issuance and then excluding evidence—which often results in an acquittal—on Fourth Amendment grounds.[110]

Finally, it may be that the Court is partisan and therefore unwilling to respond flexibly to the challenges of governing digital privacy. Several studies have shown that appellate courts, and especially the Supreme Court, are rigidly divided along partisan lines.[111] This may explain aspects of the Court's approach to privacy, particularly its controversial "third-party" doctrine. It may also explain the significant deference Justice Alito and others have shown to Congress in the digital privacy context.[112]

The latter explanation may nevertheless have limited staying power. In many of the Court's decisions, "privacy friendly" rulings have resulted from the property-centric understanding of the Fourth Amendment.[113] Even in *Carpenter*, Justice Gorsuch was able to apply the property-centric approach to find that people maintain a reasonable expectation of privacy in cell site records.[114]

---

[108] See Daniel Solove, *Nothing to Hide: The False Trade-off between Privacy and Security* (New Haven: Yale University Press, 2011) at 139-42; Christopher Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* (Chicago: University of Chicago Press, 2007) at 29-30.
[109] *Ibid*. As will be discussed in more detail in the following Chapter, the American exclusionary rule has become less stringent in recent years.
[110] *Ibid*.
[111] See Cass Sunstein and Thomas Miles, "Do Judges Make Regulatory Policy? An Empirical Investigation of Chevron" (2006) 73 University of Chicago Law Review 823; William Eskridge and Lauren Baer, "The Continuum of Deference: Supreme Court Review of Agency Statutory Interpretations from Chevron to Hamdan" (2008) 96 Georgetown Law Journal 1083; Rick Noack, "America's Supreme Court Picks are Highly Politicized: They Don't Have to be that Way" *Washington Post* (February 1 2017); Geoffrey Stone, "Our Politically Polarized Supreme Court?" *The Huffington Post* (November 25 2014); Adam Liptak, "The Polarized Court" *New York Times* (May 10 2014).
[112] *Supra* notes 90-91.
[113] See for instance *Kyllo*, *supra* note 21; *Jones*, *supra* note 48; *Carpenter*, *supra* note 73 (reasons of Justice Gorsuch).
[114] See *Carpenter*, *supra* note 73 (reasons of Justice Gorsuch).

As such, it may be that privacy rules are an exception to the general partisanship of the Court, as privacy cuts across party lines. Any argument about the impact of judicial partisanship in American courts should therefore be approached with caution.

II. Congressional Capacity to Govern Digital Technologies

As with the Canadian Parliament, Congress has faced significant challenges passing efficient, coherent, and balanced criminal procedure rules in the digital privacy context. As I contend below, Congress has been relatively efficient in responding to the challenges of governing digital privacy, although its legislation does have notable gaps. More importantly, Congress' rules frequently fail to provide for a meaningful balance between privacy and security interests and at times succumb to majoritarian and lobbyist interests.

(a) Congress as Privacy Leaders or Stragglers?

In *Olmstead v United States*,[115] the police had tapped several telephone lines running between the defendant's homes and offices. The majority of the Court rejected the defendant's claim that the wiretapping constituted a "search" under the Fourth Amendment. As Chief Justice Taft explained, there was no search because "[t]here was no entry of the houses or offices of the defendant."[116] In his dissent, Justice Brandeis rejected this property-based view of the Fourth Amendment. In his view, privacy mattered, not property.[117] Although the majority originally failed to regulate wiretapping, the Court reversed thirty-nine years later in *Katz* and followed the path set out by the Brandeis minority in *Olmstead*. This history illustrates that courts are capable of constitutionalizing law enforcement practices pertaining to new technologies.[118] As the Court

[115] 277 US 438 (1928).
[116] *Ibid* at 464.
[117] *Ibid* at 478.
[118] See Kerr, "Fourth Amendment", *supra* note 6 at 839 citing Ken Gormley, "One Hundred Years of Privacy" (1992) Wisconsin Law Review 1335 at 1363; Lawrence Lessig, *Code and Other Laws of Cyber Space* (Harvard: Basic Books, 1999) at 116-18; Ric Simmons, "Can Winston Save Us from Big Brother? The Need for Judicial Consistency in

reversed itself in *Katz*, scholars argue that it is reasonable to expect that it can adjust its jurisprudence to meet the challenges of the digital age.[119]

This line of argument ignores considerable legislative efforts to regulate wiretapping.[120] Before *Olmstead* was decided in 1928, over half of the states had adopted regulations to govern wiretapping.[121] The Federal government had also briefly regulated wiretapping near the end of World War I.[122] Six years after *Olmstead* was decided, Congress passed the *New Deal's Communications Act* which included a provision prohibiting wiretapping.[123] By the time *Katz* was decided in 1967, thirty-six states had joined Congress in regulating wiretapping.[124] These responses were nevertheless viewed as unsatisfactory,[125] prompting Congress to pass its comprehensive *Federal Wiretap Act*[126] (hereafter referred to as "Title III") one year after the Court handed down its decision in *Katz*.[127]

Since Title III was passed, Fourth Amendment decisions regulating wiretapping have been rare.[128] Courts generally refused to use the Fourth Amendment to strike down provisions in Title III.[129] Even in cases of clear gaps the courts have generally refused to regulate the practice of

---

Regulating Hyper-Intrusive Searches" (2003) 55 Rutgers Law Review 547 at 562-64; Scott Sundby, "Everyman's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?" (1994) 94 Columbia Law Review 1751 at 1756; Fred Cate, "The Changing Face of Privacy Protection in the European Union and the United States" (1999) 33 Indiana Law Review 173 at 199; Anjali Singhal, "The Piracy of Privacy? A Fourth Amendment Analysis of Key Escrow Cryptography" (1996) 7 Stanford Law and Policy Review 189 at 192.

[119] *Ibid*.

[120] See Kerr, "Fourth Amendment", *supra* note 6 at 839-40.

[121] For a review of the applicable legislation at the time, see *Berger v New York*, 388 US 41 at 45 (1967).

[122] See Kerr, "Fourth Amendment", *supra* note 6 at 841 citing the Law of October 29, 1918, ch 197, 40 Stat 1017.

[123] *Ibid* at 845. The provision was later codified as 47 USC § 605.

[124] See *Berger*, *supra* note 121 at 48 (note 5).

[125] See President Johnson's Crime Commission, "President's Commission on Law Enforcement and Administration of Justice, the Challenge of Crime in a Free Society" (1967) at 202-03.

[126] 18 USC § 2520.

[127] The Act was passed in 1968.

[128] See Kerr, "Fourth Amendment", *supra* note 6 at 850.

[129] *Ibid* at 851 citing *United States v Sklaroff*, 506 F 2d 837 at 840 (5th Cir 1975); *United States v Ramsey*, 503 F 2d 524 at 526-31 (7th Cir 1974); *United States v Martinez*, 498 F 2d 464 at 467-68 (6th Cir 1974); *United States v Tortorello*, 480 F 2d 764 at 771-75 (2d Cir 1973); *United States v Bobo*, 477 F 2d 974 at 978-82 (4th Cir 1973); *United States v Whitaker*, 474 F 2d 1246 at 1247 (3d Cir 1973); *United States v Cafero*, 473 F 2d 489 at 493-501 (3d Cir 1973); *United States v Cox*, 449 F 2d 679 at 683-87 (10th Cir 1971).

wiretapping. The judicial refusal to extend wiretapping law to cordless phones is exemplary.[130] The anomaly arising from Title III applying to corded but not cordless phones was passively accepted by several courts.[131]

Congress has also been relatively efficient in areas other than wiretapping law. In response to the Court's decision in *Smith v Maryland*[132] to remove Fourth Amendment protections for pen register and trap and trace devices, Congress responded seven years later by enacting the *Pen Register and Trap and Trace Devices Act*.[133] Congress also acted on its own initiative in 1974 with its passage of the *Privacy Act*,[134] which gave citizens the right to check information about themselves in federal databases. Similarly, Congress passed the *Cable and Communication Act*[135] in 1984 to place limits on the disclosure of user's subscriber information to cable services, as well as the *Video Privacy Protection Act*[136] to place limits on access to an individual's movie rental history. Further, Congress passed privacy protections for stored emails and internet communications in 1986 in the *Electronic Communications Privacy Act*,[137] long before email and the internet had become dominant modes of communication.[138] The *ECPA* has been amended thirteen times since its enactment.[139]

Although Congress responded to *Olmstead* six years after the Court found no reasonable expectation of privacy in police use of wiretapping devices, it is notable that the law was widely

---

[130] *Ibid* at 852 citing *McKamey v Roach*, 55 F 3d 1236, at 1238-40 (6th Cir 1995); *Tyler v Berodt*, 877 F 2d 705 at 707 (8th Cir 1989); *United States v McNulty (In re Askin)*, 47 F 3d 100 at 104-106 (4th Cir 1995); *United States v Smith*, 978 F 2d 171 at 177-81 (5th Cir 1992); *Price v Turner*, 260 F 3d 1144 at 1149 (9th Cir 2001).
[131] *Ibid*.
[132] *Supra* note 30.
[133] 18 USC §§ 3121-27 [*PRA*].
[134] 5 USC § 552a.
[135] 47 USC § 551 [*CCA*].
[136] 18 USC § 2710 [*VPPA*].
[137] 18 USC § 2701 [*ECPA*].
[138] See also Kerr, "Fourth Amendment", *supra* note 6.
[139] *Ibid*. Kerr observed in 2004 that the act had been amended 11 times, and two other substantive amendments have occurred since. See United States Department of Justice, "Electronic Communications Privacy Act of 1986 (ECPA)", online: <https://www.it.ojp.gov/PrivacyLiberty/authorities/statutes/1285>.

criticized for being both overprotective and under protective.[140] It was overprotective because it did not allow much wiretap evidence to be used in court, and under protective because it allowed all wiretapping so long as the evidence was not used in court.[141] Congress' response to the Court's decision in *Katz* was exactly as it sounds: a response to a judicial ruling.[142] And as Daniel Solove observes, since *Katz*, only three substantial legislative responses have followed, and none during the period from 1986 until 2001: a period where digital technologies were rapidly advancing.[143]

The *ECPA* also resulted in a number of arbitrary distinctions which developed as technology progressed. For instance, whether the Act provides privacy protections may turn on whether an individual accessed a website via an iPad as opposed to a desktop computer; whether a video recording has audio; or whether a caller uses a cordless phone.[144] Many other statutes are understandable only because Congress provides a vague "catch all" phrase that courts may interpret flexibly when needed.[145] As opposed to reacting to new developments in technology, Erin Murphy concludes that Congress' privacy legislation is by far more commonly prompted by some external event such as a Supreme Court case,[146] a newspaper story,[147] or a tragic incident.[148]

---

[140] See Crime Commission, "Free Society", *supra* note 125 at 202-03.
[141] *Ibid*.
[142] See Solove, "Fourth Amendment", *supra* note 6 at 769-71.
[143] *Ibid*. It is also notable that Solove observes that the last amendment was rushed through Congress in seven weeks as a response to the terrorist attacks of 9/11. See Beryl Howell, "Seven Weeks: The Making of the USA-PATRIOT Act" (2004) 72 George Washington Law Review 1145. The unique circumstances of 9/11, however, make this type of rushed response the exception.
[144] *Ibid* citing Kenneth Bamberger & Dierdre Mulligan, "Privacy on the Books and on the Ground" (2011) 63 Stanford Law Review 247 at 257; Lior Jacob Strahilevitz, "Reunifying Privacy Law" (2010) 98 California Law Review 2007 at 2034 (note 108).
[145] *Ibid*.
[146] *Ibid* at 498 noting that *Miller, supra* note 27 prompted passage of the *Right to Financial Privacy Act*, 12 USC §§ 3401-3422 [*RFPA*]; *Katz*, *supra* note 2 prompted passage of *Title III*, *supra* note 126; *Zurcher v Stanford Daily,* 436 US 547 (1978) prompted the passing of the *Privacy Protection Act*, 42 USC § 2000aa [*PPA*].
[147] *Ibid* noting that "an article [revealing how even the video rental records of Supreme Court Justice Nominee, Robert Bork, could readily be obtained] inspired the VPPA… Likewise, an article in *Parade* magazine about student records inspired Senator Buckley, who entered the article into the *Congressional Record,* to push for the passage of FERPA."
[148] *Ibid* noting that "the *DPPA* was passed after it came to light that actress Rebecca Schaeffer had been murdered by a stalker who had easily obtained her address from the Department of Motor Vehicles."

There are also various areas where Congress has failed to act promptly and, in some cases, failed to provide any privacy protections.[149] Global Positioning Systems (GPS) technologies; facial recognition systems; tracking devices; key logging devices; and sensory enhancement technologies are exemplary.[150] Congress has also failed to regulate video surveillance of citizens. This is ironic because, as Solove observes, the *Foreign Intelligence Surveillance Act* "regulates video surveillance…meaning that the video surveillance of a foreign spy receives more federal statutory protection than that of [an American] citizen."[151]

There are also significant gaps in the law regulating government access to records held by third parties. As one author observes, under the *FCRA* and *RFPA* "there are many situations where financial data is unprotected, such as when the information is held by employers, landlords, merchants, creditors, [and] database companies".[152] The *HIPAA* regulates access to medical records, but only when in the possession of limited third parties (doctors, hospitals, and insurers), which notably excludes personal information found on medical websites.[153] Other third parties in possession of private information about individuals are not regulated at all, "including bookstores, merchants, restaurants, employers, and other businesses."[154]

(b) Coherence of Response

Congress' legislation frequently provides underwhelming privacy protections.[155] The *Stored Communications Act*[156] is illustrative. The *SCA* governs communications that are stored by

[149] See Solove, "Fourth Amendment", *supra* note 6 at 762-65; Murphy, "Politics of Privacy", *supra* note 6 at 498; Sklansky, "Two More Ways", *supra* 6 at 227-28.
[150] *Ibid* at 762-64.
[151] *Ibid* at 764.
[152] *Ibid* at 765.
[153] *Ibid*.
[154] *Ibid*. It is notable that the observations made in this and the two preceding notes were repeated a decade later by Murphy, "Politics of Privacy", *supra* note 6 at 533-34.
[155] See Solove, "Fourth Amendment", *supra* note 6 at 762.
[156] 18 USC § 2701-12 [*SCA*].

third parties such as emails. It also governs state seizure of internet protocol (IP) addresses capable of revealing the identity of those behind online activity.[157] To access such data, the government must only point to "specific and articulable facts showing that there are reasonable grounds" to believe the communications are "relevant" to its criminal investigation.[158] The *SCA* also does not provide for exclusion of evidence as a remedy for a breach.[159] As such, the protections provided by the *SCA* are minimal and, in case of a breach, courts are not able to provide an effective remedy.[160] In the criminal law context, this lack of effective remedy does not incentivize defendants to contest even egregious breaches of privacy.[161]

The *Pen Register Act*[162] provides another prominent example. It regulates government use of pen registers and trap and trace devices. The court order required to obtain such information requires only that "the information likely to be obtained by such installation and use is relevant to an ongoing investigation."[163] This not only falls far short of the default probable cause standard provided by the Fourth Amendment, courts have virtually no discretion to deny a government application.[164] The *PRA* also fails to provide for the possibility of exclusion of evidence if a breach occurs.[165] As David Sklansky persuasively argues, the *PRA* "doesn't sound like a regime aimed at

[157] See Solove, "Fourth Amendment", *supra* note 6 at 755. The records available include "[i]nternet session times, addresses, phone numbers, and billing data."
[158] See *Stored Communications Act*, *supra* note 156, s 2703(d). It is notable that this lower standard does not apply to unread email or email that has been stored for fewer than 180 days. See sections 2510(17) and 2703(b).
[159] See Solove, "Fourth Amendment", *supra* note 6 at 755 citing *United States v Kennedy*, 81 F Supp 2d 1103 at 1111 (2000); *United States v Hambrick*, 55 F Supp 2d 504 at 507 (1999).
[160] *Ibid*. As Solove observes at 763, Kerr wrote an article broadly lamenting the fact that exclusion is generally not included as a remedy in federal criminal procedure statutes. See Orin Kerr, "Lifting the 'Fog' of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law" (2003) 54 Hastings Law Journal 805.
[161] See Solove, "Fourth Amendment", *supra* note 6 at 763. It is self-evident that for criminal procedure rules to work, there must be some incentive for defendants to argue that their rights were breached. Exclusion is not the only possible incentive, but Kerr does not explain how other remedies will incentivize litigation.
[162] *Supra* note 133.
[163] *Ibid*, s 3121(a).
[164] *Ibid*, s 3123(a)(1). See also Solove, "Fourth Amendment", *supra* note 6 at 756.
[165] See Solove, "Fourth Amendment", *supra* note 6 at 756.

protecting privacy. It sounds like a regime designed to get the government the information it wants while giving legal cover to telecommunication companies."[166]

The *Patriot Act*[167] provides yet another example. The Act amended the *SCA*, adding within its ambit any "records of session times and durations," "any temporarily assigned network address," and "any credit card or bank account number" used for payment.[168] This greatly expanded the information available to government under the *SCA* all the while keeping the governing threshold the same and without adjusting the possible remedies. The *Patriot Act* also expanded the definition of "pen register" under the *PRA* from "numbers dialed . . . on the telephone line" to all "dialing, routing, addressing, or signaling information."[169] As one author observes, "[t]his expansion means that the [*PRA*] now covers the addressing information on e-mails, Internet Protocol addresses ('IP addresses'), and Uniform Resource Locators ('URLs')."[170] This broadening was again done without increasing the relevant standard or providing exclusion as a possible remedy.

A variety of other statutes passed by Congress follow a similar pattern. The *Right to Financial Privacy Act*,[171] *Fair Credit Reporting Act*,[172] *Family Education Right to Privacy Act*,[173] *Cable Communications Policy Act*,[174] *Video Privacy Protection Act*,[175] and *Health Insurance Portability and Accountability Act*,[176] purport to protect the privacy of those within each Act's

[166] See Sklansky, "Two More Ways", *supra* note 6 at 231.
[167] The full title is the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*, 50 USC § 1801-62 [*Patriot Act*].
[168] *Ibid*, s 2703(c)(2).
[169] *Ibid*, s 3127(3).
[170] See Solove, "Fourth Amendment", *supra* note 6 at 757.
[171] *Supra* note 146.
[172] 15 USC § 1681 [*FCRA*].
[173] 20 USC § 1232g [*FERPA*].
[174] 47 USC § 55 [*CCPA*].
[175] *Supra* note 136.
[176] 29 USC §§ 1181-1183, 42 USC § 300gg [*HIPAA*].

ambit but in reality provide protections as thin as those found in the *PRA*, *SCA*, and *Patriot Act*. In other words, each statute allows information which might be thought to engage a reasonable expectation of privacy[177] to be disclosed upon showing that the information is broadly relevant to an investigation, or some similar standard.[178] These statutes also do not provide an exclusionary remedy in the event of a breach.[179]

In some instances, low standards were kept in place despite legislative proposals to raise issuing standards. Shortly after the Court in *Smith v Maryland*[180] found no reasonable expectation of privacy was engaged by state use of pen register and trap and trace devices,[181] two proposals were made to bring these devices within Title III,[182] another to adopt the probable cause standard,[183] and several other variations on these proposals.[184] All of these efforts failed.[185] Instead, the existing law was passed to serve the interests of telephone companies seeking legal protection for such disclosures.[186] As David Sklansky observes, a similar process unfolded concerning state

---

[177] In the order listed above: bank records, credit records, school records, cable television subscriptions, video rentals, and medical records.
[178] See Solove, "Fourth Amendment", *supra* note 6 at 757-59, 765-66 citing *RFPA*, *supra* note 146, s 3407; *FCRA*, *supra* note 172, ss 1681b(a)(1), 1681f, 1681u; *FERPA*, *supra* note 173, s 1232g(b)(2)(B); *VPPA*, *supra* note 136, s 2710(b)(2)(C); *HIPAA*, *supra* note 176, s 164.512(f)(2). It is notable that the *CCPA*, *supra* note 174, s 551(h)(1) provides a higher standard of "clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case."
[179] For an overview see Solove, "Fourth Amendment", *supra* note 6 at 757-59.
[180] *Supra* note 30.
[181] See Sklansky, "Two More Ways", *supra* note 6 at 231
[182] *Ibid* citing S 1207, 96th Cong, 1st Sess, in 125 Cong Rec 22668 (Aug 3, 1979) (statement of Senator Carl Levin); HR 5285, 96th Cong, 1st Sess, in 125 Cong Rec 25955 (Sept 24, 1979) (statement of Representative Robert Drinan).
[183] *Ibid* citing HR 933, 97th Cong, 1st Sess, in 127 Cong Rec 514, 518 (Jan 19, 1981) (statement of Representative Ted Weiss). Sklansky also notes that in the alternative, "the bill provided that telephone toll records could be accessed by subpoena, but if they were then the telephone customer would need to be notified and given an opportunity to challenge the request in court."
[184] *Ibid* citing *Criminal Code Revision Act of 1981,* HR 1647, 97th Cong, 1st Sess 297-98 (Feb 4, 1981) ("barring installation or use of a pen register without a judicial finding of 'reason for the belief' that the information obtained would be 'relevant to a legitimate criminal or civil investigation'"); *Electronic Surveillance Act of 1984,* HR 6343, 98th Cong, 2d Sess 5-6 (Oct 1, 1984).
[185] *Ibid* at 232.
[186] *Ibid* citing *Hearing on Privacy in Electronic Communications before the Subcommittee on Patents, Copyrights and Trademarks of the Senate Committee on the Judiciary,* 98th Cong, 2d Sess 12 (1984) (statement of HW William Caming, Senior Counsel, AT&T); *1984: Civil Liberties and the National Security State, Hearings before the Sub-committee on Courts, Civil Liberties, and the Administration of Justice of the House Committee on the Judiciary,* 98th Cong, 2d Sess 150 (1984) (testimony of US Magistrate Judge James Carr).

access of metadata, such as "the collection and monitoring of routing information in e-mails and text messages, and the wholesale archiving of the kind of telephone records that pen registers and trap-and-trace devices previously collected much more selectively."[187]

Given the above review, several authors contend that privacy protection from federal statutes is much more likely to turn on whether the information sought is useful to investigations than on widely shared notions of the degree of privacy inherent in the item searched.[188] As Christopher Slobogin concludes in a survey study, data from websites visited, credit card purchases, and pharmacy and bank records are considered much more invasive than a pat-down search and comparable to a car search.[189] Yet, access to one's driving, email, health, and personal credit records are disclosable upon administrative request, while items scoring much lower on the privacy scale, such as video and cable records, require significantly heightened evidentiary requirements.[190]

Erin Murphy explains this lack of effective gathering and weighing of evidence by noting Congress' "extraordinarily piecemeal" enactment of privacy laws.[191] In stark contrast to many other nations' comprehensive privacy regulations, "the United States has largely relied on independent enactments tailored to particular sectors or interests."[192] Nor is a single agency entrusted with overseeing privacy practices in the United States.[193] The result is that it is difficult to discern a single unified theory of privacy from the available legislation.[194] Without an

[187] *Ibid* at 233 citing "Data Mining, Dog Sniffs, and the Fourth Amendment" (2014) 128 Harvard Law Review 691 at 697-98.
[188] See Murphy, "Politics of Privacy", *supra* note 6 at 506.
[189] See Slobogin, *New Government Surveillance*, *supra* note 108 at 184.
[190] *Ibid*.
[191] See Murphy, "Politics of Privacy", *supra* note 6 at 495.
[192] *Ibid* citing Kenneth Bamberger & Dierdre Mulligan, "Privacy on the Books and on the Ground" (2011) 63 Stanford Law Review 247 at 250-51. See also Paul Schwartz, "Privacy and Democracy in Cyberspace" (1999) 52 Vanderbilt Law Review 1609 at 1632-33.
[193] *Ibid* at 496.
[194] *Ibid*.

overarching theory, it is unsurprising that Congress has had difficulties maintaining a consistent approach to privacy protection.[195]

This is not to say that all Federal statutes provide underwhelming privacy protections.[196] For instance, several Federal privacy statutes in fact impose burdens of proof similar to or higher than that provided by the Fourth Amendment. The probable cause standard is required for interceptions[197] and for obtaining warrants to search media offices for evidence of a third-party crime.[198] These requirements are, however, required according to the Court's Fourth Amendment jurisprudence.[199] The *VPPA* also requires a court order to be based on the probable cause standard,[200] as does the IRS Code for non-tax related criminal investigations, with the latter imposing a necessity requirement as well.[201] The *CCPA*'s requirement that court orders be based upon "clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material in the case"[202] provides a standard which is higher than that prescribed by the Fourth Amendment.[203]

Other privacy legislation allows for different types of protections. For instance, several laws allow for issuance of private information via subpoenas but require advance notice to the

---

[195] *Ibid* at 495-99.
[196] For an extensive review, see Murphy, "Politics of Privacy", *supra* note 6 at 515-22.
[197] This legislation, as discussed above, responded to the Court's decisions in *Katz*, *supra* note 2 and *Berger*, *supra* note 121.
[198] See the *PPA*, *supra* note 146 in response to *Zurcher*, *supra* note 146. The police had obtained a search warrant to search the Stanford Daily newspaper office as it had reasonable grounds to be believe that photographic evidence was present in the office. The issue was whether the warrant could provide such authority as the government could just as easily have applied for a subpoena *ducus tecum* to obtain the information. The Court concluded that the warrant procedure was valid, and Congress responded by entrenching the requirements for a warrant to obtain such information in the *PPA*.
[199] See *Katz*, *supra* note 2; *Zurcher*, *supra* note 146.
[200] See Murphy, "Politics of Privacy", *supra* note 6 at 518 citing 18 USC § 2710(b)(3) (2006).
[201] *Ibid* citing 152 IRC § 6103(i)(l)(B) (2006).
[202] *CCPA*, *supra* note 174, § 551(h)(1).
[203] See Murphy, "Politics of Privacy", *supra* note 6 at 518-19.

subject of the disclosure.[204] Such a process ensures that the defendant will have an opportunity to challenge the merits of these (usually third party) disclosures to government.[205] It is notable, however, that these statutes often provide for multiple ways of circumventing these notice requirements in criminal investigations.[206] Notice may, for instance, be delayed until the completion of an investigation or foregone altogether based on law enforcement showing that notice would interfere with the investigation or safety of a person involved therein.[207]

Several Federal statutes also provide restrictions on the use of the data obtained.[208] For example, the *RFPA* restricts the transfer of financial records, requiring notice in the event of a transfer.[209] Similarly, the *Driver's Privacy Protection Act* limits the allowable reasons for disclosing information to other parties or departments.[210] Moreover, the *VPPA* requires destruction of records,[211] as does the *CCPA*, when the information is "no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access."[212] These restrictions on use help ensure that privacy invasions are not perpetuated.

Other federal statutes enhance accountability by requiring state agencies to document and report on its disclosures.[213] Title III requires several reporting requirements for state interceptions of private communications.[214] *FERPA* requires that all requests for access indicate the reason for the request, and provides for a review body to investigate potential violations.[215] The IRS Code

---

[204] *Ibid* at 519 citing the *RFPA*, *supra* note 146, §§ 3405(2), 3406(b), 3407(2), 3408(4)(A); *CCPA*, *supra* note 174, §§ 551(h)(2), 551(c)(1); *VPPA*, *supra* note 136, § 2710(b)(2)(C)(3); *FERPA*, *supra* note 173, § 1232g(b)(2); *PPA*, *supra* note 146, § 2000aa(c).
[205] See Murphy, "Politics of Privacy", *supra* note 6 at 535.
[206] *Ibid* at 520 citing as examples *RFPA*, *supra* note 146, § 3409; *FERPA*, *supra* note 173, § 1232g(b)(l)(J).
[207] *Ibid*.
[208] *Ibid*.
[209] *Ibid*.
[210] *Ibid* at 520-21 citing 18 USC § 2721(c) (1994) [*DPPA*].
[211] *Ibid* citing *VPPA*, *supra* note 136, § 2710(e).
[212] *Ibid* citing *CCPA*, *supra* note 174, § 551(e).
[213] *Ibid* at 526-27.
[214] See Title III, *supra* note 126, § 2519.
[215] See *FERPA*, *supra* note 173, §§ 1232g(b)(4); 1232g(g).

requires, as one author concludes, "compliance with a comprehensive system of administrative safeguards and record keeping requirements".[216] Finally, the *CMPA* requires regular congressional reports and creates a "data integrity board".[217] Recordkeeping requirements are nevertheless much less common in statutes regulating private entity disclosures, such as the *VPPA* (video rental agencies), *FCRA* (credit agencies), and *COPPA* (internet service providers).[218] Moreover, the trend in recent years has been to scale back, if not eliminate, many reporting requirements for both law enforcement and private actors.[219]

These additional protections are not available under the Fourth Amendment. As one author suggests, "[a]lthough the Supreme Court has stated in *dicta* that the Fourth Amendment continues to limit the subpoena power of the government, the Court has rejected Fourth Amendment objections to subpoenas in every case it has decided in modern times."[220] Moreover, courts applying the Fourth Amendment have effectively restricted its application to the moment of the search.[221] The Court's narrow interpretation of the Fourth Amendment thereby ensures that the legislature has exclusive responsibility to regulate these important aspects of digital privacy.

Compliance measures have also been used ineffectively by Congress.[222] Only two federal statutes provide for exclusion of evidence as a remedy for a breach: Title III and the *VPPA*.[223] Title III's exclusionary provision is required by the Fourth Amendment.[224] The reasons behind why the *VPPA* includes exclusion of evidence as a remedy are less clear. As one author speculates, the

---

[216] See Murphy, "Politics of Privacy", *supra* note 6 at 527 citing Stephen Mazza, "Taxpayer Privacy and Tax Compliance" (2003) 51 University of Kansas Law Review 1065 at 1095.
[217] 5 USC §§ 552a(u), 552a(s) (2006) [*CMPA*].
[218] See Murphy, "Politics of Privacy", *supra* note 6 at 527.
[219] *Ibid* citing recent adjustments to the *Privacy Act*, *supra* note 134 and *RFPA*, *supra* note 146 as two prominent examples.
[220] *Ibid* citing Wayne Lafave, *Search and Seizure*, 4th ed (2004) at 4.13(a).
[221] *Ibid* at 535.
[222] *Ibid* at 522.
[223] *Ibid*.
[224] See *Katz*, *supra* note 2.

legislative submissions before the *VPPA* was passed had an unusual feature: very limited submissions from law enforcement, none of which commented on the appropriate remedy for breaches.[225] Although Congress heard many examples of abusive police acts undertaken pursuant to the *VPPA*, it is curious that the only statute not constitutionally required to include exclusion of evidence did so when police did not actively oppose such a remedy.[226]

Every other Federal statute governing privacy either explicitly or implicitly provides lesser remedies.[227] Where exclusion is not explicitly rejected, courts have generally found that exclusion is an inappropriate remedy absent a constitutional breach.[228] The statutes instead show a strong preference for civil remedies.[229] This is problematic as such remedies are generally only available if the breach is wilful or deliberate, which excludes the much more likely scenario of negligent or reckless disclosure to or by law enforcement.[230] Where damages are allowed for negligent disclosure, the claims are also minimal given that punitive damages are only available for wilful or deliberate breaches.[231] As I explain in more detail in the next Chapter, it is highly unlikely that such remedies deter law enforcement because they will not incentivize litigation.

(c) Public Choice Theory

Kerr contends that the main advantage for courts vis-à-vis legislatures commonly articulated by public choice theorists—the neutrality of courts—is inapplicable in the criminal

---

[225] See Murphy, "Politics of Privacy", *supra* note 6 at 522-23.
[226] *Ibid*.
[227] For a detailed review, see Murphy, "Politics of Privacy", *supra* note 6 at 523-24.
[228] *Ibid* citing *United States v Elliott*, 676 F Supp 2d 431 at 439 (D Md 2009); *State v Mubita*, 188 P 3d 867 at 874 (Idaho 2008); *United States v Bunnell*, No CRIM.02-13-B-S, 2002 WL 981457 at 4 (10 May 2002); *United States v Davis*, 657 F Supp 2d 630 at 663 (D Md 2009) aff'd 690 F 3d 226 (4th Cir 2012); *United States v Edgar*, 82 F 3d 499 (1st Cir 1996); *Word v United States*, 604 F 2d 1127 at 1129-30 (8th Cir 1979); *United States v Orlando*, 281 E3d 586 at 596 (6th Cir 2002); *Nowicki v Comm'r*, 262 F 3d 1162 at 1164 (11th Cir 2001); *United States v Michaelian*, 803 F 2d 1042 at 1046-48 (9th Cir 1986); *Marvin v United States*, 732 F 2d 669 at 672-73 (8th Cir 1984).
[229] See Murphy, "Politics of Privacy", *supra* note 6 at 524.
[230] *Ibid* at 524-25. As Murphy observes, even where a breach is found, the statutes tend to provide for a variety of defences such as good faith, various doctrines of immunities, or applicable limitation clauses.
[231] *Ibid* at 524.

procedure context,[232] or at least with respect to new technologies.[233] He admits that American legislatures are often subject to lobbyist pressures, as shown by various public choice theorists.[234] However, Kerr maintains that few if any rent seeking actors may be identified in the *criminal procedure* context.[235] Although the police do ask for greater powers and prove highly influential in so doing, such actions, Kerr maintains, are generally in line with legitimate public preferences.[236]

Kerr also rejects the contention that majoritarian politics might negatively influence legislatures when developing privacy rules responding to new technologies.[237] First, he points to a lack of evidence supporting the view that legislatures have no incentive to protect the rights of the accused vis-à-vis majority desire to increase crime control.[238] Even if such evidence existed, Kerr asserts that it would be unlikely to affect rules relating to complex and rapidly changing technologies.[239] As new technologies are generally expensive, they tend to be used by politically powerful groups.[240] These groups, Kerr asserts, will use their political power to defend their interests through the legislative process.[241]

Erin Murphy has persuasively rebutted this view. Kerr's assertion that law enforcement efforts are in line with the "public interest"[242] rings hollow in light of the following conclusion arising from Murphy's detailed study of federal privacy rules: "the degree of protection from law

---

[232] See Kerr, "Fourth Amendment", *supra* note 6 at 884-85.
[233] *Ibid* at 886-87. Although Kerr also raises the potential argument that interstitial judicial rule-making provides a judicial advantage, the many defects in the adversarial process he identifies in the criminal law context address any benefit that might be derived from a judicial approach to creating criminal procedure rules for digital technologies.
[234] *Ibid* at 884-85.
[235] *Ibid*.
[236] *Ibid* at 885.
[237] *Ibid* at 886-87 citing Donald Dripps, "Criminal Procedure, Footnote Four, and the Theory of Public Choice: Or, Why Don't Legislatures Give a Damn About the Rights of the Accused?" (1993) 44 Syracuse Law Review 1079.
[238] *Ibid*.
[239] *Ibid* at 887.
[240] *Ibid*.
[241] *Ibid*.
[242] *Ibid* at 885.

enforcement seems far more likely to turn on whether the information is useful in investigations than it does on widely shared intuitive notions of what is more or less deserving of privacy".[243] In other words, the more useful a piece of information is to law enforcement, the lower the privacy protections the information is likely to receive. This suggests that law enforcement has routine and significant influence on the content of rules regulating privacy, and that its influence does not encourage a principled balancing of privacy and security interests.[244]

The history of the *VPPA* is illustrative. Lobbying by law enforcement was sufficient to ensure that borrowing history from libraries did not receive increased statutory protection, even though video rentals received unusually high protection and the relevant Act was called (up until the final stages) the "Video and Library Privacy Protection Act".[245] Why did the video rental portion of the proposal pass with a high threshold for obtaining records compared to virtually every other privacy statute? Not only was the catalyst for the Act an improper seizure of then-Supreme Court nominee Richard Bork's video rental history, the *VPPA* represents a rare occasion where law enforcement did not provide in-Congress testimony or extensive written submissions on the law.[246] The result was not only a higher governing threshold, but also a rare non-constitutionally required inclusion of an exclusion remedy in a federal privacy statute.

Congress' privacy legislation has also often left the privacy of the poor unprotected or, worse, deliberately exposed for law enforcement and public consumption.[247] For instance, Federal legislation concerning public assistance grants for housing requires that these agencies provide

---

[243] See Murphy, "Politics of Privacy", *supra* note 6 at 506 citing Slobogin, *Privacy at Risk*, *supra* note 108 at 183-84.
[244] *Ibid*.
[245] *Ibid* at 501-02.
[246] *Ibid* at 506 citing the *Video and Library Privacy Protection Act of 1988: Joint Hearing Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H.* Comm. *on the Judiciary and the Subcomm. on Tech. & the Law of the S. Comm. on the Judiciary,* 100th Cong. 123-50 (1989).
[247] *Ibid* at 508.

law enforcement with the address, social security number, and photo of any recipient.[248] The officer need only state that the information "is necessary for the officer to conduct the officer's official duties".[249] Identical provisions exist for welfare recipients.[250] Federal law enforcement agencies actively exploited the availability of this information with its infamous "Operation Talon", a program "designed to mine welfare and housing roles to apprehend persons with outstanding warrants."[251] The program resulted in the arrest of over 10,000 low-income individuals.[252]

Relatedly, those with criminal records (80 to 90 percent of whom are indigent)[253] have their records exposed for public and private consumption.[254] This is possible because increased storage capacities and refined searching techniques make these records available in short order.[255] As digital technologies have made criminal records easy to compile and access, Federal law has in turn made criminal records relevant to a wide range of services including "government benefits, voting rights, student loans, public housing, educational programs, public licenses, and so on."[256] This in turn has created a "thriving private sector industry" which compiles and sells criminal records to public and private parties[257] with very few restrictions.[258] To the contrary, protections

[248] *Ibid* citing 42 USC § 1437z (2006).
[249] *Ibid*.
[250] *Ibid* at 509 citing the *Temporary Assistance to Needy Families Act*, 2 USC § 608(a)(9).
[251] *Ibid* at 510 citing Kaaryn Gustafson, "The Criminalization of Poverty" (2009) 99 Journal of Criminal Law & Criminology 643 at 668-69.
[252] *Ibid* citing Gustafson, "Criminalization of Poverty", *supra* note 251 at 671.
[253] *Ibid*.
[254] *Ibid* at 511 citing James Jacobs and Dimitra Blitsa, "Sharing Criminal Records: The United States, the European Union, and Interpol Compared" (2008) 30 Loyola of Los Angeles International & Comparative Law Review 125 at 142.
[255] *Ibid* citing James Jacobs & Tamara Crepet, "The Expanding Scope, Use, and Availability of Criminal Records" (2008) 11 New York University Journal of Legislation and Public Policy 177 at 180-83.
[256] *Ibid* at 511 (note 115) citing Jacobs and Crepet, "Expanding Scope", *supra* note 255 at 178-79.
[257] *Ibid* citing Jacobs and Crepet, "Expanding Scope", *supra* note 255 at 186 (note 57). As Daniel Solove and Chris Hoofnagle observe in their article "A Model Regime of Privacy Protection" (2006) University of Illinois Law Review 357 at 363, the private sector "provides data to companies for marketing, to the government for law enforcement purposes, to private investigators for investigating individuals, to creditors for credit checks, and to employers for background checks."
[258] *Ibid* citing Jacobs and Blitsa, "Criminal Records", *supra* note 254 at 133.

for Federal social security benefits, driver's licence, and income tax records—benefits that involve a much more diverse socioeconomic class of recipients—receive significantly increased protections such as checks on accuracy of information and notice of disclosure.[259]

It is also uncommon for privacy-protective interveners with a focus on criminal justice to provide comments during the legislative process.[260] Instead, the repeat players advocating for privacy interests at legislative hearings—such as the American Civil Liberties Union, Electronic Privacy Information Centre, Electronic Frontier Foundation, and Centre for Democracy and Technology—are all purpose organizations whose agenda focuses on mainstream socioeconomic concerns.[261] Among those groups that regularly appear in front of legislative hearings and focus on criminal law issues, none specialize in privacy issues.[262] Moreover, the effort put into representing the privacy interests of the poor is severely restricted due to these groups' funding being tied up with multiple other civil rights issues.[263]

In Murphy's view, federal statutory law has not only failed to provide adequate safeguards to protect the privacy of indigent persons, "it has actually affirmatively compromised their privacy by mandating disclosure on the thinnest showing of law enforcement need."[264] As she concludes, "[t]o the extent that technology has played a role with respect to the privacy of the poor, it has been to capitalize on opportunities to share information, rather than to view digitalization as a threat".[265] This undermines Kerr's assertion that the mostly mainstream interest in new technologies will ensure digital technologies will not be used to undermine privacy.[266] Not only

[259] *Ibid* at 512-14. See the extensive sources cited therein and the review provided above in this section.
[260] *Ibid* at 505.
[261] *Ibid*.
[262] *Ibid*.
[263] *Ibid* at 505-06.
[264] *Ibid* at 512.
[265] *Ibid*.
[266] *Ibid* at 507.

must American society be vigilant in how the state searches new technologies possessed by citizens, it must also ensure that those technologies are not used by the state for purposes that undermine privacy protections, especially the interests of vulnerable members of society.

Murphy also questions Kerr's conclusion that private lobbying for expanded police powers is unlikely to occur.[267] As she observes, technological devices are generally developed and sold by private companies.[268] As government constitutes a vast and deep-pocketed client, these companies have a strong incentive to convince legislatures to increase use of their technologies.[269] As Murphy posits, "many contemporary tools of criminal justice (such as DNA, drug analysis machines, and even computer software) rely upon the development of materials and instruments by the private sector."[270] The profitability of expanding state use of these and similar tools provides private businesses with an incentive to lobby for increased use of their technologies, which in effect means increased state intrusions onto personal privacy will be encouraged.[271]

It is true that some entities which design and operate technologies used by the mainstream population may profit from opposing privacy invasive rules. For instance, internet and wireless phone service providers may refuse to disclose information, such as internet subscriber information, that would offend their customers.[272] However, as one author maintains, "legislators can easily minimize such problems by providing legal safe harbors for compliance with requests, and even by mandating nondisclosure ('gag orders') to ward off public relations nightmares."[273] The passing of the *PRA* discussed earlier was illustrative: Congress was not motivated by a

[267] *Ibid* at 536.
[268] *Ibid*.
[269] *Ibid*.
[270] *Ibid*.
[271] *Ibid* citing Ian Herbert, "Where Are We with Location Tracking: A Look at the Current Technology and the Implications on Fourth Amendment Jurisprudence" (2011) 16 Berkeley Journal of Criminal Law 442 (describing companies behind GPS tracking devices).
[272] *Ibid* at 536.
[273] *Ibid*.

perceived need to protect privacy interests, but rather by a desire to protect companies from lawsuits for disclosing private information.[274]

III. Lessons from the American Experience

It is useful at this juncture to summarize the conclusions drawn from the above review. Although the literature on courts has been less comprehensive than that assessing the institutional capacity of Congress, the update provided in the preceding sections makes it possible to draw some general conclusions with respect to the relative capacity of both American courts and Congress to respond to the challenges of governing privacy in the digital age.

(a) Judiciary

Kerr's conclusion that judicial rules will lag behind technology is uncontroversial. It is also uncontested that lower courts tend to receive inadequate evidence upon which to make rules concerning digital privacy. However, appellate courts are capable of putting together well-informed evidentiary records. The responses from interveners in particular are able to help ensure appellate courts make their decisions in adequate information environments. The Court's strict adherence to *stare decisis* norms, however, has proven problematic. It took until 2018 for the Court to affirm that the third-party doctrine will not apply to all digital data. In so doing, the Court made it clear that the doctrine will only not apply to extreme digital privacy intrusions. This will likely leave many digital technologies unregulated by the Fourth Amendment. Whether it is the wording/structure of the Fourth Amendment or the partisan nature of the Court, it is likely that the judiciary will continue to cede digital privacy rule-making duties to Congress and provide minimal oversight of rules deriving from the legislative branch.

(b) Congress

[274] See Sklansky, "Two More Ways", *supra* note 6 at 231.

The above review shows that Congress is relatively active in the area of new technology, even if there are a variety of technologies which have received no regulation or developed significant gaps due to Congress failing to update its statutes. It is notable, however, that the nature of the protection Congress provides is frequently underwhelming. Although some additional privacy protections are available in several statutes, it is questionable whether many of these protections are meaningful. For instance, the fact that notice is sometimes given provides cold comfort to the defendant who has little recourse to contest the disclosure given the low issuing standards. The lack of exclusion of evidence and the unrealistic chance that civil remedies will be available or pursued for searches or seizures of most private information provides citizens with very little in terms of privacy protection.[275]

To better understand why Congress tends to pass unbalanced digital privacy legislation, it is necessary to provide an overview of the legislative process in the United States. Before a Bill becomes a law, it must be approved by the House of Representatives, Senate, and President.[276] If the President rejects a Bill, both houses may override the President with a two-thirds majority vote.[277] It is, however, rare for both houses to be held by the same political party let alone a two-thirds majority.[278] Moreover, as each house and the President are elected independently from one another, these actors need not tow a strict party line.[279] These conditions often make it difficult to marshal a majority of legislators to support contentious initiatives.[280] In other words, the American

[275] See Murphy, "Politics of Privacy", *supra* note 6 at 524; Donald Dripps, "Constitutional Theory for Criminal Procedure: *Dickerson*, *Miranda*, and the Continuing Quest for Broad-but-Shallow" (2001) 43 William and Mary Law Review 1 at 46. I will discuss this literature in detail in Chapter Five.
[276] See Article I, section 7 of the United States Constitution.
[277] *Ibid*
[278] See Stephen Brooks, Douglas Koopman, and Matthew Wilson, *Understanding American Politics*, 2nd ed (Toronto: University of Toronto Press, 2013) at 131-32.
[279] *Ibid* at 140, 148.
[280] *Ibid* at 145, 148.

system is designed to provide numerous checks and balances which tend to result in deadlocks when passing legislation.[281]

To pass laws in this environment, legislators frequently resort to passing omnibus bills.[282] Such bills bunch together various and wide-ranging types of laws into one legislative package.[283] The purpose of so doing is to allow for laws which otherwise would not pass individually to pass collectively as a matter of political compromise. Although this allows desirable laws to be passed, it also allows non-desirable laws to pass despite cogent opposition.[284] Scholars also observe that omnibus bills frequently fail to foster the conditions under which thorough study and review of legislation occurs.[285] Given the broad ambit of omnibus bills, there will often not be time for proper committee study with respect to all aspects of the bill.[286] Moreover, it is often the case that the legislature will not have time to debate the merits of all aspects of a wide-ranging group of laws.[287]

These issues passing legislation are exacerbated by the fact that Congress is vulnerable to significant public choice theory concerns. Although the authors reviewed above provide some insights as to why these problems arise in Congress, prominent public choice theorists explain this tendency in part by observing that the American legislative system provides multiple forums for lobbying as the House of Representatives, Senate, and to a lesser degree the President, can block laws.[288] Although this also makes it more difficult for lobbyists to persuade Congress to pass laws,

---

[281] *Ibid*.
[282] See Louis Massicotte, "Omnibus Bills in Theory and Practice" (2013) 36 Canadian Parliamentary Review 13 at 13. See also Adam Dodek, "Omnibus Bills: Constitutional Constraints and Legislative Liberations" (2017) 48 Ottawa Law Review 1.
[283] *Ibid*.
[284] *Ibid* at 15-16.
[285] *Ibid*.
[286] *Ibid*.
[287] *Ibid*.
[288] See Jerry Mashaw, "Public Law and Public Choice: Critique and Rapprochement" in Daniel Farber and Anne O'Connell (eds), *Research Handbook on Public Choice and Public Law* (Cheltenham: Edward Elgar Publishing Ltd, 2010) at 30.

the increasing need to receive independent corporate support to be competitive in future elections makes American legislatures increasingly beholden to lobbyists' interests.[289] Although scholars have not identified an overwhelming number of instances where public choice theory concerns arose in the digital privacy/criminal procedure context, the concerns that have arisen are nevertheless significant enough to brings its institutional competence into question.

Conclusion

The above review of the American experience responding to the challenges of governing digital privacy confirms that both courts and Congress have difficulties keeping pace and providing coherent, even-handed rules with respect to digital technologies. Although appellate courts are able to receive adequate information, there are other concerns related to the neutrality of the judiciary and the wording/structure of the Fourth Amendment that impede judicial ability to govern digital privacy. Similarly, despite the fact that Congress is often keen on legislating with respect to new technologies, its legislation tends to provide underwhelming weight to digital privacy interests. Instead, Congress is often susceptible to law enforcement and lobbyist influence when crafting digital privacy laws. As should be evident from the discussion in previous Chapters, the reasons for the difficulties governing digital privacy in Canada differ from those in the American context. Comparing these experiences will therefore prove useful for developing a normative framework for determining how courts and legislatures should respond to the challenges of governing privacy in the digital age.

[289] *Ibid*. See also Raj Chari, Gary Murphy, and John Hogan, "Regulating Lobbyists: A Comparative Analysis of the United States, Canada, Germany and the European Union" (2007) 78 The Political Quarterly 422.

Chapter Five

Drawing Lessons from the Canadian and American Experiences

Introduction

The preceding Chapters illustrate that despite relatively well-functioning democratic systems, courts and legislatures in both Canada and the United States have had considerable difficulty developing efficient and coherent digital privacy laws. The reasons for these difficulties, however, diverge in important ways. Whereas Canadian courts have difficulty teasing out relevant facts within its adversarial system, the American system has not. Instead, strong *stare decisis* norms and a rigidly interpreted Fourth Amendment have proven most burdensome. Whereas Parliament's slow reaction times to developments in digital technologies can partly be attributed to difficulties obtaining majority governments, Congress has the potential to be even more deadlocked given its republican and bicameral system of governance. This in turn often results in Congress relying heavily on omnibus bills which generally do not facilitate thorough study of complex facts before legislation becomes law. Congress' difficulties are also compounded by a greater susceptibility to lobbying by both private actors and law enforcement agents.

The lack of research outside of the United States concerning the institutional capacity of courts and legislatures to respond to the difficulties of governing digital privacy has prevented

scholars from undertaking comparative analysis. The review offered in the preceding chapters makes such a comparison possible. By comparing the Canadian and American experiences, this Chapter aims to develop a normative framework for determining the kinds of digital privacy regulation to which each institution in any given polity is best suited. I contend that a variety of factors—ranging from a country's mode of constitutional interpretation, to the structure of the right to be protected from state searches and seizures, the remedies available for breaches, conceptions of *stare decisis*, the degree of intervener participation at appellate courts, as well as the legislative model used for passing laws—all impact the relative institutional capacity of courts and legislatures.

I. Comparative Methodology

In its most basic sense, "comparison is the construction of relations of similarity or dissimilarity between different matters of fact."[1] Comparison as a methodology, however, compares objects to create more than simple knowledge about similarities and differences. Instead, the comparative method interrogates similarities and differences between objects of study to test previous hypotheses and/or construct normative theories about social and political phenomena.[2] As Luc Turgeon observes, "[b]y exploring variations in outcomes among cases, we are prompted to find the roots of such differences and to outline factors, or a combination of factors, that might account for shared or unique aspects of the [political] experience."[3]

[1] See Nils Jansen, "Comparative Law and Comparative Knowledge" in Mathias Reimann and Reinhard Zimmermann, eds, *The Oxford Handbook of Comparative Law* (Oxford: Oxford University Press, 2006) 305 at 310.
[2] See Jaako Husa, *A New Introduction to Comparative Law* (Portland: Hart Publishing, 2015) at 71.
[3] See Luc Turgeon, "Introduction" in Luc Turgeon et al., eds, *Comparing Canada: Methods and Perspectives on Canadian Politics* (Vancouver: UBC Press, 2014) 3 at 10 citing Hugh Stretton, *The Political Sciences: General Principles of Selection in Social Science and History* (London: Routledge, 1969) at 245-47; Arend Lijphart, "The Comparable-Cases Strategy in Comparative Research" (1975) 8:2 Comparative Political Studies 158 at 159-60.

Arend Lijphart situates the comparative method among one of four main means of scientific inquiry, the others being the experimental, statistical, and case-study methods.[4] In terms of deriving normative conclusions, the comparative method is inferior to the experimental or statistical methods. The most obvious limitation has been described as one of "many variables, small number of cases."[5] As basic statistics teaches, fewer case studies result in increased explanatory factors, which makes drawing reliable explanations for social phenomenon more difficult.[6] The comparative method nevertheless serves an important role where there are significant limitations in information and/or time to fully comprehend the relevant objects of study that would allow the researcher to draw more statistically significant conclusions.[7]

To mitigate the limits inherent in the comparative method, "small n" studies frequently employ what is known as the most similar systems design method.[8] This method "is a comparative approach in which the common characteristics of the different cases constitute 'control variables' that cannot account for the observed difference, while the remaining differences constitute the explanatory, or independent, variables."[9] Comparable cases, then, are those that "(a) are matched on many variables that are *not* central to the study, this in effect 'controlling' for these variables; and (b) differ in terms of the key variables that *are* the focus of analysis, thereby allowing a more adequate assessment of their influence".[10]

---

[4] For a more detailed review, see Arend Lijphart, "Comparative Politics and Comparative Method" (1971) 65 The American Political Science Review 682.
[5] *Ibid* at 685.
[6] See David Collier, "The Comparative Method" in Ada Finifter, ed, *Political Science: The State of the Discipline II* (Washington: American Political Science Association, 1993) at 105.
[7] See Lijphart, "Comparative", *supra* note 4 at 685.
[8] See Carsten Anckar, "On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research" (2008) 11:5 International Journal of Social Research Methodology 389.
[9] See Turgeon, "Introduction", *supra* note 3 at 13 citing Adam Przeworski and Henry Teune, *The Logic of Comparative Social Inquiry* (New York: John Wiley, 1970).
[10] See Lijphardt, "Comparative", *supra* note 4 at 687-91; Giovanni Sartori, "Comparing and Miscomparing" (1991) 3 Journal of Theoretical Politics 243 at 246.

The most similar systems design method is commonly employed for Canadian and American comparative studies. This follows because of the countries "shared Anglo-American heritage, federal structures, and liberal-market economies".[11] The fact that both are common law countries with strong powers of judicial review vested in their judiciaries are also key shared variables. Yet, the distinct nature of parliamentarian and republican systems of government can serve as key "explanatory" or "independent" variables.[12] Moreover, as will be discussed in detail below, the legal context within which each country operates also has several differences which may help explain the challenges that courts in each country have had responding to state intrusions onto digital privacy.

II. Comparing the Canadian and American Experiences

The ability of courts and legislatures to respond to uses of digital technologies in an efficient, coherent, and fair manner are the driving factors impacting their relative institutional competency. Comparing the difficulties American and Canadian institutions have encountered meeting these ends with those of its jurisdictional counterpart will lend several valuable insights for institutional and constitutional design strategies within other broadly similar polities.

(a) Judiciary

(i) Constitutional Interpretation

In the United States, much disagreement about the meaning of the Fourth Amendment turns on how the Constitution is interpreted. Originalist interpretation, defended most adamantly by the

[11] See Turgeon, "Introduction", *supra* note 3 at 13. See also James Stribopoulos, "Lessons from the Pupil: A Canadian Solution to the American Exclusionary Rule" (1999) 22 Boston College International & Comparative Law Review 77 ("For comparative purposes, Canada is unlike any other Commonwealth nation. Canada and the United States share close geographic proximity, similar cultures, and a common language. Both nations have ethnically diverse populations forged from immigrant citizens who predominately reside in concentrated urban areas. Both nations have prospered throughout the post-war era and share similar levels of economic development. Although differences definitely exist, it is arguable that no two nations share so many similarities").
[12] *Ibid*.

late Justice Scalia, provides that constitutional text must be interpreted as the text would have been understood at the time of ratification.[13] The meaning of the text is equated with what reasonable persons living at the time of ratification would have thought the words meant.[14] This interpretive philosophy is most commonly contrasted with the understanding of the constitution as a living document whose meaning can adapt to changing times.[15] In Canada, the metaphor that the *Charter* is a "living tree" is often employed to justify judicial interpretation of constitutional rights in a broad and flexible manner.[16]

My purpose in raising these different models of constitutional interpretation is not to suggest one is better than the other. Originalist conceptions of the Fourth Amendment—generally based on property law rules—often lead to similar results as the normatively-based inquiry. The Court's decision in *United States v Jones*[17] is demonstrative. Therein, the police installed a Global Positioning System (GPS) tracking device on the appellant's vehicle.[18] The majority concluded that the Fourth Amendment was violated as the police committed a physical trespass when planting the GPS device.[19] Justice Sotomayor, writing for the minority, agreed in the result but determined that the appellant's reasonable expectation of privacy was engaged given the clear privacy interests implicated when police track individuals using precise and surreptitious technologies.[20]

---

[13] For a recent review, see Randy Barnett and Evan Bernick, "The Letter and the Spirit: A Unified Theory of Originalism" (2018) 107:1 Georgetown Law Journal 1 at 7-18.
[14] This is to be contrasted with the branch of originalism that interprets constitutional provisions based on evidence of the intent of the drafters. See generally Barnett and Bernick, "The Letter and the Spirit", *supra* note 13.
[15] For a review of the two schools of thought, see Peter Smith, "How Different are Originalism and Non-Originalism?" (2011) 62 Hastings Law Journal 707.
[16] See *Re BC Motor Vehicle Act*, [1985] 2 SCR 486, 24 DLR (4th) 536.
[17] 132 S Ct 945 (2012).
[18] *Ibid* at 1 (opinion of Justice Scalia).
[19] *Ibid* at 4.
[20] See the reasons of Justice Sotomayor at 4.

A similar point arises from the Court's decision in *Carpenter v United States*.[21] The Court was asked to determine whether the Fourth Amendment was engaged when the police obtained "cell site location information" (CSLI) from the defendant's cellular provider. Although the originalist approach in the main dissent did not result in CSLI attracting a reasonable expectation of privacy,[22] Justice Gorsuch's application of originalist doctrine did. In his view, providing cell phone site data to third parties was sufficiently analogous to committing a bailment.[23] The majority agreed with Justice Gorsuch's conclusion, but determined that the "qualitatively different category" of privacy interests implicated by using CSLI to precisely track the prior location of a person is what demanded Fourth Amendment protection.[24]

Given the Court's recent rulings in *Jones* and *Carpenter*, it is not clear that different models of constitutional interpretation always have a meaningful impact on digital privacy protection.[25] Entertaining competing interpretive philosophies does, however, provide significantly more room to disagree about the content of the Fourth Amendment. This in turn can lead to unclear legal doctrine. A more detailed examination of the Supreme Court of the United States' jurisprudence determining the constitutionality of state use of tracking devices is demonstrative.

Beginning with *United States v Knotts*,[26] the majority of the Court applied originalist doctrine in determining that state use of tracking devices only attracts constitutional protection if it monitors historically protected places. A car travelling on a public thoroughfare was therefore

[21] 16 S Ct 402 (2018).
[22] See generally the reasons of Justices Kennedy, Thomas, and Alito.
[23] See generally the reasons of Justice Gorsuch.
[24] See the reasons of Chief Justice Roberts at 11.
[25] Although speculative, it is not clear that "privacy" as an area of law has a particularly conservative or liberal tilt. As a result, subscribing to the more "conservative" originalist school of constitutional interpretation need not lead to results one might associate with conservatism.
[26] 460 US 276 (1983).

found not to attract constitutional protection.[27] A year later in *United States v Karo*,[28] the Court determined that a surreptitiously planted beeper which at some point physically entered a home engaged the Fourth Amendment. This result followed as the founders clearly intended the Fourth Amendment to protect against physical intrusions into the home.[29]

A continued emphasis on originalist interpretation resulted in the jurisprudence still not being settled nearly three decades later when the Court decided *Jones*. Although a majority of the Court concluded that physically attaching a tracking device to a vehicle constituted at least a physical trespass which engaged the Fourth Amendment,[30] Justices Sotomayor and Alito queried whether physical trespass would apply in all cases, such as when a GPS device was remotely activated.[31] Although originalist conceptions of the Fourth Amendment *may* account for such scenarios, the law remains unclear as to how it would do so.[32] Given the primacy attached to common law property rules, the majority of the Court was able to dodge answering whether remotely activated GPS searches engage the Fourth Amendment.[33]

In Canada, the reasonable expectation of privacy test governing whether state searches or seizures must be "reasonable" is not subject to competing theories of constitutional interpretation.[34] As a result, when faced with a similar issue as in *Knotts*, *Karo*, and *Jones*, the

---

[27] *Ibid* at 281.
[28] 468 US 705 (1984).
[29] *Ibid*. The Fourth Amendment explicitly mentions the home as a constitutionally protected area.
[30] It should be noted that in *Knotts*/*Karo*, the beeper had been placed in a container by the state which had subsequently been sold to the suspects.
[31] See *Jones*, *supra* note 17 at 955, 961-64.
[32] Originalist doctrine may find such an intrusion to be unforeseen by the founding fathers and therefore unprotected by the Fourth Amendment. Applying the living tree understanding of the Fourth Amendment would likely result in the search tactic engaging constitutional protection because the privacy interests in the two scenarios are identical.
[33] This primacy has been the subject of judicial disapproval. As Justice Stephens wrote in dissent in *Wyoming v Houghton*, 526 US 295 (1999) at 311 (note 3), "[t]o my knowledge, we have never restricted ourselves to a two-step Fourth Amendment approach wherein the privacy and governmental interests at stake must be considered only if 18th-century common law 'yields no answer'".
[34] See generally *Hunter v Southam*, [1984] 2 SCR 145, 11 DLR (4th) 641.

Supreme Court of Canada was able to issue a far more comprehensive ruling in *R v Wise*.[35] Even though the tracking device utilized by the police was unsophisticated,[36] the Court determined that its use infringed the occupant's normative privacy interests.[37] This ensured that all similarly invasive tracking practices would attract the protection of section 8 of the *Charter*.[38] As such, the Supreme Court of Canada was able to provide a reasonably determinate rule on a prominent digital privacy issue in 1992, while in 2012 the Supreme Court of the United States had yet to provide comparably clear guidance. Given the greater economies of adjudication in the United States, this result is counterintuitive.[39]

(ii) Constitutional Drafting

The wording of the constitutional protection from state searches and seizures can also significantly impact judicial responses to privacy rules. Consider the wording of the Fourth Amendment. It provides as follows:

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[40]

Courts and scholars have debated whether the Amendment should be read as one interconnected text or as two separate clauses. As a result, the provision has been subject to two competing

---

[35] [1992] 1 SCR 527, 70 CCC (3d) 193.

[36] The device at issue was a low powered radio transmitter capable of revealing an approximate location of a motor vehicle.

[37] Although the Crown had conceded this point, the majority came to this conclusion on its own as well. As Justice Cory observed at 532, "it seems artificial to distinguish between the installation of the beeper and the subsequent monitoring. The monitoring is the extension of the installation. It is the aim and object of the installation and cannot be divided from the latter. The installation of the device and its subsequent use to monitor the vehicle, together, constituted the unreasonable search."

[38] The device was a low power radio transmitter that could provide a general location for the thing being tracked.

[39] As the United States is significantly larger than Canada and at least comparably wealthy per capita, it should expect to have such issues comprehensively dealt with before smaller polities.

[40] For a history of the drafting of the Fourth Amendment, including how the controversial conjunction "and" was inadvertently adopted in the text, see Thomas Clancy, "The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures" (1995) 25 University of Memphis Law Review 483.

interpretations. As Justice Thomas explained in *Groh v Ramirez*,[41] "the Court has vacillated between imposing a categorical warrant requirement and applying a general reasonableness standard."[42]

For much of the twentieth century, the Fourth Amendment was subject to the first interpretation.[43] The Court therefore required police to generally seek a pre-authorized warrant based on probable cause if a state activity qualified as a "search" or "seizure".[44] This approach, although a reasonable reading of the text of the Fourth Amendment, significantly impacted the scope of privacy protections in the United States. As Christopher Slobogin and Erin Murphy observe, imposing such a high standard of "probable cause" in all cases has had a chilling effect on judicial willingness to recognize a reasonable expectation of privacy.[45]

The Court's development of the infamous third-party doctrine is illustrative.[46] This doctrine provides that once otherwise private information is passed on to a third party, the person from whom the information derives no longer maintains a reasonable expectation of privacy in the

---

[41] 540 US 551 (2004).
[42] *Ibid* at 571-72.
[43] See Thomas Davies, "Recovering the Original Fourth Amendment" (1999) 98 Michigan Law Review 547 at 559 ("For most of [the twentieth] century, the Supreme Court has endorsed what is now called the 'warrant-preference' construction of Fourth Amendment reasonableness, in which the use of a valid warrant…is the salient factor in assessing the reasonableness of a search or seizure"). Although the Court's decision in *Katz v United States*, 389 US 347 (1967) ushered in the normatively based "reasonable expectation of privacy" test, scholars have shown that the Court largely ignored this decision in the twentieth century and instead applied property law rules. See Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution" (2004) 102 Michigan Law Review 801at 809-24.
[44] For an excellent review of this history, see Cynthia Lee, "Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness Analysis" (2012) 81 Mississippi Law Journal 1133 at 1134-35, 1138. For endorsements of the "probable cause forever" approach, see Gerald Reamey, "When 'Special Needs' Meet Probable Cause: Denying the Devil Benefit of Law" (1992) 19 Hastings Constitutional Law Quarterly 340; Morgan Cloud, "The Fourth Amendment during the Lochner Era: Privacy, Property, and Liberty in Constitutional Theory" (1996) 48 Stanford Law Review 555.
[45] See Christopher Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* (Chicago: University of Chicago Press, 2007) at 29; Erin Murphy, "The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions" (2013) 111 Michigan Law Review 485 at 542.
[46] The third-party doctrine provides that once otherwise private information is passed on to a third party, the person from whom the information derives no longer maintains a reasonable expectation of privacy. See *Smith v Maryland*, 442 US 735 (1979).

information.[47] As the Court observed, this rule applies "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[48]

As explained in the preceding Chapter, American courts have used the third-party doctrine to determine the absence of a reasonable expectation of privacy in a variety of cases where most individuals would expect to attract at least *some* constitutional protection. In my view, it is reasonable to conclude that the third party doctrine developed as a means to avoid unduly hampering police investigations.[49] When the state seeks information with relatively low privacy interests, it is likely because police are trying to *make out* a case for probable cause so as to pursue more invasive investigation methods.[50] Allowing the state to access information such as incoming and outgoing call records or minimal internet service provider records on a lower standard than probable cause facilitates such investigations. However, the Court's interpretation of the Fourth Amendment generally did not authorize searches on a standard lower than probable cause.[51] In turn, this forced the Court to choose between hampering law enforcement or providing no privacy protections at all.

More recently, the Court's Fourth Amendment jurisprudence has ignored the explicit warrant requirement and instead allowed courts to require that state searches and seizures simply be "reasonable".[52] Under this view, reasonableness was not meant to be determined by a "fixed formula", but instead by "the facts and circumstances of each case."[53] This interpretation of the

[47] See *United States v Miller*, 425 US 435 (1976).
[48] *Ibid* at 443.
[49] This follows similar reasoning as employed in Slobogin, *Privacy at Risk*, *supra* note 45 at 29.
[50] See Steven Penney, "Updating Canada's Communications Surveillance Laws: Privacy and Security in the Digital Age" (2008) 12 Canadian Criminal Law Review 115 at 146-47 citing *R v Cody*, [2004] QJ No 14164 at para 26.
[51] For one example, see *Terry v Ohio*, 392 US 1 (1968) ("stop and frisk" was found to be legal if the officer had reasonable suspicion that the subject committed a crime or was about to do so).
[52] Slobogin, *Privacy at Risk*, *supra* note 45 at 60.
[53] *Ibid* at 63.

Fourth Amendment was eventually overruled in 1969,[54] leading to the warrant based on probable cause approach outlined above.[55] The Court's modern approach to interpreting the Fourth Amendment has revitalized emphasis on the "reasonableness" clause of the Fourth Amendment, thus allowing for a more flexible judicial response to recognizing privacy interests.[56]

Reasonableness may, of course, be viewed through competing lenses of constitutional interpretation. As seen above, originalists contend that reasonableness is determined by querying whether a search is inconsistent with a property law rule under the common law.[57] Only if the answer to this question is unclear will it be necessary to consider whether the relevant privacy and security interests of the state are balanced in a "reasonable" manner.[58] The latter interpretation, however, allows for a more nuanced and flexible approach to regulation of state searches and seizures, and is now favoured by some justices as the only approach to determining whether a search or seizure is consistent with the Fourth Amendment.[59] Allowing judges to impose a lower standard under the Fourth Amendment avoids forcing judges to make the stark choice between providing any privacy protection at all and undermining law enforcement investigations.[60]

The plain language of section 8 of the *Charter* does not lend itself to competing interpretations. Although warrantless searches are presumed unreasonable,[61] the reasonableness standard has resulted in courts permitting searches or seizures on less restrictive grounds than the probable cause standard dictated by the Fourth Amendment. In turn, courts have proven willing to

---

[54] See *Chimel v United States*, 395 US 752 (1969)
[55] *Ibid*. See also *Terry*, *supra* note 51 at 20.
[56] See Lee, "Reasonableness", *supra* note 44 at 1134-36.
[57] *Ibid* at 1143-44 citing David Sklansky, "The Fourth Amendment and Common Law" (2000) 100 Columbia Law Review 1739 at 1760.
[58] *Ibid* citing *Minnesota v Dickerson*, 508 US 366 (1993) at 379-80 (Reasons of Justice Scalia).
[59] For a review of the present application of the reasonableness test, see Lee, "Reasonableness", *supra* note 44 at 1139-47.
[60] For instance, when litigating how to govern state searches of pen register and trap and trace devices, the Court could have required that police demonstrate a "reasonable suspicion" that a search will garner evidence related to a crime.
[61] See *Hunter*, *supra* note 34 at 161.

find a reasonable expectation of privacy in even minimally intrusive searches.[62] The "reasonable suspicion" standard found in sections 492.1 and 492.2 of the *Criminal Code* applying to pen register, trap and trace, and tracking devices is exemplary.[63] It is also likely that subscriber information from internet service providers could be accessed on grounds significantly lower than warrant based on probable cause.[64]

I do not mean to suggest, however, that flexibility in interpretation will lead to a more robust conception of privacy. For instance, there are critics who charge that the Supreme Court of the United States' "reasonableness" analysis generally results in undue weight being placed on law enforcement interests.[65] My point is rather that providing courts with flexibility in determining the standard upon which any search may receive judicial approval fosters an environment in which courts will be able to objectively craft digital privacy rules. Imposing a "one-size-fits-all" standard forces courts to determine whether a police tactic engages a reasonable expectation privacy in a zero-sum fashion.

(iii) Constitutional Remedies

A driving theme in the American scholarship is that the availability of constitutional remedies has historically affected the interpretation of rights. In particular, the fact that the United States' Constitution previously had one main remedy for a breach of the Fourth Amendment—exclusion of evidence—was cited by several scholars as contributing to the Court's narrow

[62] For an extensive review of the various ways diminished expectations of privacy have nevertheless been found "reasonable", see James Fontana and David Keeshan, *The Law of Search & Seizure in Canada*, 8th ed (Markham: Lexis Nexis, 2010) at 17-21.
[63] Despite an early appellate decision failing to find a reasonable expectation of privacy in metadata related to incoming and outgoing calls (see *R v Fegan* (1993), 13 OR (3d) 88, 80 CCC (3d) 356 (ONCA)), Parliament inferred from the Court's conclusion in *Wise*, *supra* note 35 that minimally intrusive tracking devices (also known as "beepers") attracted a reasonable expectation of privacy and therefore that *Fegan* would not be upheld by the Court.
[64] See Chapter Two, Part II(b)(iii).
[65] See Lee, "Reasonableness", *supra* note 44 at 1151 citing Tracey Maclin, "The Central Meaning of the Fourth Amendment" (1993) 35 William & Mary Law Review 197 at 200.

approach to interpreting the Fourth Amendment.[66] Guido Calabresi goes further, contending that the broad application of the exclusionary rule is "most responsible for the deep decline in privacy rights in the United States."[67] This is a tenable conclusion as a judge faced with finding a reasonable expectation of privacy vis-à-vis a relatively non-serious search may well prefer to include the evidence as opposed to exclude evidence that often results in an acquittal.

The fact that a similar problem does not exist in Canada is at least partially attributable to the addition of an independent remedies provision in the *Charter*. Whenever a state actor breaches a constitutional right, section 24 of the *Charter* provides courts with a variety of remedies to rectify the breach.[68] Section 24(2) in particular allows for courts to exclude evidence only if its admission "would bring the administration of justice into disrepute." As the Court concluded in *R v Grant*,[69] determining whether this standard is met requires a careful balancing of the seriousness of the *Charter*-infringing state conduct, the impact of the breach on the *Charter* rights of the accused, and society's interest in having the case adjudicated on its merits.[70] Allowing judges to balance competing interests at the remedy stage ensures that they will not be significantly influenced by the effect finding a reasonable expectation of privacy will have on law enforcement.[71]

---

[66] See Solove, *Nothing to Hide*, *supra* note 47 at 140-41; Slobogin, *Privacy at Risk*, *supra* note 45 at 29-30; Erin Murphy, "The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions" (2013) 111 Michigan Law Review 485 at 542.

[67] See Guido Calabresi, "The Exclusionary Rule" (2002) 26 Harvard Journal of Law and Public Policy 111 at 112.

[68] The wording of section 24 reads as follows: "(1) Anyone whose rights or freedoms, as guaranteed by this Charter, have been infringed or denied may apply to a court of competent jurisdiction to obtain such remedy as the court considers appropriate and just in the circumstances. (2) Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this *Charter*, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute."

[69] 2009 SCC 32, [2009] 2 SCR 353.

[70] *Ibid* at para 71. For an in-depth review of each consideration see paras 72-86.

[71] For a good example, see the Court's decision in *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212. While anonymously online, Mr. Spencer had possessed and traded child pornography. The police obtained his ISP subscriber information without a warrant, as it was unclear whether the accused possessed a reasonable expectation of privacy in the information. The Court applied a generous and robust understanding of the reasonable expectation of privacy doctrine to find a reasonable expectation of privacy. The breach was, however, found to be inadequately serious to exclude the evidence.

The American jurisprudence eventually responded to these concerns by incrementally allowing inclusion of evidence despite breaches of the Fourth Amendment.[72] Beginning with *US v Leon*,[73] the Court allowed for reliable physical evidence to be admitted where the officer's breach was made in "good faith".[74] Exceptions were subsequently developed to allow admission where police discovered the evidence from a separate source,[75] would have inevitably discovered the unconstitutionally obtained evidence,[76] or where the breach was adequately attenuated from the original constitutional harm.[77] The continuing development of exceptions resulted in the Court rendering a general rule permitting exclusion of evidence only "where its deterrence benefits outweigh its substantial social costs."[78] As a result, evidence is now excluded only where it "serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence."[79]

This narrowing of the exclusionary rule rests on strong empirical evidence demonstrating that police are unlikely to be deterred by the prospect of excluding evidence.[80] In turn, this evidence has resulted in authors advocating for the abolition of the exclusionary rule altogether,[81] or at least limiting its application to clear instances of "bad faith."[82] In its place, remedies for breaches would

---

[72] The Court originally found that the exclusionary rule applied only to the American federal government under the Fourteenth Amendment. In *Mapp v Ohio*, 367 US 643 (1961), however, the Court extended the exclusionary rule's applicability to state infringements, such as those under the Fourth Amendment. For an historical overview of the exclusionary rule, see Thomas Davies, "Recovering the Original Fourth Amendment" (1999) 98 Michigan Law Review 547.
[73] 468 US 897 (1984).
[74] *Ibid*. Similarly, see *Illinois v Krull*, 480 US 340 (1987). The Court held that reasonable reliance on a statute that was later declared unconstitutional would result in the evidence obtained being admitted under the "good faith" exception.
[75] See *Murray v United States*, 487 US 533 (1988) at 537.
[76] See *Nix v Williams*, 467 US 431 (1984) at 443-44.
[77] See *Hudson v Michigan*, 547 US 586 (2006); *Utah v Strieff*, 136 US 2056 (2016).
[78] See *Hudson*, *supra* note 77 at 591.
[79] *United States v Herring*, 555 US 135 (2009) at 144.
[80] For an extensive overview, see Christopher Slobogin, "Why Liberals Should Chuck the Exclusionary Rule" (1999) 1999 University of Illinois Law Review 363 at 363-403; James Stribopoulos, "In Search of Dialogue: The Supreme Court, Police Powers, and the Charter" (2005) 31 Queen's Law Journal 1 at 53-54.
[81] See Murphy, "Politics of Privacy", *supra* note 45 at 537-44.
[82] See Solove, *Nothing to Hide*, *supra* note 47 at 141-45.

rely on civil suits, fines, or judicial denouncement of state conduct to deter violations of the Fourth Amendment.[83] Others have suggested that significant decreases in sentences combined with individualized punishments of police officers via additional training or fines could provide a better calibrated incentive/deterrent structure.[84]

Each of the above proposals nevertheless comes with its own challenges. It is questionable whether imposing fines on individual police officers or their departments will effectively deter police conduct.[85] Given the influence law enforcement often exacts on legislatures, any effect would likely be offset by increased allocation of resources to policing departments.[86] Punishing individual officers may also provide an "overdeterrent" resulting in police failing to do their jobs for fear of monetary punishment.[87] Although reducing sentences may sometimes provide a feasible incentive, in many other cases it will not. Where sentences are slight, or mandatory minimum punishments are in place, reducing a sentence either will provide little incentive or simply not be an option.[88]

Without convincing empirical evidence, it would therefore be unwise to abandon the greatest incentive for litigants to bring constitutional claims.[89] This is especially true in the field

---

[83] For an historical overview, see Slobogin, "Liberals", *supra* note 80.
[84] See Calabresi, "Exclusionary Rule", *supra* note 67 at 113-15.
[85] Justice Sotomayor makes a similar point in her dissenting reasons in *Strieff*, *supra* note 77 at 2069. See also Wayne Lafave, Jerold Israel, and Nancy King, *Criminal Procedure*, 3rd ed (St. Paul: West Group, 2000) at 115-16.
[86] Although Slobogin, "Liberals", *supra* note 80 at 400-05 suggests that the provision of a "bench trial" initiated by state-paid litigators would provide a workable scheme, no such scheme has been instituted in the United States, which speaks to the significant difficulty instituting such a process would be politically.
[87] See Slobogin, "Liberals", *supra* note 80 at 406-12. The author's retorts (social pressure to fight crime, professional pride, and personal motivation to do justice) are all speculative and unconvincing. It is possible that officers would be more motivated to "shield" themselves from liability by increasing warrant applications, but that itself raises significant financial stresses on an already overburdened criminal justice system.
[88] As for why exemptions are not permitted for mandatory minimum punishments in Canada, see *R v Ferguson*, 2008 SCC 6, [2008] 1 SCR 96.
[89] Studies have long questioned the efficacy of the exclusionary rule in deterring police conduct. See Slobogin, "Liberals", *supra* note 80 at 368-401. It is, however, unclear that the alternatives proposed will better deter police intrusions onto constitutional rights without actual empirical testing. Much more importantly, it is unclear how replacing exclusion with police sanctions will incentivize litigation. See Lafave et al., *Criminal Procedure*, *supra* note 83 at 115-16.

of digital privacy. As both Canada and the United States' legislative development of digital privacy law lags considerably behind technological advancement, courts are increasingly expected to play a "gap filling" role to ensure rules exist to govern state intrusions onto digital privacy.[90] Allowing individual judges to balance a variety of competing factors in determining if exclusion is appropriate is much more likely to incentivize litigants to bring constitutional challenges than a rule restricting exclusion of evidence to "deliberate, reckless, or grossly negligent conduct".[91]

The American Supreme Court's abandonment of an automatic exclusionary rule is therefore reasonable as it lessens the pressure on judges to refuse to find that a search engaged a reasonable expectation of privacy. Yet, the Court has arguably swung the pendulum too far in the other direction by restricting exclusion of evidence to only the narrowest of circumstances.[92] The Court's emphasis on using exclusion of evidence to deter rights violations ignores the other major purpose of constitutional remedies: incentivizing litigation. Constitutional remedies in the Canadian context are more open-ended, thus allowing courts to exercise significant discretion in determining whether to exclude evidence. This approach is much more likely to incentivize litigation and better ensures that courts may objectively determine whether a search tactic engages a reasonable expectation of privacy.

(iv) Conceptions of Stare Decisis

American scholars also observe that *stare decisis* norms will prevent courts from altering the meaning or application of its constitution to fit novel and/or changing circumstances relating

[90] See Chapter Three; Kerr, "Fourth Amendment", *supra* note 43; Murphy, "Politics of Privacy", *supra* note 45; Daniel Solove, "Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference" (2005) 74 Fordham Law Review 747.
[91] See *Herring*, *supra* note 79 at 144.
[92] See Tonja Jacobi, "The Law and Economics of the Exclusionary Rule" (2011) 87 Notre Dame Law Review 585 at 656 ("[f]or advocates of the exclusionary rule, the great tragedy of recent jurisprudence has been the erosion of the strength of the rule: courts have developed numerous exceptions, a process which has arguably steadily eroded Fourth Amendment protections over time.")

to digital privacy.[93] As Orin Kerr maintains, to keep up with such changes it would be necessary for courts "either to expressly change the governing rules at regular intervals or else articulate the governing rule using a standard that keeps the result unclear to incorporate changed circumstances."[94] The first option is difficult to accept in a judicial system with strong *stare decisis* norms; the second option leads to significant uncertainty about the content of legal rules.[95] As Kerr concludes, "[t]he result is constitutional law's version of the Heisenberg uncertainty principle in quantum physics; you can know the law at one time or you can know its general direction, but you can't know both at the same time."[96]

The American Supreme Court recognizes that *stare decisis* is not an "inexorable command."[97] Instead, it involves "a series of prudential and pragmatic considerations designed to test the consistency of overruling a prior decision with the ideal of the rule of law, and to gauge the respective costs of reaffirming and overruling a prior case."[98] Four main considerations are relevant in making this determination:[99] (i) whether the precedent "def[ies] practical workability";[100] (ii) whether overturning the precedent would impose a "special hardship" on anyone relying on past precedent;[101] (iii) whether subsequent legal developments had "left the old rule no more than a remnant of abandoned doctrine";[102] and (iv) "whether facts have so changed,

[93] See Kerr, "Fourth Amendment", *supra* note 43 at 873.
[94] *Ibid*.
[95] *Ibid*.
[96] *Ibid* (citations omitted).
[97] See *Planned Parenthood of Southeastern Pennsylvania v Casey*, 505 US 893 (1992) at 854.
[98] *Ibid*.
[99] *Ibid* at 854-55. More recently, see *Janus v American Federation of State, County, and Municipal Employees, Council 31 et al*., 585 US 1 at 34-35.
[100] *Ibid* at 854.
[101] *Ibid*.
[102] *Ibid* at 855.

or come to be seen so differently, as to have robbed the old rule of significant application or justification."[103]

Despite this seemingly principled approach to *stare decisis*, the Court's jurisprudence has been widely criticized for applying *stare decisis* in a sporadic, inconsistent manner, and at times for operating in "bad faith."[104] These criticisms derive largely from the structure of the Court's test. As one author puts it, "[t]he sheer number of these considerations, combined with the fact that the Court often selects a few items from the catalog without explaining how much work is being done by each, makes it difficult even to find a starting point for thinking critically about *stare decisis* as a judicial doctrine."[105] This under theorized approach to *stare decisis* thus allows opinion about the merits of a case, as opposed to the values underlying the *stare decisis* principle, guide judicial determinations.

The way in which this approach to *stare decisis* has affected digital privacy in the United States is well illustrated by the Court's recent decision in *Carpenter v United States*,[106] reviewed in the previous Chapter. The Court's conclusion that cell site location information (CSLI) attracted a reasonable expectation of privacy was reasonable. The majority, however, warned that its ruling would not apply in other instances of serious privacy infringement such as real-time CSLI tracking of cell phones or so-called "tower dumps".[107] The latter procedure involves "a download of

---

[103] *Ibid*.
[104] See Kurt Lash, "The Cost of Judicial Error: *Stare Decisis* and the Role of Normative Theory" (2014) 89 Notre Dame Law Review 2189 at 2189 citing Randy Kozel, "*Stare Decisis* as Judicial Doctrine" (2010) 67 Washington & Lee Law Review 411 at 414; Henry Paul Monaghan, "*Stare Decisis* and Constitutional Adjudication" (1988) 88 Columbia Law Review 723 at 743; *Lawrence v Texas*, (2003) 539 US 558 at 587 (Reasons of Justice Scalia). See also Thomas Lee, "*Stare Decisis* in Historical Perspective: From the Founding Era to the Rehnquist Court" (1999) 52 Vandebilt Law Review 647 at 648; William Consovoy, "The Rehnquist Court and the End of Constitutional *Stare Decisis*: Casey, Dickerson and the Consequences of Pragmatic Adjudication" (2002) Utah Law Review 53 at 92 (criticizing the Court as "a bastion of political ideology cloaked in jurisprudential garb, masking a pragmatic approach to the doctrine of *stare decisis* [as] just another tool, pliable and flexible enough to reach any end").
[105] See Kozel, "Judicial Doctrine", *supra* note 104 at 414.
[106] *Supra* note 21.
[107] See *Carpenter*, *supra* note 21 at 17-18 (opinion of Chief Justice Roberts).

information on all the devices that connected to a particular cell site during a particular interval."[108] Such a search has been found to be an especially invasive investigative procedure given its wide and indiscriminate reach.[109] As these types of searches seriously implicate digital privacy, the Court has signalled that it will not revisit much of its questionable third party doctrine jurisprudence any time soon. This decision, I suggest, derives in no small part from the Court's under theorized and therefore unpredictable approach to *stare decisis*.

The Canadian approach to *stare decisis* is much more straight forward. As the Supreme Court recently concluded in *Canada (Attorney General) v Bedford*,[110] a constitutional precedent may be reconsidered if significant factual changes underlying the initial decision have occurred.[111] Although the Court has cautioned against liberal use of this exception in relitigating decisions based on complex social science evidence,[112] it is not difficult to imagine changes in technology "fundamentally shifting" the applicable privacy and security interests central to determining whether a search or seizure is reasonable. Importantly, the Court also held that even lower courts may reconsider Supreme Court precedents when the underlying facts of a constitutional case have fundamentally shifted.[113]

This approach, although still in its relative infancy, has much to commend itself to the field of digital privacy. First, it does not require a broad balancing of various factors to determine if a decision ought to be reconsidered. In the digital age, the facts underlying technologies shift frequently with significant implications for privacy. Being prohibited from reconsidering a

---

[108] *Ibid*.
[109] In the United States, see Brian Owsley, "The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance" (2013) 16 Journal of Constitutional Law 1. In Canada, see *R v Rogers Communications*, 2016 ONSC 70, 128 OR (3d) 692.
[110] 2013 SCC 72, [2013] 3 SCR 1101.
[111] *Ibid* at para 44. The Court has other reasons for overturning prior precedent. However, these factors operate independently to overturn prior precedents.
[112] See *R v Comeau*, 2018 SCC 15 at paras 30-34, [2018] 1 SCR 342.
[113] See *Bedford*, *supra* note 110 at para 44.

decision for other reasons is too rigid an approach to ensure a principled and up-to-date balancing of privacy and security interests in digital technologies. Second, as binding precedents from the Supreme Court on digital privacy issues are often outdated shortly after (or even when) rendered,[114] it is prudent to allow lower courts to conduct a novel balancing of privacy and security interests where the technology has fundamentally shifted. This ensures that judicial rules will not be frozen in time, waiting for the next Supreme Court decision to be rendered, which will typically occur many years after a technology has shifted.[115]

The Canadian approach to *stare decisis* in the constitutional context is not without its problems. As with most determinations related to digital privacy, there is an inherent trade-off between consistency in rule application and the need to ensure the law develops in a principled and expeditious manner. The Canadian approach to *stare decisis* certainly trades the former for the latter. Although all of these values are important, it must be kept in mind that it is unusually difficult for courts to keep pace with digital technologies, let alone render determinate rules to ensure principled development of the law. This trade-off between consistency and principled/expedient rule development therefore is a reasonable one in the context of crafting digital privacy rules.

(v) The Role of Interveners

Interveners are allowed to make submissions, typically at appellate courts, to help judges come to reasoned resolutions about legal issues.[116] Not only do interveners provide courts with

---

[114] See Daniel Scanlan, "Issues in Digital Evidence and Privacy: Enhanced Expectations of Privacy and Appellate Lag Times" (2012) 16 Canadian Criminal Law Review 301 at 312. As the author observes, "the time between when the technology first appears, some criminal use is made of it, police investigations occur, trials are held, and appeals are heard can be many years." When a judicial decision responds to a particularly fluid piece of technology, the result "may well be an appellate pronouncement of historical interest only."

[115] *Ibid*.

[116] See Benjamin Alarie and Andrew Green, "Interventions at the Supreme Court of Canada: Accuracy, Affiliation, and Acceptance" (2010) 48 Osgoode Hall Law Journal 381.

legal arguments, they also serve a separate but equally important role: correcting factual misunderstandings. As the literature has revealed in both Canada and the United States, the adversarial process is prone to miss or misunderstand relevant facts about digital technologies.[117] The "factual updating" provided by interveners is therefore important in ensuring that judicial development of a rule implicating a digital technology occurs in a principled manner.

Interveners in the United States frequently participate in hearings before appellate courts.[118] As several authors have observed, the Court allows virtually unlimited participation by interveners.[119] The digital privacy context is no exception. On average, fifteen interveners made written submissions at hearings involving the digital privacy issues canvassed in the Court's most recent digital privacy jurisprudence.[120] These submissions typically include detailed efforts to help courts understand the technologies relevant to the case before them.[121]

In Canada, interveners make submissions much less frequently,[122] and are much more restricted in their participation at the Supreme Court of Canada. Interveners other than Attorney

---

[117] See Chapter Two; Kerr, "Fourth Amendment", *supra* note 43.

[118] For an historical overview of the increased participation of *amici curiae* at the Court, see Benjamin Hopper, "Amici Curiae at the United States Supreme Court and the Australian High Court: A Lesson in Balancing Amicability" (2017) 51 John Marshall Law Review 81 at 84.

[119] See Omari Scott Simmons, "Picking Friends from the Crowd: Amicus Participation as Political Symbolism" (2009) 42 Connecticut Law Review 185 at 195; Joseph Kearney and Thomas Merrill, "The Influence of Amicus Curiae Briefs on the Supreme Court" (2000) 148 University of Pennsylvania Law Review 743 at 764. See also Allison Orr Larsen, "The Trouble with Amicus Facts" (2014) 100 Virginia Law Review 1757 at 1758 noting that amicus briefs have risen by 800% over the last 50 years.

[120] See *Jones*, *supra* note 17; *Carpenter*, *supra* note 21; *Riley v United States*, 134 S Ct 2473 (2014). Briefs submitted at the Supreme Court are accessible online. See American Bar Association, "16-402" (26 January 2018), online: <https://www.americanbar.org/groups/public_education/publications/preview_home/2017_2018_briefs/16-402/>; Electronic Privacy Information Centre, "Riley v California", online: <https://epic.org/amicus/cell-phone/riley/>; Electronic Privacy Information Centre, "United States v Jones", online: <https://epic.org/amicus/jones/>.

[121] *Ibid*.

[122] This conclusion derives again from looking at the proceedings of the most recent digital privacy cases in Canada. See *R v Morelli*, 2010 SCC 8, [2010] 1 SCR 253 (privacy interests implicated by computer searches); *R v Gomboc*, 2010 SCC 55, [2010] 3 SCR 211 (digital tracking of electricity consumption); *R v Cole*, 2012 SCC 53, [2012] 3 SCR 34 (whether accused had reasonable expectation of privacy in computer issued by employer); *R v Vu*, 2013 SCC 60, [2013] 3 SCR 657 (whether computer searches must be specifically authorized in a warrant); *R v Fearon,* 2014 SCC 77, [2014] 3 SCR 621 (searches of cell phones incident to arrest); *R v Spencer*, 2014 SCC 43, [2014] 2 SCR 212 (reasonable expectation of privacy in ISP subscriber information); *R v Marakah*, 2017 SCC 59, [2017] 2 SCR 608

Generals[123] are only permitted to write ten-page factums and are limited to speaking for a maximum of fifteen minutes if allowed to make oral submissions at all.[124] As a result, it is reasonable to expect the intervener's legal argument to take precedence over attempting to correct factual misunderstandings or providing courts with relevant "digital context." This relative restrictiveness in allowing interveners to make submissions can negatively affect the capacity of courts to render coherent digital privacy rules. Each countries jurisprudence on whether police should be allowed to search cell phones incident to arrest is exemplary.

Canadian trial and appellate courts made numerous technological mistakes when determining the relevant privacy and security interests relevant to determining the constitutionality of the search.[125] As discussed in Chapter Two, the Court in *R v Fearon*[126] did not consider how password and biometric evidence can prevent police from searching a device "promptly"[127] or how these features of cell phones implicate different constitutional rights such as the right against self-incrimination,[128] right to silence,[129] and other privacy interests.[130] It also did not adequately consider how destruction of evidence might be thwarted by turning off a cell phone, removing its battery, or placing it in a Faraday bag.[131] Moreover, the Court did not draw any distinction between

(reasonable expectation of privacy in text messages); *R v Jones*, 2017 SCC 60, [2017] 2 SCR 696 (definition of "intercept" under Part VI of the *Criminal Code*).

[123] See *Rules of the Supreme Court of Canada*, SOR/2002-156, s 42(5)(a).

[124] *Ibid*, s 42(5)(b). It is notable, however, that there is limited discretion to increase the pages allotted to interveners. It is unclear how often this discretion is exercised.

[125] See Chapter Two; Colton Fehr and Jared Biden, "Divorced from (Technological) Reality: A Response to the Supreme Court of Canada's Decision in *R v Fearon*" (2015) 20 Canadian Criminal Law Review 93; Colton Fehr, "Cell Phone Searches Incident to Lawful Arrest: A Case Comment on the Ontario Court of Appeal's Decision in *R v Fearon*" (2014) 60:3 Criminal Law Quarterly 343.

[126] *Supra* note 122.

[127] The benefits of being able to search a cell phone "promptly" is the main justification offered by the Court for allowing searches of cell phones. If the search is not done promptly, then evidence may be destroyed or leads lost. See *Fearon*, *supra* note 122 at paras 49, 59, 66.

[128] See Fehr and Biden, "Divorced", *supra* note 125 at 103.

[129] *Ibid*. Some phones are unlocked using voice recognition.

[130] *Ibid* at 104-05. Retina scans and fingerprints engage privacy interests in addition to those inherent in searching the phone itself.

[131] See Chapter Two.

allowing searches of "dumb" phones as opposed to smartphones despite the qualitatively different privacy interests implicated in such searches.[132]

The United States Supreme Court was able to avoid these factual errors in *Riley v California*.[133] As for the argument that the state needs to search cell phones incident to arrest to preserve evidence, the Court was aware of potential remote or programmed wiping of a phone,[134] as well as the possibility of data becoming encrypted upon the phone being locked.[135] It was also aware that data will be extremely difficult to access without the cell phone's password.[136] The Court further observed that turning a phone off, removing its battery, and/or placing the phone in a Faraday Bag provide potential responses to prevent deletion of data.[137] Although the Court correctly recognized that such techniques do not provide a "complete answer", these options were found to provide a "reasonable response" to concerns about losing evidence.[138] Substantial intervener submissions describing these technologies were available to the Court when balancing the relevant privacy and security interests relevant to searching cell phones.[139]

It is also notable that the ability of interveners to correct factual misunderstandings will be affected by the sheer number of available interveners. Such a consideration is likely attributable to a different consideration: size and economic status of the country within which the issue is being litigated. As the United States is roughly ten times the size of Canada,[140] it is no surprise that there are more interest groups, Non-Government Organizations, and law professors willing and able to

---

[132] *Ibid*. See also Jordan Fine, "Leaving Dumb Phones Behind: A Commentary on the Warrantless Searches of Smart Phone Data Granted in *R v Fearon"* (2015) 13 CJLT 171 at 180-81.
[133] *Supra* note 120.
[134] *Ibid* at 2486.
[135] *Ibid*.
[136] *Ibid* at 2486-87.
[137] *Ibid*.
[138] *Ibid*.
[139] *Supra* notes 120-23.
[140] "World Population Review" (7 December 2018), online: <http://worldpopulationreview.com/continents/north-america-population/>.

participate in the adversarial process. This greater number of participants contributes to the American appellate system's increased capacity to process complex and rapidly shifting facts. Thus, it is reasonable to expect a smaller judicial system to have greater difficulties understanding digital technologies. As a result, countries such as Canada should be *more*, not less generous in allowing intervener submissions in criminal procedure cases implicating digital privacy.

(b) Legislatures

(i) Models of Democracy

A state's choice to employ a parliamentary or presidential model of democracy can also impact the challenges governments face in crafting coherent and effective digital privacy laws. Beginning with the United States, two key features of their presidential model of democracy make it difficult to pass coherent digital privacy laws. First, it is uncommon for the House, Senate, and President's office to be held by the same party. This results in broad-based and individually tailored negotiations between Congressmen to attract a majority of votes in each house as well as presidential approval.[141] Second, individual Congressmen are not restricted in negotiating along party lines when discussing the shape of any proposed law. Instead, they primarily seek to appease their local constituents.[142] As a result, coming to consensus on any given proposed law is difficult in the American presidential model.[143]

These features of the American presidential model of democracy result in the frequent use of what are known as "omnibus bills".[144] These bills package together various unrelated laws into one general bill for government approval. This process allows the government to appease various

[141] See Louis Massicotte, "Omnibus Bills in Theory and Practice" (2013) 36 Canadian Parliamentary Review 13 at 14-16.
[142] *Ibid*.
[143] *Ibid*.
[144] *Ibid*.

different interests when negotiating the content of a variety of proposed laws, and typically limits the ability of a law to receive time for adequate debate or necessary scrutiny at the development stage.[145] As several authors have demonstrated, this model of rulemaking has resulted in a set of privacy rules where the governing standards employed for permitting various searches are frequently and substantially out of touch with empirical studies and normative ideals about reasonable expectations of privacy.[146]

Legislatures in a Parliamentary system are better situated to enact laws quickly and more coherently in response to the challenges of governing digital privacy, at least when sitting as a majority. Unlike legislatures in Presidential systems, those in Parliamentary systems generally will "not vote for their most preferred outcome since leaders have the resources to force party members to support or oppose a particular bill."[147] The incentives to toe the party line are much greater since it is necessary for the cabinet to maintain majority support of the legislature to maintain political power.[148] Where minority governments are common, however, it is likely that political bargaining will become the norm.

Given the predominantly four-party system that exists in Canada, a minority governing party will need to engage with only the party whose interests are most aligned with the governing party's interests to pass its desired law.[149] This significantly reduces the risks inherent in omnibus

---

[145] *Ibid*.
[146] See Slobogin, *Privacy at Risk*, *supra* note 45 at 183-85; Solove, *Nothing to Hide*, *supra* note 47 at 164; Murphy, "Politics of Privacy", *supra* note 45 at 495.
[147] See Jean-Francois Godbout, "Parliamentary Politics and Legislative Behaviour" in Luc Turgeon et al., eds, *Comparing Canada: Methods and Perspectives on Canadian Politics* (Vancouver: UBC Press, 2014) 171 at 173.
[148] *Ibid* at 175 citing Gary Cox and Mathew McCubbins, *Legislative Leviathan: Party Government in the House* (Berkeley: University of California Press, 1993).
[149] This will not always be the case. The Conservative government's attempts to pass lawful access legislation is a prime example. For a description of the perils of this experience, see Chapter Three. See also Christopher Parsons, "Stuck on the Agenda: Drawing Lessons from the Stagnation of 'Lawful Access' Legislation in Canada" in Michael Geist, ed, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (Ottawa: University of Ottawa Press, 2015) 257.

bill rulemaking. That is not to say, however, that a minority government will always be able to find another party aligned with its interests. In such a scenario, persistent minority governments will lead to significant stalemate in developing digital privacy rules. In fact, the most recent and substantial overhaul of digital privacy criminal procedure rules—the lawful access scheme passed in 2014—occurred only after a majority government came into power, despite a decade of attempts to pass such a scheme under Liberal and Conservative minority leadership.[150] The struggles to pass these laws while prior minority governments were in power suggests that negotiation on digital privacy issues was not fruitful for political reasons.[151]

This difficulty aside, a general lesson may be drawn for legislatures operating in similar situations as their Canadian and American counterparts. Parliamentary systems will, especially when the governing power holds a majority, be better situated to draft efficient and coherent bodies of law regulating the field of digital privacy. Presidential systems, such as exists in the United States, are less likely to pass laws coherently, especially if their political system and culture result in heavy use of omnibus bills. In such circumstances, the legislature is at risk of developing digital privacy laws in a patchwork and thus less coherent manner.

(ii) Majoritarianism

Although greater centralization of legislative power in Parliamentary systems of democracy theoretically makes it easier to pass coherent rules, this centralization of power also risks a powerful Prime Minister succumbing to majoritarian biases. This has the potential to significantly undermine digital privacy and other constitutional interests in the name of broad public appeals to be "tough on crime".[152] Where institutional actors—such as a judiciary utilizing

[150] See Chapter Three.
[151] *Ibid*.
[152] See generally Daniel Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy" (2007) 44 San Diego Law Review 745.

judicial review or civil rights groups seeking to influence the development of the law—are not able to respond to majoritarian policies this could create significant problems for the efficacy of criminal procedure rules implicating digital privacy. Although Canadian courts and civil rights groups have thus far responded effectively to majoritarian demands, the Canadian experience is not extensive enough to draw definitive conclusions. The lawful access experience implicated the rights of a broad socio-economic class. Where proposed laws are directed at the poor, it is unclear that civil society or the courts will respond in the same way.[153]

One of the virtues of the presidential system is that it is well-tailored to protect against majoritarian concerns.[154] The fact that all laws must be approved by the House, Senate, and the President makes it much more likely that critical perspective will influence the development of proposed laws. Similarly, the fact that each member of Congress is not required to toe the party line makes it more likely that laws will be decided based on their merits.[155] It is true that American federal laws frequently end up passed as omnibus bills, greatly lessening the degree to which legislatures can be expected to strike coherent balances between privacy and security interests.[156] However, the practice of omnibus bills is one that may be abolished at the federal level, as it has been in many American states,[157] which would theoretically allow for greater realization of the benefits of presidential systems.

---

[153] See Steven Penney, "Fear the Fearon? Searches of Digital Devices Incident to Arrest" Webcast (6 February 2015) online: <https://ualawccsprod.srv.ualberta.ca/index.php/webcasts/811-fear-the-fearon-searches-of-digital-devices-incident-to-arrest-professor-steven-penney>. Penney observes a difference in judicial privacy protections in cases where upper-class citizens' privacy is implicated (ISP subscriber information) and those where lower-class privacy interests are at issue (searches of cell phones incident to arrest).

[154] See Neil Komesar, *Imperfect Alternatives: Choosing Institutions in Law, Economics, and Public Policy* (Chicago: University of Chicago Press, 1994) at 220-21 responding to the competing view expressed by Jonathan Macey, "Transaction Costs and the Normative Elements of the Public Choice Model: An Application to Constitutional Theory" (1988) 74 Virginia Law Review 471 at 509-10.

[155] As I discuss below, however, this point is subject to the political system being relatively free of lobbyist influence, a condition which does not describe the United States.

[156] See the discussion in Part II(b)(i).

[157] For a review, see Massicotte, "Omnibus Bills", *supra* note 141 at 14-16.

It is therefore reasonable to believe that majoritarian concerns may arise in the context of criminal procedure rules affecting digital privacy. Parliamentary systems are especially vulnerable to majoritarian concerns when sitting as majorities. As such, protections against majoritarian policies will often need to come from courts exercising judicial review or civil society lobbying government for increased digital privacy protections.[158] To the contrary, the American presidential system's requirement that laws pass through Congress and the President provides more protection from legislative tendencies to pass unbalanced digital privacy rules. The American presidential system is nevertheless particularly vulnerable to another threat to passing balanced digital privacy rules.

(iii) Lobbying

Lobbying is the process of articulating one's preferences to government in order to influence public policy.[159] Although lobbying is a controversial feature of politics in general, American scholars contend that lobbying ought not give rise to governance concerns in the criminal procedure context. They offer two reasons. The first relies on the structure of the American Constitution. The second relies on the unique social context within which criminal procedure rules implicating digital privacy are enacted. As I explain below, both rationales are unconvincing. This in turn should give rise to concern in the American context that digital privacy rules will develop either in line with special interests or (more likely) not develop at all, creating grey area within which special interests may be served. In contrast, the Canadian Parliamentary model is much better placed to thwart undue special interest influence.

[158] See Chapter Three; Parsons, "Stuck on the Agenda", *supra* note 149. We discuss civil society's largely successful attempt at blocking particularly invasive attempts at facilitating lawful access laws.
[159] See Gerry Ferguson, *Global Corruption: Law, Theory & Practice*, 3rd ed (Victoria: University of Victoria Press, 2018) at 890. See 892-93 for a broader discussion of the term.

Scholars contend that the structure of the American Constitution checks rent-seeking behaviour by raising the costs for participants engaged in lobbying.[160] The Constitution purportedly achieves this end in three ways. First, it employs a bicameral legislature, each branch of which has veto power over whether a bill becomes law. To influence the passing of a law, then, is twice as difficult as in a unicameral legislature.[161] Second, the Constitution allows the President to overrule any law passed by Congress which, in turn, requires increased Congressional support to override the President's decision.[162] Finally, the American Constitution employs a strong model of judicial review which in theory allows judges to interfere where rights-invading lobbying inappropriately shapes legislation.[163]

Each of these arguments is problematic. As Neil Komesar explains, when the Senate and House of Representatives became multiple venues to lobby against, it became more expensive to participate in politics, and thus only smaller, better organized groups could participate.[164] This privileging of wealthy parties coincided with a greater need to receive large donations to finance future campaigns. This, in turn, made Congress more beholden to lobbyist interests.[165] Moreover, the lobbyists that can be expected to provide defendant perspectives on criminal procedure rules—such as civil liberties groups—are unlikely to be heard as they are woefully underfunded as compared to law enforcement agencies and other invested commercial groups.[166]

---

[160] See Macey, "Transaction Costs", *supra* note 154.
[161] *Ibid* at 509-10.
[162] *Ibid* at 510.
[163] *Ibid*.
[164] See Komesar, *Imperfect Alternatives*, *supra* note 154 at 220-21. See also Jerry Mashaw, "Public Law and Public Choice: Critique and Rapprochement" in Daniel Farber and Anne O'Connell (eds), *Research Handbook on Public Choice and Public Law* (Cheltenham: Edward Elgar Publishing Ltd, 2010) at 30.
[165] See Raj Chari, Gary Murphy, and John Hogan, "Regulating Lobbyists: A Comparative Analysis of the United States, Canada, Germany and the European Union" (2007) 78 The Political Quarterly 422.
[166] See Murphy, "Politics of Privacy", *supra* note 45 at 505-06.

Arguments relying on the structure of the American Constitution may also be reversed. The problem in the digital privacy context is that criminal procedure rules are frequently in need of updating. Although the bicameral legislature can prevent lobbyists from successfully lobbying for adoption of favourable rules, such a scheme also makes it easier to *prevent* privacy protecting rules from being adopted, as the bicameral legislature ensures multiple venues may be lobbied against to block proposed rules. As protecting digital privacy typically requires frequent updating of rules, the American Constitution makes it more difficult for groups to convince politicians to pass any rules.[167] This in turn results in judges being required to craft digital privacy laws in the context of broad legislative or common law powers. These rules will lag behind technological development allowing for privacy invasive practices to go inadequately regulated.

As for allowing courts to deal with lobbying via the Constitution, it is questionable whether judges should combat such "minoritarian" bias. As Komesaar observes, "[a]ny serious attempts to root out minoritarian bias by judicial review would confront courts with the overwhelming task of examining virtually all forms of legislation and remaking all the public policy decisions inherent in that legislation."[168] He continues, "[t]he scale of activity inherent in such an endeavor would completely overwhelm the judicial system as presently constituted or even as feasibly augmentable."[169] In other words, to require counsel to investigate lobbying practices in the requisite amount of detail and for a court to decide what constitutes an "inappropriate" degree of lobbying both overworks the justice system and inappropriately politicizes the legal process.

---

[167] As one author observes, "[t]he regulated industry of law enforcement has a concentrated interest in reducing regulation - pushing for fewer warrants, less onerous reporting requirements, and so on." See Peter Swire, "*Katz* is Dead: Long Live *Katz*" (2004) 102 Michigan Law Review 904 at 914.
[168] See Komesar, *Imperfect Alternatives*, *supra* note 154 at 229. See also 82.
[169] *Ibid.*

Even if the American Constitution fails to protect against minoritarian bias, the fact that digital technologies are mainly possessed by the wealthy may serve to counter law enforcement and corporate interests.[170] Yet, as discussed in the preceding Chapter, this position ignores the extent to which greater use of digital technologies by a major customer, such as a federal government, may equate to significant economic benefits for private corporations. Increased lobbying may also be beneficial for law enforcement agencies seeking greater police powers, or lesser privacy protections, to meet investigatory challenges within their respective budgets. It is likely for these reasons that private corporations and law enforcement agencies have been shown to have significant influence in the creation of many privacy-restrictive American criminal procedure rules and blocking many other privacy protective rules.[171]

Despite similar regulations of lobbyists in the United States and Canada,[172] the Canadian Parliamentary system has proven significantly less susceptible to lobbying in the criminal procedure context.[173] Canada's experience with its lawful access legislation is exemplary. Legislative attempts to pass such legislation spanned from the late 1990s until 2014.[174] As discussed in detail in Chapter Three, lobbying concerns were either non-existent in the context of private corporations or, where present due to law enforcement lobbying, were adequately met by concerned members of civil society.[175]

This result is arguably counterintuitive given Canada's *de facto* unicameral legislature. As this system requires that lobbyists focus on one entity, not two, it should be easier to convince

[170] See Kerr, "Fourth Amendment", *supra* note 43 at 887.
[171] See Murphy, "Politics of Privacy", *supra* note 45 at 504-07, 535-36; David Sklansky, "Two More Ways Not to Think about Privacy and the Fourth Amendment" (2015) 82 The University of Chicago Law Review 223 at 227; Swire, "*Katz* is Dead", *supra* note 167 at 914-15; William Fenrich, "Common Law Protection of Individuals' Rights in Personal Information" (1996) 65 Fordham Law Review 951 at 958.
[172] For an extensive review and comparison, see Ferguson, *Global Corruption*, *supra* note 159 at 912-39.
[173] See Chari et al., "Regulating Lobbyists", *supra* note 165.
[174] See Chapter Three.
[175] *Ibid*.

legislatures to pass laws. As discussed earlier, legislatures in Canadian Parliament tend to toe the party line to ensure the government maintains political power.[176] This means fewer legislatures are able to be targeted by lobbyists compared to the American context, where individual legislatures may succumb to lobbyist demands to help raise funds for the next election.[177] The omnibus bill process explained earlier also makes it likely that individual legislatures can influence the shape of any particular law. The absence of such a process in Canada likely makes lobbying in the Canadian context significantly more difficult.

III. A Normative Approach to Governing Digital Privacy

The comparison between the American and Canadian experiences shows that the ability of courts and legislatures to implement efficient, coherent, and even-handed digital privacy laws is impacted by a variety of factors. These factors should be balanced against one another to come to meaningful conclusions about what role courts and legislatures should play in crafting digital privacy rules. In many cases, the challenge will be not which institution should govern to the exclusion of the other. Instead, individual countries will need to determine how courts and legislatures can each operate to their strengths and best work together to ensure effective criminal procedure rules implicating digital privacy are put in place.[178]

The latter point is especially important as the problems facing both courts and legislatures are not of a static nature. In other words, courts and legislatures may be relatively better equipped to address digital privacy concerns under different institutional conditions. For instance, a minority legislature may be unable to gain adequate consensus to grant necessary police powers.[179] Courts

[176] See Godbout, "Parliamentary Politics", *supra* note 147 at 173-75.
[177] See Ferguson, *Global Corruption*, *supra* note 159 at 910.
[178] This is the predominant conclusion drawn in the literature. See Solove, "Fourth Amendment", *supra* note 90; Murphy, "Politics of Privacy", *supra* note 45; Sklansky, "Two More Ways", *supra* note 171.
[179] The lawful access debate in Canada is exemplary. For a review, see Chapter Three; Parsons, "Stuck on the Agenda", *supra* note 149.

might also receive less help from interveners in times of economic hardship or where other issues are dominating the legal/legislative agenda. As such, one of the main lessons to take from the above comparison is that crafting digital privacy rules in an efficient, coherent, and even-handed manner requires courts and legislatures to be flexible in determining which institution makes a rule. As institutional conditions can change quickly and unexpectedly, courts and legislatures should both be able to receive necessary information to craft well-informed and prompt rules.

The above factors are also not exhaustive. It is implicit in "small n" comparative studies that the conclusions offered are tentative. This allows for any normative theory to be tested as research into the broader question of institutional capacity to respond to the challenges of governing state intrusions into digital privacy accelerates. Certainly, there would be much to gain from examining the experiences of other comparable countries. To my knowledge, however, there is inadequate research to facilitate further comparison at this time.[180] As the above review illustrated, comparison requires thick description of the relevant countries' experiences. Conducting such a review in a third country would therefore require significant engagement with that country's experience crafting criminal procedure rules implicating digital privacy.

Several other factors may nevertheless be highlighted as potentially relevant even if at this point their value is difficult to predict. First, it is possible that the relative politicization of a countries' judicial appointments might affect the ability of courts to devise coherent and even-handed digital privacy rules. In that regard, it is noteworthy that the Canadian judicial system has been found to be significantly less politicized than its American counterpart.[181] However, it is

[180] As Erin Murphy writes, "[w]hereas Europe has embraced a coherent, comprehensive approach to privacy regulation, the United States has largely relied on independent enactments largely tailored to particular sectors or interests." However, she does not elaborate as to the institutional reasons underlying the different quality of privacy rules in Europe. See Murphy, "Politics of Privacy", *supra* note 45 at 495.

[181] See for instance David Weiden, "Judicial Politicization, Ideology, and Activism at the High Courts of the United States, Australia, and Canada" (2011) 64 Political Research Quarterly 335 at 345. Others, however, have speculated that the political culture that allowed for a depoliticized court evaporated under Prime Minster Harper's terms in

difficult to tease out a relationship between political leanings of individual judges and any effect on digital privacy rules. It may be that privacy, and digital privacy especially, cuts through the conservative-liberal divide.[182]

Second, any increased role for judges in crafting digital privacy rules may negatively impact substantive equality. As Dana Raigrodski notes, "reasonableness and common sense have always been assigned a race (white), a gender (male), and a class (wealthy)."[183] If judges developing the law are not taking into account considerations of race, gender, and class, among other typical equality considerations,[184] the law will undoubtedly serve to perpetuate historical injustices. Studies of judicial bias, although limited, suggest that judges harbour the same implicit racial biases as other citizens, although they are able to compensate for such biases when race is directly brought up in the proceedings.[185] To the extent that these considerations can be teased out for study, they may very well have a significant impact on whether judges should be trusted to craft fair and reasonable rules with respect to constitutional rights.

Third, there is no known research on the question of how legislative committees engage with the challenge of developing adequate understandings of digital technologies before recommending criminal procedure rules to the legislature. If the committee system in a country is unable to develop a complete understanding of digital technologies—due to inadequate staff,

---

governance. See Craig Forcese, "Politicized Judicial Appointments & the Absence of Checks and Balances" *Public Law Blog* (28 May 2014).

[182] In that regard, it is prudent to recall from the above discussion that the Supreme Court of the United States in *Jones*, *supra* note 17 and *Carpenter*, *supra* note 21, witnessed Republican appointees render privacy protecting rulings.

[183] Dana Raigrodski, "Reasonableness and Objectivity: A Feminist Discourse of the Fourth Amendment" (2008) 17 Texas Journal of Women and the Law 153 at 187.

[184] American courts have been heavily criticized in this regard. See for instance, Anthony Thompson, "Stopping the Usual Suspects: Race and the Fourth Amendment" (1999) 74 New York University Law Review 956; Janice Nadler, "No Need to Shout: Bus Sweeps and the Psychology of Coercion" (2002) 202 Supreme Court Review 153; Lee, "Reasonableness", *supra* note 44 at 1151 (see the extensive sources cited in footnote 83).

[185] See Jeffrey Rachlinskiet al., "Does Unconscious Racial Bias Affect Trial Judges?" (2009) 84 Notre Dame Law Review 1195; Justin Levenson, Mark Bennett, and Koichi Hioki, "Judging Implicit Bias: A National Empirical Study of Judicial Stereotypes" (2017) 69 Florida Law Review 63.

resources, or time allotted to study a matter[186]—it will likely contribute to the incoherency commonly found in digital privacy criminal procedure legislation. A similar result may occur if committee members are frequently captured by third party interests[187] or are expected to toe the party line.[188] In both scenarios, committees cannot reasonably be expected to objectively investigate legislative proposals. Given the dearth of academic consideration of this point, investigating the role of committees in each country requires separate treatment before meaningful comparison can be undertaken.

Finally, it must be recognized that changes to broader aspects of legal systems—such as rules involving the interpretation of constitutional documents, *stare decisis*, exclusion of evidence, or the role of interveners in appellate proceedings—clearly involve competing policy considerations. In other words, making the changes recommended above may involve spillover effects that outweigh any benefits that may accrue to digital privacy criminal procedure rules. Suffice it to say that broader consideration of the costs of changing generally applicable rules or frameworks could deter a polity from adopting the changes recommended here. This does not, however, take away from the purpose of this Chapter: identifying factors relevant to determining whether courts or legislatures are better equipped to govern digital privacy in the criminal procedure context.

Conclusion

[186] American Congress members from both major parties have lamented the fact that committee staffing has received significant cuts over the past few decades, nearly 35 percent from the period 1994-2014. See Bill Pascrell, "Why is Congress so Dumb?", *Washington Post* (11 January 2019), online: < https://www.washingtonpost.com/news/posteverything/wp/2019/01/11/feature/why-is-congress-so-dumb/>; Bruce Bartlett, "How Congress Used to Work: The Deep Roots of Republicans' Failure on Capitol Hill", *Politico Magazine* (4 April 2017), online: < https://www.politico.com/magazine/story/2017/04/how-congress-used-to-work-214981>.
[187] *Ibid*.
[188] David Docherty, *Legislatures* (Vancouver: UBC Press, 2005) at 130.

Comparing the Canadian and American experiences has exposed several factors that impact each countries' judicial and legislative ability to construct efficient, coherent, and even-handed digital privacy rules. From the perspective of the judiciary, entertaining debates about the proper method for interpreting a constitution can lead to less determinate rules. Moreover, utilizing broad and flexible language when drafting a constitutional protection against state searches and seizures is preferable to imposing rigid standards as the latter are likely to impede proper balancing of privacy and security interests. Constitutional remedies should be similarly flexible to avoid forcing judges to choose between excluding valuable evidence, which typically results in an acquittal, and recognizing a reasonable expectation of privacy. The doctrine of *stare decisis* must also be relatively open to allowing rule change in the field of digital privacy. Finally, the adversarial process should be augmented to allow interveners to make extensive submissions before courts, with an emphasis on correcting factual misunderstandings.

With respect to relevant legislative considerations, the model of democracy employed can impact the challenges governments face in crafting coherent and efficient digital privacy criminal procedure rules. Although a bicameral legislature provides a counter to majoritarian concerns, it also makes it significantly more difficult to pass laws. In the American presidential system, this has resulted in lawmakers utilizing patchwork methods of law making which in turn often leads to incoherent law. Although the *de facto* unicameral legislature employed in Canada allows for more focused law making, it also centralizes power in the majority political party leading to significant majoritarian concerns. The fact that there are fewer paths for lobbyist activity in Canada's parliamentary system nevertheless mitigates concerns that special interest groups will unfairly influence digital privacy rules. The multiple venues available for lobbying in the United States

makes blocking privacy-protecting rules significantly easier, while increased concerns about campaign financing injects significantly more lobbyist influence into the American system.

Given the relatively underdeveloped state of the literature, these considerations should not be viewed as exhaustive. Other potentially fruitful areas of study include the degree to which judges exercising constitutional powers make politically charged decisions or are prone to implicit bias. Another area in need of study concerns the differences in the ways legislatures study laws before proposing them to legislative bodies. Our collective understanding of the challenges of governing digital privacy in the criminal procedure context would also greatly benefit from conducting further comparison with other jurisdictions. When the empirical evidence is in place to conduct such a study, the above comparison of Canadian and American capacity to govern the field of criminal procedure in the digital age may be tested and, if necessary, revised to provide further guidance for similarly situated polities.

Chapter Six

Governing Digital Privacy in Canada

Introduction

By comparing the difficulties American and Canadian courts and legislatures have encountered when creating rules surrounding digital technologies, the preceding Chapter identified several factors relevant to institutional design strategies. The aim of this Chapter is to apply this framework to determine how Canadian courts and legislatures should approach governing state intrusions into digital privacy. My model for determining institutional competence for crafting digital privacy rules requires that courts and Parliament enter into a form of institutional dialogue. Under this approach, Parliament should modify the adversarial framework to allow courts to better understand digital technologies and as a result exercise significant, but by no means exclusive, control over digital privacy rules in the criminal procedure setting.

Parliament, on the other hand, should take a more cautious approach when legislating rules. Although Parliament is theoretically able to pass prompt and coherent legislation, the reality is that it is not doing so any better than courts. As courts must deal with technologies as they arise, Parliament should set up conditions that allow courts to make expedient and coherent rules. That is not to say that Parliament should never legislate. Where technologies are reasonably stable,

legislative rules may provide *ex ante* guidance, which is preferable to judicial development of rules *ex post*. Where the technology is rapidly advancing, however, Parliament should legislate more cautiously, taking advantage of tools such as sunset clauses to ensure rules are frequently returned to Parliament for updating. Where Parliament is unable to act, allowing courts to interpret broad police powers in accordance with the *Charter* will provide a reasonable backstop.

I. Modifying the Adversarial Framework

Given the evidentiary shortcomings that tend to arise when courts decide issues relating to complex digital technologies, it is necessary to consider options that better equip courts to decide future cases. In my view, courts should be aided in three primary ways. First, Parliament should utilize the reference procedure when requiring courts to make or decide on the constitutionality of a rule concerning a complex digital technology. Second, Parliament should ensure that up-to-date and independent expert reports describing technologies that are expected to come before courts are accessible to counsel. Finally, the courts should routinely grant extended written and oral submissions to interveners appearing as *amicus curiae* at appellate court hearings.

(a) Reference Procedure

The federal government may refer to the Court virtually any question of law pursuant to section 53 of the *Supreme Court Act*.[1] The provinces are to be notified of any question in which they have a "special interest" and are entitled to make submissions before the Court.[2] The Court also has jurisdiction to notify any "interested parties" of the proceedings and allow those parties to make submissions.[3] It may even direct that specific counsel argue the case brought before the

[1] RSC 1985, c S-26 [*Supreme Court Act*]. It is notable that the constitutions of several jurisdictions bar such a possibility. For instance, Article III of the United States Constitution—known as the "case" or "controversy clause"—prohibits legislatures from sending references to American courts. Australia's Constitution contains a similar restriction. See *Commonwealth of Australia Constitution Act*, adopted 9 July 1900, ss 75-76.
[2] *Ibid*, s 53(5).
[3] *Ibid*, s 53(6).

Court.[4] Finally, the Court may bring forward any "papers or other proceedings had or taken before any court, judge or justice of the peace, and that are considered necessary with a view to any inquiry, appeal or other proceeding had or to be had before the Court."[5]

Utilizing the reference procedure in cases where courts are left to make or decide on the constitutionality of a rule with respect to complex digital technologies has several benefits. First, the reference procedure can avoid the adversarial system's tendency to hear insufficient evidence from limited parties.[6] In the context of a reference, the Court may hear from any parties or take evidence from any proceedings. The Court may even call on parties to argue a particular legal issue. This procedure therefore allows the Court to build the best possible evidentiary record for deciding a legal issue. Importantly, utilizing the reference procedure also ensures that impecunious accused persons are not required to facilitate expensive expert testimony concerning a digital technology to contextualize any intrusion onto privacy interests.

Second, a reference can ensure that courts deciding issues pertaining to novel search technologies do not render decisions of "historical interest only."[7] Bypassing first instance trials and provincial appeals helps ensure that rules concerning novel search technologies are made within a reasonable amount of time. This benefit is exemplified by observing the judicial development of the law of cell phone searches incident to arrest discussed in Chapter Two. The

---

[4] *Ibid*, s 53(7).
[5] *Ibid*, s 55.
[6] See Centre for Constitutional Studies, "The Reference Procedure: The Government's Ability to Ask the Court's Opinion", online: <https://ualawccsprod.srv.ualberta.ca/>. Notably, not all references achieve this aim. For instance, *Reference re ss. 193 and 195.1(1)(C) of the Criminal Code (Man.)*, [1990] 1 SCR 1123, 68 Man R (2d) 1 was overturned in large part due to an inadequate evidential record. See *Canada (Attorney General) v Bedford*, 2013 SCC 72, [2013] 3 SCR 1101. Yet, as Carrisma Mathen observes in her book, *Courts Without Cases: The Law and Politics of Advisory Opinions* (Oxford: Hart, 2019) at 151, references allow for "an enormous amount of material" to be submitted in proceedings which often will not occur in the normal course of litigation.
[7] See Mathen, *Courts Without Cases*, *supra* note 6 at 97 citing *Attorney-General for Manitoba v Manitoba Egg and Poultry Association et al*., [1971] SCR 689, 19 DLR (3d) 169. See also Daniel Scanlan, "Issues in Digital Evidence and Privacy: Enhanced Expectations of Privacy and Appellate Lag Times" (2012) 16 Canadian Criminal Law Review 301 at 312.

first judicial decision to address this issue arose in 2005.[8] Although the technology of cell phones improved dramatically between 2005 and 2014 when the Court rendered its decision in *R v Fearon*,[9] it was certainly possible to foresee that cell phones would come to have basic features, such as password and biometric protection, which would make prompt access difficult without help from the user. It was also possible to foresee cell phones becoming "mini-computers". As such, a reference to the Court in the mid-2000s could have resulted in an informed legal decision that fully canvassed cell phone technology and would have remained relatively current even today.

Finally, the reference procedure ensures that privacy issues are decided by a neutral arbitrator. Scholars have observed that courts are better suited than legislatures to govern privacy with respect to disadvantaged minorities such as criminal accused.[10] However, it may be countered that this concern is counterbalanced by the fact that courts are institutionally less capable of developing an informed evidentiary record.[11] By utilizing the reference procedure, however, these concerns are assuaged. Not only does the court ensure that the issue is decided by a neutral third party, it is also provided with significantly higher informational capacities than those typically provided by the adversarial system.

Despite the above benefits, the fact that the Court's answer to a reference question is not binding on lower courts arguably means that the reference process will not affect how lower courts approach digital technology cases.[12] Courts may simply ignore reference decisions and decide the

---

[8] See *R v Giles*, 2007 BCSC 1147, 77 WCB (2d) 469. Although decided in 2007, the facts of the case are from 2005.
[9] 2014 SCC 77, [2014] 3 SCR 621.
[10] See John Hart Ely, *Democracy and Distrust* (Cambridge: Harvard University Press, 1980) at 135-79; Donald Dripps, "Criminal Procedure, Footnote Four, and the Theory of Public Choice; or, Why Don't Legislatures Give a Damn About the Rights of the Accused?" (1993) 44 Syracuse Law Review 1079 citing footnote four of *United States v Carolene Products Company*, 304 US 144 (1938).
[11] See Steven Penney, "Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach" (2007) 97 Journal of Criminal Law and Criminology 477 at 501; Steven Penney, "The Digitization of Section 8 of the *Charter*: Reform or Revolution?" (2014) 67 Supreme Court Law Review 505 at 531.
[12] See *Reference re Remuneration of Judges of the Provincial Court*, [1998] 1 SCR 3 at para 10, 155 DLR (4th) 1 [*Remuneration*].

issue based on the factual record before them. This criticism ignores the Court's conclusion that reference decisions are "of highly persuasive weight" which, in practice, are followed as if they were normal cases.[13] In fact, no lower court has ever exercised its discretion to ignore a reference decision.[14] As such, it is reasonable to conclude that such decisions would be followed by lower courts unless the technology at issue changed in a legally relevant way.[15]

Second, it may be argued that use of the reference procedure unduly sacrifices the benefit of having multiple courts opine upon the legality of searching a digital device. This criticism is of limited merit. First, courts tend to make their decisions with respect to the legality of searching a digital device in an inadequately informed evidentiary environment. Any rules developed in this context are therefore of limited utility. Second, the reference procedure permits the Court to draw upon a variety of perspectives. Not only will the Crown raise arguments, but interveners may also apply to, or be solicited by, the Court to make submissions, and experts may be called to provide relevant testimony. Therefore, the benefits of having multiple lower court opinions are significantly offset. Third, requiring that resources be concentrated in one hearing is far more efficient than bringing arguments (some of which are bound to overlap) before multiple courts. As such, the benefits of utilizing the reference procedure when courts must make or decide on the constitutionality of a rule with respect to complex technologies likely outweigh any costs.

Third, it may be argued that there are political obstacles that make this proposal unlikely to work in practice. In other words, it may be difficult to convince legislatures to send digital privacy issues to the courts via the reference procedure. The reference procedure nevertheless

---

[13] *Ibid*. See also Mathen, *Courts Without Cases*, *supra* note 6 at 192-233.
[14] See Peter Hogg, *Constitutional Law of Canada* (Toronto: Thomson Reuters Canada, 2009) at s 8.6(d). Although it is notable that courts have utilized different constitutional principles, or significantly changed facts, to avoid following a prior Supreme Court of Canada precedent. See generally *Bedford*, *supra* note 6.
[15] For a detailed and persuasive analysis, see Mathen, *Courts Without Cases*, *supra* note 6 at 192-233.

provides a process similar to a trial wherein the government can defend its preferred method for governing a digital technology. As such, a responsible legislature should view the reference process as more pragmatic than expending significant resources on multiple trials wherein a rule will be subject to constitutional challenge and/or developed with inadequate evidence.

Finally, it may not be obvious how Parliament would raise digital privacy reference questions to the Court. Depending on the nature of the question, Parliament may simply propose hypothetical questions for the Court to answer. This would be most efficient if the relevant police power derives from the common law or fits into a broadly crafted police power such as the general warrant under section 487.01 of the *Criminal Code*. In other instances, Parliament may want to propose a legislative police power which it anticipates passing if found constitutional. Such a proposal could take the form of any other statutory police power.

(b) External Aid

As many digital cases will not involve making or deciding on the constitutionality of a rule, the reference process is of limited utility. Instead, courts will need assistance applying established rules to complex digital facts. As such, it is necessary to find other means for courts and counsel to learn about relevant digital technologies. One way of addressing this issue is to provide counsel with independent, up-to-date, and readily available information about digital technologies expected to come before the courts. This proposal is obviously vague and raises at least two general questions. First, what types of questions would courts want answered? Second, who would counsel turn to for independent advice?

The digital jurisprudence discussed in the preceding chapters illustrates the types of questions courts would want answered. Determining how a search takes place, when the search may be thwarted, and the nature of the privacy and law enforcement interests implicated were all

integral to deciding the constitutional issues. As technologies are generally in development long before they are released, these questions could have been answered at an early stage.

Take again the example of searching cell phones incident to arrest. As the first smartphone was developed in 1992,[16] it is reasonable to conclude that those in the industry could have predicted the mass adoption of smartphones by the time a court first decided the issue in 2007.[17] Likewise, password and biometric security features have long been available to computer users. Given the increased privacy interests implicated by modern cell phones, it was reasonable to assume that the technology would develop in a manner that would make it increasingly difficult for police to promptly enter cell phones or prevent destruction of evidence.

Although experts can be called at trial to serve a similar function, the adversarial system provides no guarantee that the Crown or defence will call such evidence.[18] This is especially problematic as courts operating within the Canadian adversarial model are not permitted to call their own experts, as is possible in some civil[19] and common law[20] jurisdictions. Even if Canadian courts could call their own experts, this sort of aid may not be desirable from an economic standpoint as frequent resort to experts would be expensive. Given the increased frequency with which judicial decisions can be expected to implicate complex digital technologies, it is desirable to think of less costly ways for courts to avail themselves of necessary evidence.

To this end, it may be prudent for Parliament to task an independent institution with providing detailed and up-to-date overviews of technologies which are expected to come before

---

[16] The first smartphone was developed fifteen years before the first iphone was released. See Steven Tweedie, "The World's First Smartphone, Simon, was Created 15 Years before the Iphone" *Tech Insider* (14 June 2015), online: <http://www.businessinsider.com/worlds-first-smartphone-simon-launched-before-iphone-2015-6>.

[17] See *Giles*, *supra* note 8, which was the first case to decide the issue.

[18] See the extensive review provided in Chapter Two, Part III.

[19] For instance, see s 404 of the *German Code of Civil Procedure* (5 December 2005).

[20] For instance, see s 53 of the United States *Federal Rules of Civil Procedure*, as amended 1 December 2016. The appointment of law and technology expert Lawrence Lessig as a "special master" (who serves effectively as an expert witness) proved useful in the landmark digital case of *United States v Microsoft Corporation*, 253 F 3d 34 (2001).

the courts. Counsel could then rely on this evidence during a trial. An institution that would be suitable for providing such advice would be the Office of the Privacy Commissioner of Canada (OPC), or other similar provincial bodies.[21] The OPC operates independently from government,[22] and its purpose is to "protect and promote the privacy rights of individuals."[23] Although its mandate is currently restricted to overseeing compliance with Canada's main privacy acts,[24] their office could be tasked with providing detailed overviews of technologies which are expected to arise in the jurisprudence.[25] Indeed, the OPC would be well suited to such a role given its expertise in issues relating to privacy which, in today's day and age, it is reasonable to assume includes an in-depth knowledge of complex digital technologies.

Three criticisms of this proposal merit comment. First, as the OPC has a mandate of *protecting* privacy, it may be perceived as biased against legitimate security interests. Either explicitly or implicitly, those researching the relevant digital technologies may conduct research that they believe tends to bolster privacy-based arguments. This problem could, however, be offset in two ways. First, Parliament could explicitly require that the OPC conduct this research in a neutral manner. Second, even if the research ignored security interests, the Crown could still call its own experts in reply. As the Crown has significant resources to expend vis-à-vis individual

---

[21] In Alberta, for instance, see "Office of the Information and Privacy Commissioner of Alberta", online: <https://www.oipc.ab.ca/>. I do not mean to suggest that the various offices of privacy commissioners would be the only suitable institution. The now disbanded Law Reform Commission of Canada would also have been a suitable candidate. As it is no longer in existence, however, I will not entertain this potential avenue for addressing the problems raised by digital technologies and the adversarial system.

[22] Office of the Privacy Commissioner of Canada (OPC), "Who we are", online: <https://www.priv.gc.ca/en/about-the-opc/who-we-are/>.

[23] *Ibid*.

[24] *Ibid*. The OPC particularly oversees the *Privacy Act*, RSC 1985, c P-21 [*Privacy Act*] and *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*].

[25] For instance, the OPC provided an exemplary document describing what IP addresses could reveal about individual internet users. See Office of the Privacy Commissioner of Canada, "What an IP Address Can Reveal About You" (May 2013), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/>. Unfortunately, only one court cited such a document. See *R v Cuttell*, 2009 ONCJ 471 at para 24, [2009] OJ No 4053.

criminal accused, it does not seem overly burdensome to require it to call rebuttal evidence if it has reason to believe that the work of the OPC was inadequate.

Second, it may be asked whether such a proposal would serve the main purpose of section 8 of the *Charter*: *preventing* unreasonable searches and seizures.[26] Many digital privacy issues come before courts *ex parte* as warrant applications. As defence counsel is not present, courts would suffer from the same informational deficit as currently exists. The proposal here at least better ensures that *ex post* review will be conducted with an adequate factual basis. Moreover, if a judge was aware of an independent report that raised factual concerns with a warrant application, I see no reason why the judge could not inform its decision to dismiss or modify a Crown's application on that basis.[27] In this way, my proposal at least has the potential to prevent some unreasonable searches, even if its main role will be to ensure laws are fairly applied *ex post*.

Finally, this proposal does not address one additional problem that arose from my review of the digital privacy jurisprudence: the inability of some judges to understand digital technologies.[28] If some judges truly do not understand digital technologies, providing issue-specific reviews may not aid in developing more principled decisions. This problem is likely unavoidable. However, individual judges with a lack of understanding likely are aware of this weakness. As such, they could rely more heavily on others within the judicial system. Law clerks, for instance, are generally available to trial judges. Increased reliance on their input could help courts tasked with making decisions relating to digital technologies.[29] Even if there is no way to fully and immediately address this problem, any framework for governing digital privacy must still compare this risk to those identified with legislative rulemaking.

---

[26] See *Hunter et al. v Southam Inc*., [1984] 2 SCR 145 at 160, 33 Alta LR (2d) 193.
[27] See *Re C.(S.)*, 2006 ONCJ 343,71 WCB (2d) 241; *Re Subscriber Information*, 2015 ABPC 178, 123 WCB (2d) 553.
[28] See Chapter Two.
[29] There is no guarantee, however, that law clerks are any more technically savvy than judges.

(c) Expanding the Role of Interveners

The adversarial process in Canada was also found in the preceding Chapter to be hindered by restrictions on intervener submissions. Given that interveners are capable of bringing relevant expertise, they might serve to correct factual misunderstandings. As such, it would be prudent to provide interveners with more opportunity to make legal arguments and correct factual misunderstandings about digital technologies. This may be done in two ways.[30] First, the overall limitations on interveners could be relaxed to allow for significantly more oral and written submissions by interveners. This may, however, be undesirable as it would allow increased intervener submissions in all contexts. Alternatively, interveners in digital privacy cases could ask courts to exercise their discretion to relax restrictions on oral and written submissions.[31] If this were routinely allowed by appellate courts, interveners could focus their submissions on updating factual records as well as providing legal arguments about the application of section 8 of the *Charter* to digital technologies.

II. The Role of Parliament

The review in Chapters Two and Three suggests that Parliament's advantage over courts in responding to complex and rapidly changing search technologies is more theoretical than real. Although Parliament should be able to respond quickly and coherently, it often fails to meet these objectives. It is notable, however, that there appear to have been few instances where public choice

[30] As the Supreme Court of Canada observed in *Reference re Workers' Compensation Act, 1983 (Nfld.) (Application to intervene)*, [1989] 2 SCR 335, 76 Nfld & PEIR 185, the Court will grant intervener status where the applicant has a recognized interest in the matter and will provide "useful and different submissions." Speaking to the second criteria, the Court noted that "[t]his criteria is easily satisfied by an applicant who has a history of involvement in the issue giving the applicant an expertise which can *shed fresh light or provide new information on the matter*" (italics mine). The italicized clause suggests the Court will be open to new factual submissions. For a detailed review of the various laws governing intervener status, see Eugene Meehan, Marie-France Major, and Thomas Slade, "Getting In, Getting Heard, Getting Practical: Intervening in Appellate Courts Across Canada" (2017) 46 The Advocates' Quarterly 261.
[31] This is possible under the *Rules of the Supreme Court of Canada*, SOR/2002-156, s 42(5).

concerns have given rise to serious problems in the context of criminal law legislation governing digital technologies. Any proposed role for Parliament thus needs to begin by recognizing that in the criminal law/digital privacy context both courts and Parliament are slow in responding, make rules in incomplete information environments, but tend to make rules in an even-handed manner.

Two other points must also affect any institutional strategy. First, Parliament has exclusive authority to pass new offences or update current offences. As such, it is Parliament's sole prerogative to carefully tailor the definition of offences to keep up with digital technologies—a task which has proven to be quite challenging.[32] Second, courts often serve a gap-filling role when developing and implementing rules governing complex and rapidly changing search technologies.[33] The challenge is therefore twofold. First, how should Parliament tailor its non-offence related legislation knowing that it tends to react slowly and at times incoherently? Second, when should Parliament defer to courts to play its gap-filling role?

In answering these questions, it is prudent to begin by considering the literature on institutional choice. Neil Komesar and Adrian Vermeule have each written extensively on this topic.[34] They recognize that "comparing institutions requires identifying parallels across institutions in some acceptable, understandable, and usable fashion".[35] To accomplish this end, Komesar developed the "participation-centred approach".[36] The model is a simple economic one wherein "[t]he character of institutional participation is determined by the interaction between the benefits of that participation and [its costs]".[37]

---

[32] See the review provided in Chapter Three.
[33] *Ibid*.
[34] See Neil Komesar, *Imperfect Alternatives: Choosing Institutions in Law, Economics, and Public Policy* (Chicago: University of Chicago Press, 1994); Adrian Vermeule, *Judging Under Uncertainty: An Institutional Theory of Legal Interpretation* (Harvard: Harvard University Press, 2006).
[35] *Ibid* at 7; Vermeule, *Judging Under Uncertainty*, *supra* note 34 at 74-75.
[36] *Ibid*.
[37] *Ibid* at 8.

One of the major impediments for using courts was discussed above, namely, judicial ability to receive adequate information.[38] Another is litigation costs, how they are diffused, and whether they create incentives to litigate.[39] Komesar uses pollution as his primary example to illustrate when these considerations might influence institutional approaches to rule making. If everyone faces small losses for pollution, no individual lawsuits will arise, and unless the damage is large overall, there likely will not be a class action.[40] Moreover, preventing pollution is extremely complex. Given the ability of legislatures to thoroughly research an issue, Komesar asserts that legislatures are better suited to weigh the competing concerns.[41] As long as there are not significant majoritarian or lobbying concerns, he reasons that it is best to leave it to the legislature.[42]

As Vermeule observes, however, institutional choice must also be determined by a country's constitutional and institutional arrangements and cultures.[43] Not only was Komesar speaking in the American setting, the examples he used are not applicable in the narrower topic considered here. First, in criminal cases there is almost always an incentive to litigate vague or yet-to-be-determined police powers even if the violation seems small: exclusion of evidence.[44] Second, although public choice theory concerns have proven to be insignificant, Parliament has been at least as slow and confusing in its legislation as courts developing the common law. Although it is often assumed that legislatures will utilize their institutional advantages, the Canadian digital privacy/criminal procedure context provides an excellent example of Parliament being unable to take advantage of its institutional strengths.

---

[38] *Ibid* at 21.
[39] *Ibid* at 25.
[40] *Ibid*.
[41] *Ibid* at 26.
[42] *Ibid* at 26-27.
[43] See Vermeule, *Judging Under Uncertainty*, *supra* note 34 at 74, 284.
[44] As is possible under section 24(2) of the *Charter*.

It is therefore appropriate to be skeptical about the utility of relying on institutional competence arguments as the sole means for determining the appropriate role of each institution when governing digital privacy. As one critic of institutional choice theory concludes, relying on broad generalizations of institutional competence paints "a stilted portrait of institutions" which "focuses too heavily on the current characteristics of institutions rather than on their potential for reform and change."[45] In other words, the "inherent" strengths and weaknesses of courts and legislatures are subject to ebb and flow. This in turn affects each institution's ability to respond effectively at different times. A better approach, then, would focus on how these institutions can work together to respond to the various challenges inherent in governing digital privacy.[46]

The reforms offered above concerning the adversarial process shed light on how Parliament should tailor its digital privacy legislation. As section 8 of the *Charter* requires that searches be authorized by law, Parliament must typically pass a law granting search powers to law enforcement.[47] Although Parliament may provide courts with broad legislation like the general warrant provision (487.01) or computer search provisions (487(2.1)(2.2)), *ex post* judicial development of such rules is not an optimal procedure as it fails to communicate the rule before a technology is in widespread use. Legislative rules are thus preferable to the extent that they can provide clear and lasting guidance to law enforcement officers before searches of a technology become common.

In deciding how a law affecting digital privacy should be drafted, Parliament should therefore consider the relative costs of specific and general rules. As discussed earlier, when

[45] See Daniel Solove, "The Darkest Domain: Deference, Judicial Review, and the Bill of Rights" (1999) 84 Iowa Law Review 941 at 1011.
[46] *Ibid*.
[47] See *R v Collins*, [1987] 1 SCR 265 at 278, 38 DLR (4th) 508. Common law searches (such as investigative detentions and searches incident to arrest) are exceptions.

Parliament passes detailed legislation with respect to complex and rapidly advancing technologies, those laws tend to become outdated and/or have gaps which either needlessly undermine privacy or unduly hamper police investigations. Where the technology is stable—as with laws governing impaired driving investigations—legislative rulemaking can better respond to both law enforcement and privacy interests. This follows because stable technologies can be studied in depth and rules crafted without concern that the law will soon become outdated. Delays inherent in the adversarial process will result in judicial rules relating to stable technologies being unknown for unnecessarily lengthy periods of time.[48]

Where Parliament is unsure about the development of a technology, however, legislative rules are vulnerable to becoming quickly outdated. To address this concern, Parliament should approach drafting its legislation in one of two ways. First, it could draft digital privacy laws broadly and allow courts to update the law on a case-by-case basis. If my above recommendations allow courts to receive adequate information about digital technologies, courts will be well-equipped to develop principled digital privacy rules. Although this approach would likely result in many rules lagging behind technological development,[49] this is already a prominent feature of legislative and judicial digital privacy rules in the digital privacy setting.

The general warrant illustrates how a law might be drafted to allow for judicial development. Section 487.01 of the *Criminal Code* allows courts to issue warrants allowing police to "use any device or investigative technique or procedure or do any thing described in the warrant that would, if not authorized, constitute an unreasonable search or seizure." It is nevertheless notable that the provision, although suitably broad, does impose (among other restrictions) a rigid

[48] Although such issues could be sent to the Court via reference, it is implicit in my reference suggestion that this process be used only where regular legislative and judicial processes are likely to fail.
[49] In particular, any rules which were developed outside of the reference process.

"reasonable grounds to believe an offence occurred" requirement before a warrant may issue.[50] The provision would better meet the needs of the digital age if it were made more flexible. For instance, by making this strict requirement presumptive but placing the burden of proof on the state to prove why the reasonable grounds requirement should be relaxed, courts would be able to better calibrate the privacy and security interests in allowing novel search tactics.

Second, if Parliament is confident in its understanding of a complex and rapidly advancing technology and its ability to pass a rule expediently, it could consider passing rules with built-in sunset clauses.[51] By ensuring that a rule is no longer applicable after a designated period, Parliament can control, to some extent at least, whether its legislation will be overtaken by technological advancement. Moreover, sunset clauses can be designed to ensure that the law comes before a special committee tasked with reporting to Parliament before the law expires.[52] Parliament can then take the opportunity to consider any potential gaps in its legislation and respond accordingly.

This more dynamic approach to governing digital privacy requires that courts and legislatures be flexible in determining the process for making a rule. There are multiple options for crafting principled rules and some processes may prove more or less feasible at different times due to restrictions in judicial and political processes. The ideal procedure would witness Parliament craft and expediently revisit digital privacy rules in a way that allows for judicial review of its legislation. Recognizing that this is unlikely to frequently occur, Parliament must be attuned to its institutional weaknesses, and focus on strengthening the judicial process so as to allow the

[50] See section 487.01(a)
[51] See Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution" (2004) 102 Michigan Law Review 801 at 871.
[52] For an example, see Department of Justice, "About the Anti-Terrorism Act" (26 July 2017), online: <http://www.justice.gc.ca/eng/cj-jp/ns-sn/act-loi.html>.

courts to address the inevitable gaps that its legislation will leave. The above recommendations, I suggest, would go a long way in achieving these goals.

Several objections to this proposal may be anticipated. First, it may be argued that *stare decisis* will prevent courts from responding flexibly to technological change.[53] It should be remembered, however, that developing digital privacy rules in the criminal procedure context implicates section 8 of the *Charter*. As explained in the preceding Chapter, the rules surrounding *stare decisis* in the Canadian constitutional context are much more relaxed than in the United States.[54] In other words, it is not difficult to imagine changes in technology "fundamentally shifting" the applicable privacy and security interests at the heart of determining whether a search or seizure breaches section 8 of the *Charter*.[55]

Second, any suggestion that Parliament should play a lesser role in developing police search powers is constitutionally questionable. As James Stribopoulos posits, the principle of legality requires that police powers derive from Parliament, not from the courts.[56] The legality principle, however, has yet to inhibit Parliament from passing broad legislation to facilitate judicial development of digital privacy rules. First, it is notable that the Court has, for better or for worse, mostly abandoned the legality principle.[57] Second, although searches must at minimum be authorized by law,[58] the courts have not imposed a high threshold for meeting this requirement. For instance, the broadest provision discussed in Chapter Three—the general warrant found in

[53] See Kerr, "Fourth Amendment", *supra* note 51 at 871.
[54] See *Bedford*, *supra* note 6 at para 44.
[55] See Chapter Five.
[56] See James Stribopoulos, "In Search of Dialogue: The Supreme Court, Police Powers, and the *Charter*" (2005) 31 Queen's Law Journal 1.
[57] *Ibid*. See also Tim Quigley, "*R. v. Fearon*: A Problematic Decision" (2015) 15 CR (7th) 281.
[58] See *Collins*, *supra* note 47 at 278.

section 487.01 of the *Criminal Code*—has survived constitutional scrutiny on this ground.[59] As such, there does not appear to be a constitutional impediment to my proposal.[60]

Finally, it may be argued that it is undemocratic to vest significant digital privacy rule-making duties with courts. This argument may be countered in two ways. First, it is notable that those advocating for legislative primacy in the field of digital privacy/criminal procedure do not present any cogent arguments to address the significant limitations of legislative rule-making.[61] Political science scholars observe that politicians tend to address issues only when they arise on the public agenda.[62] Whether a legal gap will be addressed in turn depends on what other issues of the day are demanding political attention.[63] Moreover, the fact that Canadian federal governments are often in minority positions makes passing legislation with any controversy increasingly difficult.[64] Add to this the necessary study to pass legislation, as well as the need for laws to pass through both the House of Commons and the Senate, and the temporal and practical barriers may often become insurmountable for not only minority, but also majority governments.[65] Parliament should admit these limitations and explore institutional options to address them. This does not strike me as undemocratic: it exemplifies responsible governance.

My proposal also need not always stifle Parliament from passing digital privacy laws or prevent Parliament from responding to digital privacy rulings. Instead, I suggest that Parliament

---

[59] See *R v Lucas*, 2014 ONCA 561 at paras 104-26, 121 OR (3d) 303 leave to appeal ref'd 2015 CarswellOnt 639; *R v Kuitenen*, 2001 BCSC 677, 45 CR (5th) 131. For academic criticism, see Steven Coughlan, *Criminal Procedure*, 2nd ed (Toronto: Irwin Law, 2012) at 133-34.

[60] I should note that I do not wish to be taken as endorsing the Court's abandonment of the legality principle. As I will explain in the next Chapter, this principle may be re-invoked by the Court under different institutional rule-making arrangements.

[61] See in particular Kerr, "Fourth Amendment", *supra* note 51.

[62] For a literature review on agenda setting, see Christopher Parsons, "Stuck on the Agenda: Drawing Lessons from the Stagnation of 'Lawful Access' Legislation in Canada" in Michael Geist, ed, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (Ottawa: University of Ottawa Press, 2015) 257 at 258-61.

[63] *Ibid*. As the author notes, the public agenda tends to attract no more than 5-7 issues at a time.

[64] The lawful access experience is exemplary. See Chapter Three for an extensive review.

[65] See Daniel Solove, "Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference" (2005) 74 Fordham Law Review 747 at 771 for a similar argument in the American context.

should consider its institutional limitations before passing digital privacy legislation. This still allows for important dialogue on the content of rights.[66] As Professor Peter Hogg and Allison Bushell observe, the democratic legitimacy of judicial review is bolstered because the structure of the *Charter* often results in judicial review of legislation leaving room for a legislative response.[67] That response is typically able to achieve the legislature's objective while at the same time respecting constitutional rights.[68] In this way, then, constitutional dialogue provides an important mechanism for determining "how society should struggle together for the best answers to controversies about justice."[69]

Yet, as should be evident from Chapters Two and Three, dialogue in the digital privacy context has been lackluster.[70] This should not be surprising. Courts and legislatures are having difficulty determining the basic facts upon which to create rules governing digital technologies. They are also having difficulty keeping pace with the rapid development of digital technologies. Dialogue is meaningless if there is no basic understanding of what facts underlie the dialogue or if the dialogue is rendered moot because a rule becomes outdated due to its failure to keep pace with use of a particular technology. By reforming how courts receive information about digital technologies, courts will become equipped to actually participate in this dialogue.

---

[66] See Peter Hogg and Allison Bushell, "The Charter Dialogue between Courts and Legislatures (Or Perhaps the Charter of Rights Isn't Such a Bad Thing after All)" (1997) 35 Osgoode Hall Law Journal 75. Although the article has come under criticism, the findings were again confirmed in a 2007 update of the original article. See Peter Hogg, Allison Bushell Thornton, and Wade Wright, "Charter Dialogue Revisited – Or 'Much Ado About Metaphors'" (2007) 45 Osgoode Hall Law Journal 1.

[67] See Hogg and Bushell, "Dialogue", *supra* note 66 at 79-80. See also Kent Roach, *The Supreme Court on Trial: Judicial Activism or Democratic Dialogue?* (Toronto: Irwin Law, 2001) at 11.

[68] *Ibid*. As Professor Kent Roach observes, the ability of *Charter* dialogue to place issues on the legislative agenda improves democracy by ensuring that controversial issues are subject to robust public debate. See Kent Roach, "Dialogic Judicial Review and its Critics" (2004) 23 Supreme Court Law Review 49 at 75.

[69] See Roach, "Dialogic", *supra* note 68 at 104.

[70] For example, Parliament has not responded to the Court's decisions concerning ISP subscriber information, the definition of intercept, computer searches, and searches of cell phones incident to arrest.

Parliament's "tone" in this dialogue should nevertheless be altered to reflect the changing circumstances within which this conversation takes place. A revitalized dialogue in the digital privacy context requires that Parliament pay attention to judicial and legislative weaknesses in rule-making. In practice, this will often require Parliament to facilitate better judicial fact finding or speak more cautiously, using tools such as sunset clauses to ensure its legislation does not unduly hinder law enforcement or needlessly undermine privacy interests. This modified approach to passing criminal procedure rules implicating digital technologies, I suggest, provides a democratically responsible way of ensuring that Canadian institutions tasked with governing digital privacy are capable of balancing the important law enforcement and digital privacy interests at the heart of section 8 of the *Charter*.

Conclusion

As Parliamentary and judicial capacity to respond to the challenges of governing digital privacy will ebb and flow, it is not sensible to rely on institutional process arguments to exclude one institution in favour of the other. Instead, the focus should be on how to help courts and legislatures work together to ensure the best digital privacy rules are implemented. This requires thinking creatively about how to address institutional weaknesses. In addition to ensuring courts are institutionally equipped to receive adequate information to respond to digital privacy concerns, Parliament should be vigilant about weighing the costs and benefits of responding to novel and complex technologies with legislation. Although the approach offered here may periodically abscond significant rule-making authority to courts, concerns about democratic legitimacy are mitigated if Parliament approaches digital privacy rulemaking with a realistic assessment of its capacity to meet the challenges of governing digital privacy.

Chapter Seven

Criminal Procedure as Administrative Governance: The Final Frontier?

Introduction

Throughout this work I have operated within a legislative and judicial rule-making paradigm. This dichotomy does not, however, accurately portray the potential types of governing structures which may be used to craft criminal procedure rules. Nearly fifty years ago, a small number of scholars suggested governing the Fourth Amendment through law enforcement agencies.[1] A growing body of American literature has recently rejuvenated this idea.[2] The impetus for this proposal derives from the observation that law enforcement agencies "possess expertise about the various ways the criminal law and associated regulatory statutes can be enforced that legislatures (and courts) usually do not have."[3] Such institutions are therefore "much better

[1] See Kenneth Culp Davis, "An Approach to Legal Control of the Police" (1974) 52 Texas Law Review 703 at 725; Anthony Amsterdam, "Perspectives on the Fourth Amendment" (1974) 58 Minnesota Law Review 349 at 423; Carl McGowan, "Rule-Making and the Police" (1972) 70 Michigan Law Review 659.

[2] See Erin Murphy, "The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions" (2013) 111 Michigan Law Review 485 at 539-44; Barry Friedman and Maria Ponomarenko, "Democratic Policing" (2015) 90 New York University Law Review 1827; Christopher Slobogin, "Policing as Administration" (2016) 165 University of Pennsylvania Law Review 91; Andrew Crespo, "Systemic Facts: Toward Institutional Awareness in Criminal Courts" (2016) 129 Harvard Law Review 2049; Daphna Renan, "The Fourth Amendment as Administrative Governance" (2016) 68 Stanford Law Review 1039.

[3] See Slobogin, "Policing", *supra* note 2 at 121. Scholars have repeatedly shown that legislative reluctance to devise detailed legal frameworks for complex areas of law in large part accounts for the rise of the administrative state. See

positioned to make decisions about resource allocation and the relative efficacy of enforcement methods than are other institutions".[4]

Administrative agencies are thought to be acceptable substitutes for legislative and judicial rule-making so long as two main prerequisites are met: rule-making power derives from clear legislation and procedures are in place to ensure public accountability.[5] This in turn is sufficient to attract another main feature of administrative law: deference to agency rules.[6] This institutional trade-off between legislatures/courts and administrative agencies undeniably has many benefits. Agencies not only bring more expertise to their relevant fields, they also are capable of passing much more efficient rules, all the while building democratic legitimacy by soliciting and responding to public participation in rule-making.[7] Scholars nevertheless caution against adopting a new rule-making paradigm in the criminal procedure context, worrying that such an approach overlooks that which may be "lost in the bathwater of institutional redesign."[8]

The aim of this Chapter is to consider whether an administrative approach to crafting criminal procedure rules implicating digital privacy interests ought to be adopted in Canada. Although utilizing administrative decision-makers has several benefits, providing unelected, non-judicial decision-makers with significant deference when applying constitutional doctrine requires a more critical assessment than currently undertaken by its supporters. Majoritarian and Public Choice Theory concerns, I maintain, serve as a strong, though not definitive, impediments to an administrative approach to crafting digital privacy rules.

David Epstein and Sharyn O'Halloran, *Delegating Powers: A Transaction Cost Politics Approach to Policy Making Under Separate Powers* (Cambridge: Cambridge University Press, 1999) at 203-06.

[4] *Ibid*.

[5] *Ibid* at 146. See also Friedman and Ponomarenko, "Democratic Policing", *supra* note 2 at 1832, 1843.

[6] See Friedman and Ponomarenko, "Democratic Policing", *supra* note 2 at 1891-92. Under their model, democratically authorized rules would still be subject to constitutional review in a reduced fashion. See 1901.

[7] These points will be discussed in more detail below.

[8] See Crespo, "Systemic Facts", *supra* note 2 at 2060. See also David Sklansky, "Two More Ways Not to Think About Privacy and the Fourth Amendment" (2015) 82 University of Chicago Law Review 223 at 224-27.

More importantly, the problems with an administrative approach to criminal procedure must be viewed in light of the potential for courts and legislatures to adapt to changing circumstances. Given the various reforms proposed in the preceding Chapter, I contend that there is a role for all three institutions to govern criminal procedure in the digital age. Parliament, I suggest, should focus on developing rules with stable factual backgrounds. Administrative agencies should fill legislative gaps by making rules relating to complex and rapidly advancing technologies. Courts, however, should not show deference to either of these actors. If the reforms proffered result in a better judicial understanding of complex technologies, then courts will be able to provide a valuable check on majoritarianism.

Before pressing forward, I should delimit the scope of my discussion. The debate between administrative and judicial/legislative approaches to governing digital privacy at times expands to incorporate the entire field of criminal procedure.[9] I am primarily interested in assessing the feasibility of administrative approaches to governing privacy interests in new and complex technologies. As this field is among the most complicated in criminal procedure, it presents the most compelling case for administrative rule-making.[10] If cross-institutional comparison does not yield significant benefits in this context, it is unlikely that transition to a fully administrative criminal procedure regime could be justified.

I. Criminal Procedure as Administrative Governance

The literature contemplating administrative approaches to criminal procedure raises three preliminary issues. First, scholars question whether police agencies are appropriate venues for criminal procedure rule-making. Second, police agencies object to their practices being subjected

[9] Most notably see Friedman and Ponomarenko, "Democratic Policing", *supra* note 2; Crespo, "Systemic Facts", *supra* note 2.
[10] Authors such as Murphy, "Politics of Privacy", *supra* note 2 and Renan, "Fourth Amendment", *supra* note 2 focus their comments on digital technologies because they are the most difficult to keep up with and comprehend.

to detailed administrative review.[11] Finally, there is a divide between those that support agency regulation for all criminal procedure rules and those that limit agency rule-making to more complex "panvasive" searches.[12] As I contend below, a broad array of criminal procedure rules implicating digital technologies could be competently and fairly developed by administrative agencies.

(a) Should Police Agencies Develop Criminal Procedure Rules?

The common proposal for administrative rulemaking in the criminal procedure context involves delegating rule-making power to law enforcement agencies.[13] This proposal, however, should sound several alarms. It is trite to acknowledge that judges play the role of neutral arbitrator against a state that often strongly favours law enforcement interests. Substituting police for judges and legislatures when crafting rules can be expected to tilt existing rules significantly in favour of law enforcement. Moreover, requiring courts to be deferential to police-made rules increases the likelihood that civil liberties will be lessened in favour of intrusive law enforcement procedures.[14] The question, then, is whether any such delegation can be adequately cabined to ensure that both privacy and law enforcement interests are given due weight.

Scholars have identified several means to ensure public accountability in rulemaking. Those in support of an administrative regime for criminal procedure rules require administrative rule makers to first obtain authorization from legislative mandates that are sufficiently clear.[15]

---

[11] See Slobogin, "Policing" *supra* note 2 at 125.
[12] Contrast Friedman and Ponomarenko, "Democratic Policing", *supra* note 2 and Slobogin, "Policing", *supra* note 2 at 92; Renan, "Fourth Amendment", *supra* note 2 at 1042. "Panvasive" searches are also described as "dragnets" or "programmatic" searches. I follow Slobogin in using the term "panvasive" as it aptly captures the main feature of these searches: the fact that they catch mostly people innocent of any wrongdoing and are not based on suspicion that a crime was committed. See Christopher Slobogin, "Rehnquist and Panvasive Searches" (2013) 82 Mississippi Law Journal 307 at 308.
[13] *Supra* note 2
[14] Even proponents of administrative approaches to criminal procedure rule-making admit this deficiency. See Murphy, "Politics of Privacy", *supra* note 2 at 543.
[15] See Slobogin, "Policing", *supra* note 2 at 146-49.

Typically, this requires the legislature to identify the persons and activities subject to regulation, the harm to be avoided, and the means available to accomplish the agency's ends.[16] Courts can ensure agency accountability by reading legislative authorizations narrowly, especially where constitutional rights are at issue.[17] Any rule which exceeds the statutorily granted authority would be *ultra vires* and therefore null and void.[18]

Second, rules can be made with procedural safeguards in place that guarantee public input and accountability.[19] In particular, agency rules can gain political legitimacy by being made pursuant to a notice and comment rule-making procedure.[20] For instance, under the American *Administrative Procedure Act*,[21] agencies engaging in informal rule-making must make generally available "either the terms or substance of the proposed rule or a description of the subjects and issues involved."[22] The public may then comment on any aspect of the proposed rule. If the police agency fails to address critical issues inherent in the rule or identified in the comments the rule may be nullified in court.[23]

Although the *APA* does not require a response to every comment, it does require agencies to provide "a concise general statement of [the rule's] basis and purpose".[24] Such a statement must not demonstrate "arbitrary" or "capricious" intent on behalf of the drafters,[25] which the Court has interpreted as requiring a "cogent" explanation of the basis for the rule.[26] As one commentator

---

[16] *Ibid*. For instance, current legislation requiring police to "enforce the criminal law" or something similar would be woefully inadequate.
[17] See Friedman and Poromarenko, "Democratic Policing", *supra* note 2 at 1892-97.
[18] *Ibid*.
[19] *Ibid*. See also Slobogin, "Policing", *supra* note 2 at 135-51.
[20] See Slobogin, "Policing", *supra* note 2 at 137-40.
[21] 5 USC (2012) § 553(b)(3). As leading administrative law writers acknowledge, Canada has significantly less experience with notice and comment rule-making procedures. As such, the American experience is more illustrative. See Gus Van Harten et al., *Administrative Law: Cases, Text, and Materials*, 7th ed (Toronto: Emond, 2015) at 577-78.
[22] *Ibid*.
[23] See Slobogin, "Policing", *supra* note 2 at 137-38 citing *AFL-CIO v Donovan*, 757 F2d 330 at 333 (DC Cir 1985).
[24] See *Tri-State Generation & Transmission Ass'n v Envtl. Quality Council*, 590 P2d 1324 at 1330 (Wyo 1979).
[25] See *APA*, *supra* note 21 at 706(2)(a).
[26] See *Motor Vehicle Mfrs. Ass'n v State Farm Mut. Auto. Ins. Co*., (1983) 463 US 29 at 48.

explains, this requirement effectively means that the agency may not '"entirely [fail] to consider an important aspect of the problem,' may not '[offer] an explanation for its decision that runs counter to the evidence before the agency,' nor offer an explanation that is 'so implausible that it could not be ascribed to a difference in view or the product of agency expertise.'"[27] Notably, in the policing context, such a requirement would prohibit "an agency's unjustified discriminatory treatment of similarly situated parties".[28]

With this cursory overview of *APA* procedure in place, it is possible to predict at a general level how these safeguards would inhibit police agencies from making rules which weigh too heavily in favour of law enforcement interests. Requiring explicit delegation of rule-making power ensures that legislatures are held accountable for the duties they are abdicating to law enforcement agencies. Notice and comment procedures ensure law enforcement "tunnel vision" would not overlook important rights issues.[29] Requiring police to explain themselves with respect to their rule choice also makes it more likely rights issues will not be overlooked. So long as citizens actively participate and police are responsive to democratic will, law enforcement agencies should be able to promulgate accountable and efficacious criminal procedure rules.

(b) Should Police Agency Rules be Exempt from Administrative Restrictions?

Police agencies might agree to showing deference to their relative expertise in crafting criminal procedure rules, but nevertheless object to their rules being subjected to the administrative law requirements outlined above. First, police might contend that judicial review of any sort by non-expert judges could result in costly investigative mistakes.[30] Second, police may argue that

[27] Kevin Stack, "Interpreting Regulations" (2012) 111 Michigan Law Review 355 at 378-79.
[28] See Slobogin, "Policing", *supra* note 2 at 144 citing Joseph Small Jr and Robert Burgoyne, "Criminal Prosecutions Initiated by Administrative Agencies: the FDA, the Accardi Doctrine and the Requirement of Consistent Agency Treatment" (1987) 78 Journal of Criminal Law & Criminology 87 at 103-04.
[29] Specialization is often observed to lead to agency "tunnel vision". See Harten, *Administrative Law*, *supra* note 21 at 27.
[30] See Slobogin, "Policing", *supra* note 2 at 125.

they need more speed and flexibility than administrative review allows.[31] Given the rapid pace at which digital technologies change, police may be unduly slowed in crafting rules due to requirements such as notice and comment.[32] Finally, increased transparency with respect to police rules could "tip-off" criminals with respect to effective police practices.[33] For instance, disclosing how police deploy drones, wiretaps, and other digital technologies would allow criminals to devise plans to avoid such surveillance.

As Christopher Slobogin cogently argues, these difficulties are all inherent to a variety of other administrative agencies.[34] Judicial review of agencies governing pollution, food, and health regulations may also impinge important interests.[35] Similarly, a variety of agencies require speed and flexibility when making rules, "ranging from environmental protection to health-related matters to financial regulation… [Yet] the relevant agencies have managed to function despite rulemaking requirements".[36] Although law enforcement concerns may become particularly pressing, rule-making frameworks can also provide exceptions for exigent circumstances.[37] Finally, the need for secrecy can be accommodated.[38] The sort of details about use of digital technologies that might encourage circumvention—such as where and how they are used—could properly be withheld from the public while details about frequency of use and how such data is analyzed could safely be disclosed.[39]

---

[31] *Ibid* at 125. As an example, see Ganesh Sitaraman and Ingrid Wuerth, "The Normalization of Foreign Relations Law" (2015) 128 Harvard Law Review 1897 at 1935-46 (considering whether such concerns justify exempting foreign affairs from administrative law principles).
[32] *Ibid*.
[33] *Ibid*.
[34] *Ibid* at 125-26.
[35] *Ibid*.
[36] *Ibid*.
[37] *Ibid* citing Eric Posner and Adrian Vermeule, "Crisis Governance in the Administrative State: 9/11 and the Financial Meltdown of 2008" (2009) 76 University of Chicago Law Review 1613 at 1636-39.
[38] See Friedman and Ponomarenko, "Democratic Policing", *supra* note 2 at 1884-85.
[39] *Ibid* at 1885.

(c) Panvasive and Suspicion-Based Searches: A Distinction without a Difference?

State searches may be divided into two types: "panvasive" and "suspicion-based". The latter searches are transactional in nature, involving a police officer searching an individual based on some degree of suspicion that the suspect committed a crime.[40] Panvasive searches are defined by three main features: they are conducted pursuant to an executive or legislative policy; they seek to deter undetected crime, usually within a known group; and they are not based on suspicion against any named individual, thus affecting many innocent people.[41] Examples of panvasive searches include "[road stops], drug testing programs, creation of DNA databases, collection of communications metadata, and establishment of surveillance regimes involving cameras, tracking systems, and the like."[42]

Panvasive searches do not fit neatly into the traditional warrant based on reasonable grounds framework. They tend to involve multiple and layered searches each of which cannot reasonably be expected to be pre-approved by a court.[43] The warrant framework also fits awkwardly with aggregate searches, as it will be difficult for courts to foresee the effects of such searches.[44] Nor does the warrant framework allow for revisiting the efficacy of a search program at regular intervals.[45] This is especially problematic given the varying effects that any changes in technology might have on typical panvasive searches.[46] For the reasons expressed in preceding chapters, courts and legislatures are simply unlikely to keep up with and respond coherently to these challenges.

---

[40] See Slobogin, "Panvasive Searches", *supra* note 12 at 308.
[41] See Slobogin, "Policing", *supra* note 2 at 93.
[42] *Ibid*.
[43] *Ibid* at 115; Renan, "Fourth Amendment", *supra* note 2 at 1068.
[44] See Slobogin, "Policing", *supra* note 2 at 115
[45] *Ibid*.
[46] *Ibid*.

As a result, some authors explicitly limit administrative rulemaking to panvasive searches,[47] while others abstain from deciding whether such a limitation is warranted.[48] In my view, the distinction between "panvasive" and "suspicion-based" searches is unhelpful in determining institutional design questions. As the preceding chapters have explained, courts have similar difficulties crafting principled rules with respect to transactional searches of common items such as cell phones[49] and computers.[50] If administrative agencies can help create principled rules for complex panvasive searches, there is no question it could also be used to regulate complex transactional searches. This need not mean that Parliament delegate all criminal procedure rule-making to administrative agencies. Basic rules surrounding less complex criminal procedure rules—such as unreasonable delay or rights to counsel—may still be governed by legislative and judicial rules. Parliament and administrative authorities would, however, need to be vigilant in ensuring that they do not exercise their authority in a way that leaves gaps in police powers.

II. The Perils of Administrative Rule-Making

Although administrative law is a promising venue in the abstract for crafting criminal procedure rules, it is necessary to consider in more detail how administrative law may potentially hinder constitutional interests. It is notable at the outset that the American literature primarily justifies agency rule-making in the criminal procedure context by appealing to the fact that many of the panvasive searches at issue are simply not covered by the Fourth Amendment or are only given a "soft look" under what is known as the "special needs" doctrine.[51] Scholars also observe that the Fourth Amendment frequently fails to fill policy voids left by the third-party doctrine.[52]

[47] See generally Renan, "Fourth Amendment", *supra* note 2.
[48] See Slobogin, "Policing", *supra* note 2 at 150-51.
[49] See *R v Fearon*, 2014 SCC 77, [2014] 3 SCR 621.
[50] See *R v Vu*, 2013 SCC 60, [2013] 3 SCR 657.
[51] See Slobogin, "Policing", *supra* note 2 at 141.
[52] See Friedman and Poromarenko, "Democratic Policing", *supra* note 2 at 1851.

This is much less of an issue in Canada. As seen in previous chapters, section 8 of the *Charter* is considerably more flexible and far-reaching in its application than the Fourth Amendment.

Any Canadian administrative framework nevertheless should anticipate several other objections. Although relatively underutilized in Canada, notice and comment procedures akin to those mandated by the *APA* are feasible to develop.[53] Yet, it is questionable whether criminal suspects—typically marginalized peoples living in poor, urban, and minority communities—will trust such state outreach let alone participate in it.[54] To be sure, others have observed significant public participation in police outreach events.[55] It is not clear that such largely one-off participation would be sustainable under an administrative regime to criminal procedure rules wherein frequent and detailed input would be required from the public. The prospect of marginalized, poor communities putting in the study and effort to comment on criminal procedure rules—especially those considered "too complex" for courts and legislatures to adjudicate—when they are struggling to put food on the table is highly unlikely.

Studies of the extensive use of notice and comment rule-making procedure in the United States bolster this conclusion.[56] Even using a well-organized digital system for soliciting and providing comments,[57] most agencies attract only a few comments per rule.[58] These comments

---

[53] See Harten, *Administrative Law*, *supra* note 21 at 577-78. For an excellent Canadian example of notice and comment rule-making, see *Securities Act*, RSO 1990, c S.5, s 143.2, 143.3.

[54] See Crespo, "Systemic Facts", *supra* note 2 at 2062-63 noting also that the point concerning the disparate treatment of minorities is generally conceded by proponents of agency criminal procedure law making.

[55] See Murphy, "Politics of Privacy", *supra* note 2 at 543-44; Friedman and Poromarenko, "Democratic Policing", *supra* note 2 at 1879-81.

[56] In the United States, even with the advent of "e-rulemaking", most agencies attract only a few comments per rule. These comments typically are from interested industries. See Cary Coglianese, "Citizen Participation in Rule-Making: Past, Present, and Future" (2006) 55 Duke Law Journal 943; Steven Balla and Benjamin Daniels, "Information Technology and Public Commenting on Agency Regulations" (2007) 1 Regulation and Governance 46. It is notable that some rules have attracted significantly more participation, usually through grassroots organizational efforts. See Mariano-Florentino Cuéllar, "Rethinking Regulatory Democracy" (2005) 57 Administrative Law Review 411. This does, however, seem to be an anomaly.

[57] The federal website may be found here: <regulations.gov>.

[58] See Coglianese, "Citizen Participation", *supra* note 56 at 949, 956-58.

typically come from interested industries, not average citizens.[59] Where citizens do provide comments, they typically are short and more preference-based than reasoned policy arguments, or express disregard for the agency and its rule-making authority.[60] In contrast, industry comments are typically well-organized and sophisticated analyses of the policy at issue which seek to influence the rule in a manner that promotes the private interests of businesses.[61]

Even if significant numbers of citizens participated, the majority viewpoints would likely drown out those most affected by criminal law policy. As Donald Dripps maintains in an oft-cited article, "a far larger number of persons, of much greater political influence, rationally adopt the perspective of a potential crime victim rather than the perspective of a suspect or defendant."[62] Law enforcement and political actors engaged in the debate between how to strike the delicate balance between privacy and security interests would lean towards the latter in accordance with these demands.[63] On the other hand, criminal courts provide a neutral platform where criminal suspects are frequently heard.[64] Although counsel do not always advocate as well as one would hope, scholars contend that this still constitutes a *relative* institutional advantage.[65] Although it is possible that state intrusions into digital privacy may garner majority support for more balanced

[59] *Ibid* at 951, 958-59.
[60] *Ibid*. See also Cuéllar, "Regulatory Democracy", *supra* note 57 at 443.
[61] *Ibid* at 951.
[62] Donald Dripps, "Criminal Procedure, Footnote Four, and the Theory of Public Choice; or, Why Don't Legislatures Give a Damn About the Rights of the Accused?" (1993) 44 Syracuse Law Review 1079 at 1089.
[63] See Crespo, "Systemic Facts", *supra* note 2 at 2061 citing Andrew Manuel Crespo, "Regaining Perspective: Constitutional Criminal Adjudication in the U.S. Supreme Court" (2016) 100 Minnesota Law Review 1985 at 2036-37.
[64] *Ibid* at 2062 citing John Hart Ely, *Democracy and Distrust* (Cambridge: Harvard University Press, 1980). See also William Stuntz, "The Pathological Politics of Criminal Law" (2001) 100 Michigan Law Review 505 at 510.
[65] *Ibid* at 2063.

rules,[66] the limited experience in Canada reviewed in Chapter Three suggests this conclusion should be approached with caution.[67]

It is more likely that civil rights groups would provide the most effective representation for criminal defendants. This is unlikely to make the rule-making process substantially fairer. These groups require significant amounts of funding to serve their purposes. To the extent that such funding comes from voluntary donations the proposal is dependent on unpredictable public generosity. Although the state may choose to contribute to funding such groups, state funding to help criminal defendants is politically unpopular. Shoe-string budgets for legal aid organizations across the country illustrate how low a priority ensuring due process for indigent criminal suspects is for many governments.[68] These groups will largely be up against well-funded industries with the ultimate arbiter being the group with the most to benefit from rules under emphasizing privacy interests: law enforcement.

To address these concerns, it is possible to structure an appeal that allows agency rules to be subject to override by the executive branch. In theory, this would allow citizens to place pressure on elected officials to override unbalanced agency rules. Many scholars have, however, found such appeals unsatisfactory.[69] Cabinet decision-making is often shrouded with secrecy, and generally viewed as more responsive to partisan politics than demands of good regulatory decision-making.[70]

---

[66] See Orin Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution" (2004) 102 Michigan Law Review 801 at 887.

[67] Although the lawful access experience suggests telecommunication service providers, citizens, civil rights groups, and minority political parties do mobilize to protect digital privacy interests where the rules affected the populous generally, it is not at all evident that similar mobilization will happen when the group dominantly affected are from lower socio-economic backgrounds.

[68] The Chief Justice of Canada recently called on governments to provide adequate funding to legal aid, noting that the current deficit is near crises levels. See Kathleen Harris, "Supreme Court Chief Justice says Legal Aid 'Essential' to Fair Justice System" *CBC News* (20 June 2019) online: <https://www.cbc.ca/news/politics/supreme-court-chief-justice-wagner-1.5182657?fbclid=IwAR1Opazt3YIkzw2pwk3wJ-GrmZgpMSVYO2YYDzxpMbdi_cUYUfNd1MQmVo4>.

[69] See Harten, *Administrative Law*, *supra* note 21 at 16.

[70] *Ibid*.

The same majoritarianism problems inherent in criminal law policy making are therefore unlikely to be alleviated by relying on executive branch appeals.

It may be that law enforcement agencies will be less biased than expected. After all, administrative agencies share some measure of independence from the ministry with overarching responsibility for the relevant policy area. As a result, the minister cannot direct the agency to come to a particular decision.[71] Employees of an agency are not, however, similar to judges. Their appointments are usually for short terms, not life.[72] Agencies are therefore susceptible to loss of their positions if the relevant political powers do not endorse their policies. Alternatively, administrative agencies may be incapacitated by "starving them of resources" where political will is not being attained.[73]

This problem may be offset to some extent by altering the personnel tasked with crafting criminal procedure rules. There is a general assumption in the literature that law enforcement agency personnel are best suited to the task of crafting rules given their expertise in criminal procedure.[74] Yet, the optics of allowing law enforcement to be in charge of making criminal procedure rules likely accentuates fears arising from majoritarian and public choice theory. There is no reason why independent, arm's length personnel could not be appointed to serve as agency rule-makers. Lawyers with an expertise in criminal procedure—an equal number of which could come from the Crown and defence bar—constitutes one option.

Even assuming it were possible to mitigate these majoritarian and public choice theory concerns, agency rulemaking may still be criticized for being undemocratic. As Professor Martin Shapiro maintains:

---

[71] *Ibid* at 13.
[72] *Ibid*.
[73] *Ibid*.
[74] See Part I.

> Where a Parliamentary government coincides with a two-party system with strong party discipline, decision[-]making is concentrated in a cabinet that bears collective responsibility. This approach to government epitomizes democratic accountability. Voters know exactly whom to hold electorally accountable for everything that the government does or fails to do…. 'Governance' by 'network' and 'epistemic community' has the opposite effect. Where every interested group may participate in the decision[-]making process, the voters have no idea who to reward or blame for results they like or dislike.[75]

This problem is particularly acute in the criminal law context as criminal laws are often popular issues in federal elections. Yet, an informed citizen would understand the challenges of governing complex and rapidly advancing technologies within the legislative context. If it is correct to conclude that legislatures are institutionally unlikely to govern effectively in the digital privacy context, abdicating authority to those who can govern effectively would exemplify responsible governance so long as appropriate checks on agency power are in place.

III. Judicial Processing of "Systemic" Facts

The literature considering the benefits of administrative rulemaking in the criminal procedure context frequently fails to consider institutional reforms to legislative and judicial rule-making that can help ensure criminal procedure rules implicating digital technologies develop more expediently and coherently. The previous Chapter criticized this oversight in the context of typical transactional criminal procedure rules implicating digital technologies. The broader debate about whether panvasive searches might be more amenable to administrative rulemaking presents significantly more complex challenges. In turn, this has prompted Andrew Crespo to rethink the institutional capacity of courts to develop better understandings of what he calls "systemic facts".

[75] See Martin Shapiro, "Administrative Law Unbounded: Reflections on Government and Governance" (2001) 8 Indiana Journal of Global Legal Studies 369 at 372-73.

This term is meant to be distinguished from Kenneth Culp Davis' famous categorization of empirical facts relevant to the judicial process.[76] For Davis, adjudicative facts are concerned with the particular parties to a dispute, what those parties did, and for what reasons.[77] Legislative facts, to the contrary, are concerned with social and economic data about the world and typically arise when courts seek to make policy-like judgments.[78] For Crespo, however, this dichotomy is incomplete as "it fails to appreciate the significance of a unique and distinct form of information: facts that are neither narrowly transactional, like adjudicative facts, nor foreign and external to the decisionmaker, like the archetypal legislative fact."[79] It neglects "to account for information with respect to which a given decision making institution enjoys deep institutional familiarity, privileged (or perhaps even exclusive) access, or both."[80]

This systemic knowledge can help address a key criticism against courts governing panvasive searches: whether courts can appreciate the systemic dynamics of their case law necessary to address broader search policies in a fair and balanced manner. As Crespo observes, "contemporary criminal courts have at their disposal far more information about the systemic and institutional workings of their local justice systems than we—or they—have thus far come close to realizing."[81] Just like any other institution with individual employees, the knowledge of those employees can be aggregated, synthesized, and processed to create greater institutional awareness.[82] In essence, "a criminal court has the capacity as an institution to attain—at least in theory—the very informational breadth of knowledge and expertise that contemporary scholars

[76] See Crespo, "Systemic Facts", *supra* note 2 at 2052-53 citing Kenneth Culp Davis, "An Approach to Problems of Evidence in the Administrative Process" (1942) 55 Harvard Law Review 364.
[77] See Davis, "Administrative Process", *supra* note 76 at 402.
[78] *Ibid* at 403.
[79] See Crespo, "Systemic Facts", *supra* note 2 at 2067.
[80] *Ibid*.
[81] *Ibid* at 2066.
[82] *Ibid* at 2069.

crave in the administrative form—without sacrificing the unique institutional advantages of the judicial process."[83] This in turn allows "for a conceptualization of criminal courts that is broad enough to blend the epistemic virtues of agency-style expertise with the institutional virtues of constitutional judicial review—including the important advantages of neutrality, sensitivity to the interests of marginalized groups, and a balanced regard for civil rights and liberties."[84]

As Crespo explains, systemic facts "reside within the official records, internal case files, transcripts, audio recordings, and administrative metadata routinely generated by the broad network of local trial courts that constitute the American criminal judiciary".[85] Digital technologies have made systemizing and processing these facts possible.[86] Such processing in turn can help govern panvasive policing more effectively by developing detailed understandings of how police exercise their basic powers. Information concerning the consistency with respect to grounds police rely upon to arrest an individual,[87] the accuracy of statements made by police,[88] the rate at which minorities are targeted by police interactions,[89] as well as the accuracy of police predictions,[90] are all currently being synthesized with basic courtroom data. The efficacy of prosecutors is also being

[83] *Ibid*.
[84] *Ibid*.
[85] *Ibid* at 2069-70.
[86] *Ibid* at 2070.
[87] *Ibid* at 2075-78.
[88] *Ibid* at 2078-82. For instance, was the spot of the search actually a "high crime area"?
[89] *Ibid* at 2081-82. Applying this technology to the District of Columbia, Crespo was able to prove "search warrant executions almost perfectly track the city's sharply segregated racial demographics". Similarly see Tracey Meares, "Programming Errors: Understanding the Constitutionality of Stop-and-Frisk as a Program, Not an Incident" (2015) 82 University of Chicago Law Review 159 at 173-74 ("the racial composition of a neighborhood is a statistically significant predictor of the number of police stops [and frisks in a given area] even when controlling for police-reported measures of crime, police-patrol allocations, and other social conditions").
[90] *Ibid* at 2082-85. For instance, courts might be able to answer questions such as "how often do persons performing acts A, B, and C turn out to be committing crime X?"

tested. For instance, researchers are systemically studying failures to disclose relevant information,[91] race-based jury selection,[92] and race-based charging.[93]

If Crespo is correct that courts are already capable of systematizing such information, then why not procedures used by police to search computers and cell phones? The grounds usually relevant in successful intercept order applications? The type of requests made to obtain ISP subscriber information? And most importantly, how efficacious these sorts of searches turn out to be? If these practices are not working or are too often resulting in abusive searches contrary to settled legal doctrine, courts should be aware of this and inform their legal rules and exclusion of evidence decisions accordingly.

To be sure, there are potential problems with courts acquiring the type of systemic knowledge discussed above. As raised earlier, it is possible that judges and counsel simply do not understand digital technologies well enough to compile, organize, and process such a record.[94] I raised and to some extent confirmed this contention in Chapter Two. Training can likely ensure courts are able to compile the information, but partnerships with external empiricists may be necessary to ensure information is processed effectively.[95] Even if some courts cannot afford such an approach, the mere fact of having the data available to a litigant or academic group will likely result in its use, thereby allowing courts to make use of such data.[96]

A further problem would be the costs—both in terms of resources and time—of implementing such a system.[97] Docket courts are often extremely busy and recording various

[91] *Ibid* at 2087-92.
[92] *Ibid* at 2092-96.
[93] *Ibid* at 2096-2101.
[94] *Ibid* at 2104-06.
[95] *Ibid* at 2105-06.
[96] *Ibid* at 2106.
[97] *Ibid*.

aspects of the criminal justice system may result in significant slowdowns in the process.[98] However, keeping such records is not overly difficult in already "digitized" court rooms.[99] Synthesizing these records and making them intelligible may very well require additional employees. Yet, much of the information used in one case will be further usable in other cases, thus potentially saving valuable time and effort in the long term.[100] Courts might also reach out to law enforcement agencies in an effort to obtain and synthesize relevant data for the purpose of better understanding the criminal justice system.[101]

It is also possible that judges may oppose such an expanded role in the fact-finding process on ideological grounds.[102] The reforms might be thought to stunt other beneficial reforms or perpetuate current criminal justice pathologies.[103] In particular, judges ideologically tilted one way might distort fact-finding to serve their political purposes.[104] The fact that judges are not elected in Canada should significantly mitigate such concerns. In systems where appointed judges can reliably be expected to "vote one way" in terms of political outcomes such a concern might necessarily be defeating.[105]

Finally, the changes advanced by Crespo and those I advance in the previous Chapter involve departing from the traditional adversarial framework. I agree with Crespo that the types of proposals advocated are a "step removed" from adjudication of individual cases.[106] Although courts are taking steps outside the trial process to discover (or at least facilitate discovery) of the inner workings of the criminal justice process, this does not necessarily bias courts one way or the

[98] *Ibid* at 2107.
[99] *Ibid* at 2108-09.
[100] *Ibid*.
[101] *Ibid* at 2110-11.
[102] *Ibid* a 2112.
[103] *Ibid*.
[104] *Ibid*.
[105] *Ibid* at 2113 citing resources that make the United States out to be an example of such judicial failure.
[106] *Ibid* at 2114.

other. Moreover, as many applications by the Crown are necessarily *ex parte*,[107] courts employing systemic facts or utilizing externally discovered adjudicative facts can necessarily provide some representation for a class of parties who are typically unable to represent their interests in *ex parte* proceedings: criminal accused.[108]

IV. Contrasting Institutional Approaches

Crespo's observations with respect to the potential for judiciaries to utilize *systemic facts* is a welcome contribution to questions of institutional design. The work in preceding chapters has also explained how *adjudicative facts* can be better understood in the judicial process, a major barrier for courts as observed in Orin Kerr's seminal work.[109] The potential to improve judicial understanding of state use of digital technologies inherent in both suggestions paints courts in a very different light. With a fuller understanding of the potential for each institution to meet the challenges of governing digital privacy, two questions remain. First, which institutional reforms are more likely to take hold? Second, which reforms (or combination thereof) are more likely to be beneficial in the criminal procedure context?

(a) Ground Up Reform or Re-thinking the Norm?

The prospect of Parliament deciding to institute an administrative process for crafting criminal procedure rules faces a number of impediments. As explained above, police may not be open to such additional scrutiny and/or responsibility in terms of notice and comment rule-making.[110] Indeed, the American movement in the 1960s and 1970s rejected a plethora of calls for administrative governance of policing for precisely this reason.[111] It is therefore possible that

[107] *Ibid*. Warrant applications are a primary example.
[108] *Ibid*.
[109] See generally Kerr, "Fourth Amendment", *supra* note 66.
[110] See Friedman and Poromarenko, "Democratic Policing", *supra* note 2 at 1862-65.
[111] For an excellent review, see David Sklansky, "Quasi-Affirmative Rights in Constitutional Criminal Procedure" (2002) 88 Vanderbilt Law Review 1229 at 1272-76.

police agencies would lobby Parliament to ensure such a transfer in rule-making authority would not be put in place.

If there was general political agreement on the proposed administrative approach, strong opposition might still come from the judicial branch. Put simply, courts may not want to give up their institutional power. They may therefore use the constitution as a means of preventing a transfer of power. The American experience is illustrative. Although the American Supreme Court was previously amendable to the idea of utilizing administrative agencies to craft criminal procedure rules,[112] its tone appears to have changed in recent years. Writing for the majority in *Riley v California*,[113] Chief Justice Roberts refused to accede to the argument that agency protocols could be developed as a substitute for Fourth Amendment review to address the many privacy concerns inherent in searching a cell phone incident to arrest. As he starkly observed, "[t]he Founders did not fight a revolution to gain the right to government agency protocols."[114]

These anticipated struggles between institutional actors may serve as a definitive impediment to getting an administrative approach off the ground. As Adrian Vermeule observes, however, one cannot ignore law's steady abnegation to the administrative state over the last century or more.[115] Circumstances now common to criminal procedure—most notably the expansion of complex factual backgrounds requiring nuanced expertise—have been repeatedly used to justify abnegation to the administrative state.[116] As such, one should not be too surprised if the trend also infiltrates the law of criminal procedure.

---

[112] See *United States v Caceres*, (1979) 440 US 741 at 755 ("Regulations governing the conduct of criminal investigations are generally considered desirable, and may well provide more valuable protection to the public at large than the deterrence flowing from the occasional exclusion of items of evidence in criminal trials").
[113] 134 S Ct 2473 (2014).
[114] *Ibid* at 2491.
[115] See Adrian Vermeule, *Law's Abnegation: From Law's Empire to the Administrative State* (Cambridge: Harvard University Press, 2016).
[116] *Ibid*.

In my view, the proposals for improving adjudicative and systemic fact-finding serve as a more politically plausible means for institutional reform. Obviously, these reforms—whether fitting courts with necessary personnel to conduct systemic fact-finding or funding external aid to assist courts with adjudicative fact-finding—require legislative decisions to utilize scarce public resources. Using the reference procedure requires similar legislative will, and also requires legislatures to anticipate or keep a close watch on digital privacy issues percolating in the lower courts. Yet, there are unlikely to be institutional conflicts over such reform. Courts and law enforcement would simply have to do as they are told if Parliament chose to adopt these reforms. Courts would also likely welcome the external fact-finding help, as many judges are keenly aware of the limits of the adversarial process.[117] As a result, Parliamentary will seems to be the only significant barrier impeding reformation of the fact-finding process.

(b) A Multi-Institutional Approach to Criminal Procedure

Given the clear benefits of agency rulemaking, it is worthwhile considering whether adopting such an approach would be normatively desirable, notwithstanding political obstacles. As with any choice of institutional design, there will be multiple trade-offs inherent in placing governing power in one institution over another.[118] As the above review showed, scholars tend to ask whether courts and legislatures *or* agency rule-makers are better able to pass expedient, coherent, and even-handed digital privacy criminal procedure rules. In my view, this debate operates in an unnecessarily dichotomous fashion. As I contend below, there is institutional space for all three rule makers to govern criminal procedure in the digital age.

[117] See Kerr, "Fourth Amendment", *supra* note 66 at 876. No doubt this is true in Canada as well.
[118] See Neil Komesar, *Imperfect Alternatives: Choosing Institutions in Law, Economics, and Public Policy* (Chicago: University of Chicago Press, 1994); Adrian Vermeule, *Judging Under Uncertainty: An Institutional Theory of Legal Interpretation* (Harvard: Harvard University Press, 2006).

Beginning with administrative rule-makers, it is highly likely that they would be more efficient than courts and legislatures. Barriers to passing legislation or the necessity of waiting for a constitutional challenge before courts can act do not hinder agency rulemaking. As long as the agency is well-funded and employs qualified individuals to craft the rules they would likely keep on top of technological developments. Agency rules would also likely be much more coherent than those produced by legislatures and courts. The proposed agency would be able to employ experts in criminal law and digital technologies who could study the relevant technologies in depth before suggesting new rules to the public for comment. Courts and legislatures following the proposals in the previous Chapter would still face some stumbling blocks, as courts would be highly dependent on Parliament to ensure external actors are able to aid the litigation process.

This quicker response time and potential to increase the coherency of the governing rules must nevertheless be weighed against the potential for civil liberties to be severely undercut as a result of agency rulemaking. Such a rule-making emphasis is likely to become institutionally engrained if law enforcement were tasked with making criminal procedure rules, as it would align with majoritarian pressures to be "tough on crime". Perhaps staffing the agency with more neutral rule-makers would mitigate this bias, but it is unlikely to alleviate it completely as agencies may be starved of resources if their rulemaking does not align with government preferences. Moreover, there would be few institutional checks on agency rule-making power. Although citizens and civil rights groups would try to influence the rule-making process via notice and comment procedures, their comments need not be given much weight given the significant amount of deference afforded to administrative rule-makers.

Addressing concerns about majoritarian influence on agency rulemaking has thus far been given short shrift. One possibility which has yet to be explored would be to do away with the

requirement that courts show deference on questions relating to the constitutionality of agency rules. This approach has several benefits. Most obviously, rules would be made prospectively by agency experts. This is a major setback of judicial decision-making, as courts typically prescribe rules *ex post* and generally do not possess expertise in digital technologies. Legislatures also tend to lag significantly behind digital technologies when crafting criminal procedure rules and often fail to utilize their institutional advantages to ensure detailed understandings of technologies before passing rules.[119] A well-funded agency would be able to anticipate use of novel technologies thereby making rules for them even before they are in general use.

Allowing courts to strike down agency rules that are inconsistent with its jurisprudence would require agencies to take civil rights concerns seriously. As with any rule-making institution, the potential of being checked by an alternative branch of government encourages even-handedness. Having agencies craft rules could also be used as a justification for avoiding the circumstance, increasingly common post-*Charter*, where courts are asked to craft police powers. The Court's insistence on granting police significant powers—by creating new common law police powers,[120] filling gaps in statutory powers,[121] or reading down unconstitutional authorizations of police powers to conform with *Charter* standards[122]—sits uncomfortably with its role as protector of constitutional rights.[123]

As James Stribopoulos explains, before enactment of the *Charter* courts cabined police activity by relying on the legality principle.[124] Drawing its inspiration from the rule of law, this

[119] See Chapter Three.
[120] See James Stribopoulos, "In Search of Dialogue: The Supreme Court, Police Powers, and the *Charter*" (2005) 31 Queen's Law Journal 1 at 18-31.
[121] *Ibid* at 31-41.
[122] *Ibid* at 41-49.
[123] *Ibid* at 42, 65 citing among other cases *Hunter v Southam Inc*., [1984] 2 SCR 145 at 169, 11 DLR (4th) 641; *R v Wong*, [1990] 3 SCR 36 at para 35, 120 NR 34.
[124] *Ibid* at 6-13.

principle required that any state interference with liberty be expressly authorized by the legislative branch.[125] This rule was endorsed by the Court's initial jurisprudence interpreting section 8 of the *Charter*.[126] Increases in litigation under the *Charter*, however, exposed many significant gaps in police powers.[127] Although Parliament originally was able to entertain dialogic responses to judicial rulings striking down criminal procedure laws or refusing to fill gaps in police powers,[128] these challenges have become insurmountable in the digital age.[129]

Other reasons also help explain why a court would feel pressured into filling gaps in police powers. The cases that come before criminal courts always involve factually guilty persons. Hindsight provides a subtle pressure that will generally favour finding paths to uphold convictions, especially where the conduct at issue would have been deemed constitutional if it were authorized by law.[130] As Stribopoulos concludes, "[l]ost from view are the many cases of unjustified or abusive stops that involve innocent individuals."[131] This in turn "does not encourage the broader perspective that should be brought to the issue."[132] As criminal accused are unlikely to consistently provide evidence of this broader perspective—such as evidence pertaining to the rate of intrusions onto innocent persons liberty interests—such evidence is unlikely to be given any weight within the adversarial process.

---

[125] *Ibid* at 7-8 citing *Marcotte v Canada (Deputy A.G.)*, [1976] 1 SCR 108 at 115, 19 CCC (2d) 257; Trevor Allan, "Constitutional Rights and Common Law" (1991) 11 Oxford Journal of Legal Studies 453 at 457; Leonard Leigh, *Police Powers in England and Wales*, 2nd ed (London: Butterworths, 1985) at 32-33.
[126] See *Hunter*, *supra* note 123 at 156-57 ("[The *Charter*] is intended to constrain governmental action inconsistent with those rights and freedoms; it is not in itself an authorization for governmental action").
[127] See Stribopoulos, "In Search", *supra* note 120 at 11-12. See also Yves-Marie Morissette, "The Exclusion of Evidence Under the *Canadian Charter of Rights and Freedoms*: What To Do and What Not To Do" (1984) 29 McGill Law Journal 521 at 535.
[128] *Ibid* at 34, 66-70. See also Chapter Three. It is further notable that Stribopoulos observes that dialogue occurred predominantly in the section 8 context, while in other contexts—such as the rules around lawful detention—dialogue was foreclosed by many of the Court's rulings.
[129] See the review provided in Chapters Three and Six.
[130] See Stribopoulos, "In Search", *supra* note 120 at 23. See also William Stuntz, "Warrants and Fourth Amendment Remedies" (1991) 77 Virginia Law Review 881 at 912-13.
[131] *Ibid* at 23, 57-58.
[132] *Ibid* at 57-58 citing *R v Evans*, [1996] 1 SCR 8 at para 8, 131 DLR (4th) 654.

If agencies were in charge of making criminal procedure rules relating to digital technologies, courts would feel significantly less pressure to fill in gaps in police powers. This follows as agencies could be expected to respond efficiently to even the most complex criminal procedure rules given the relatively few barriers that exist for administrative rule-making.[133] Courts could also take comfort in the fact that agencies possess expertise in the field of criminal procedure, including where criminal procedure and digital technologies intersect. Further, where courts believe their rulings will impinge legitimate law enforcement interests in the short term, they may use suspended declarations of invalidity to give agencies time to respond to court rulings.[134]

The relationship between courts and agencies could therefore facilitate a correction of the current judicial role with respect to police powers. Without feeling the need to fill in or correct mistakes by the legislature, courts would be more likely to strictly enforce the legality principle. As explained above, this legal principle is directly related to the rule of law and fits well with the judicial function. Judicially created police powers have the opposite effect. Although the subtle pressures of hindsight will still exert force on judges, the Court could counter this tendency by requiring that agencies provide greater disclosure with respect to the efficacy of their search practices. If an agency is in charge of crafting the rules, it would be reasonable to expect them to also disclose the efficacy of these searches which in turn could be utilized by courts in determining the constitutionality of agency rules.

A number of objections to this proposal may be anticipated. First, it may be retorted that courts would frequently use agency failures to fill gaps in police powers to exclude evidence.

[133] As Stribopoulos observes, this is in fact what happened when the Court, relying on the legality principle, refused to craft new police powers. See Stribopoulos, "In Search", *supra* note 120 at 65-67.
[134] See generally *Schachter v Canada*, [1992] 2 SCR 679, 93 DLR (4th) 1.

However, the proposed role for courts need not result in all searches unauthorized by law resulting in exclusion of evidence. Under the Court's exclusion of evidence test,[135] police could explain why they decided to utilize an unauthorized search technique. Perhaps they understandably misread the authorization, or the search was conducted under exigent circumstances. Such searches need not result in exclusion of evidence. But where law enforcement ignored the fact that there was no authorizing law, the evidence could be excluded to motivate the agency to pass a law using administrative rule-making procedures.

Second, it is also questionable whether courts would have adequate information to conduct a judicial review of state use of complex technologies. As discussed in Chapter Two, courts have significant difficulty understanding digital technologies. Yet, if the agency conducted its rule-making pursuant to the administrative procedures described above, there would always be a factual record upon which to conduct a review. Notice and comment procedures could be particularly helpful in this regard. If notice and comment procedures were not adopted, other reforms could still help courts develop adequate records, such as reforming the intervener process or requiring the Office of the Privacy Commissioner provide overviews of digital technologies likely to come before the courts.[136] As explained in the preceding Chapters, the American appellate process was significantly improved by allowing broad intervener submissions, and the idea of allowing external aid to improve fact-finding holds promise as well.

Third, adopting an administrative approach to criminal procedure without requiring that courts show deference to agency rules would likely increase the costs of administering an already financially overburdened criminal justice system. It is possible that agency rules would be challenged as often as Parliament's laws. As such, in addition to paying for costly agency experts

[135] See *R v Grant*, 2009 SCC 32 at paras 71-86, [2009] 2 SCR 253.
[136] See Chapter Two.

and notice and comment procedures for developing rules, Parliament would still need to maintain a similarly well-staffed judiciary to oversee agency rulemaking. It should not be surprising that increased costs follow when an area of law becomes significantly more complex. Moreover, other areas of government would benefit as the time currently spent by Parliament crafting criminal procedure rules could be allotted to other pressing areas of policy concern. As such, although costs are likely to increase, overall costs of governance need not increase substantially, and the efficacy of criminal procedure rules would benefit significantly.

Finally, it may be objected that the above proposal unwisely removes Parliament from the field of criminal procedure rulemaking. This need not be the case. It would still be prudent for Parliament to decide rules that can be expected to remain relatively stable. The rules governing impaired driving investigations are exemplary. Although such *ex ante* rulemaking can be accomplished by agencies, the added democratic legitimacy of legislative rulemaking makes using the legislative process desirable where feasible. The field of digital technologies, however, arguably makes legislative rulemaking undesirable and thus should be left to agencies, subject to informed judicial review by courts.

Conclusion

The idea that law enforcement agencies could substitute for legislative and judicial criminal procedure rulemaking offers a variety of intriguing institutional benefits. Not only would law enforcement be able to avoid the many impediments inherent in legislative and judicial rulemaking, it would also be able to use its relative expertise in criminal procedure—which necessarily includes expertise in digital technologies—to create a more coherent governing framework. Deferring to agency rulemaking is nevertheless likely to negatively affect civil liberties. As a result, two potential institutional options should be considered when advocating for

criminal procedure rule-making reform. The first set of reforms were outlined in Chapter Six. The second approach would involve Parliament providing an agency with significant criminal procedure rule-making power, subject to strong form judicial review by courts. The latter approach, I suggest, would most optimally achieve efficient, coherent, and even-handed criminal procedure rules, especially those implicating digital technologies.

Chapter Eight

Conclusion

Introduction

The task of crafting criminal procedure rules has been complicated by the onset of the digital age. Although a handful of scholars in the United States have considered which of their institutions is better capable of responding to the challenges of governing digital privacy, very little scholarship has arisen in the Canadian criminal procedure context. This left me with three broad research questions to address in my dissertation. First, do Canadian courts and Parliament have similar difficulties as their American counterparts crafting efficient, coherent, and even-handed digital privacy rules in the criminal procedure context? Second, as each country operates within its own unique institutional environment, what lessons can be learned from comparing the Canadian and American experiences governing digital privacy in the criminal procedure context? Finally, what strategies might be devised to improve Canada's institutional capacity to craft digital privacy criminal procedure rules?

I. Overview of Dissertation

The first question identified was empirical, as a void was present in the literature concerning the abilities of Canadian courts and Parliament to respond to the challenges of

governing digital privacy. Although efforts of early scholars were valuable, none had set out to conduct a comprehensive review of Parliament's legislative record or to identify with much precision why courts were having significant difficulties crafting digital privacy rules. My review showed that Parliament struggled to pass laws for a variety of reasons, including its frequent minority status and limited ability to devote significant time and resources to study and revise criminal procedure rules. Importantly, however, typical public choice theory concerns did not raise significant governance concerns.

As with American trial courts, Canadian courts often fail to develop well-informed factual records. This may be attributed to a variety of factors inherent to the adversarial process. For instance, it is unreasonable to expect typically indigent accused persons to call appropriate witnesses to explain digital technologies to courts. Even when such evidence is called, some judges were unable to understand the digital technologies for which they were making rules. Finally, traditional adjustments to the adversarial process—such as calling expert witnesses or relying on intervener factums—were often ineffective. Expert witnesses were infrequently called, likely due to resource restraints, while interveners are restricted in the types and amount of submissions they may make to appellate courts.

The second question my dissertation addressed was normative. Given the lack of research outside of the United States regarding the capacity of courts and legislatures to respond to the challenges of governing digital privacy, scholars were unable to draw any lessons from comparative study. With a robust empirical record from Canada and the United States now available, I was able to compare the two countries' experiences and draw several lessons for similarly situated polities.

My comparison revealed that judicial debate about the proper method for interpreting a constitution can be expected to result in less determinate rules. I also found that utilizing broad and flexible language is preferable to imposing rigid standards when drafting constitutional protections against unreasonable searches and seizures. The latter are likely to impede judicial balancing of privacy and security interests. Remedies in the constitutional context should also be flexible to avoid forcing judges to choose between excluding valuable evidence and recognizing a reasonable expectation of privacy in the item being searched. It is also important that the *stare decisis* doctrine be open to allowing rule change given the rapidly advancing nature of digital technologies. Finally, I suggest that the adversarial process ought to allow interveners to make more extensive submissions before courts, especially with respect to correcting factual misunderstandings arising at trial.

As for legislatures, the model of democracy employed impacts the challenges governments face in crafting criminal procedure rules implicating digital technologies. Although a bicameral legislature provides a response to majoritarian concerns, it also makes it much more difficult to pass laws expediently. This has resulted in American lawmakers implementing patchwork and incoherent bodies of law. Although Canada's *de facto* unicameral legislature allows for more focused law making, it also serves to centralize power in the majority political party. The fact that Canada's parliamentary system provides fewer opportunities for lobbying nevertheless mitigates concerns that special interest groups will unfairly influence criminal procedure rules. Being able to lobby multiple venues makes blocking privacy-protecting rules much easier in the American context, while increased concerns about campaign financing allows for more lobbyist influence in America's political system.

The final question my dissertation addressed was prescriptive. A noticeable gap in the literature arose due to too few scholars considering how courts and legislatures could be reformed to address the unique challenges of governing digital privacy. To address this gap, I developed a dialogical framework in which courts and legislatures in Canada could work together to improve governing processes. Under this approach, Parliament should only make rules where the technology is stable or, if the technology is in flux, employ tools such as sunset clauses to ensure any rule does not become significantly outdated. In most instances, however, I suggest that Parliament focus its efforts on helping courts render expedient decisions with informed evidentiary records. It may do so by using the reference procedure to allow courts to decide controversial digital privacy cases. Encouraging external institutions to neutrally describe the operation of technologies likely to be litigated would also aid courts in deciding complex digital privacy issues. Finally, I recommend granting interveners more leeway in making submissions so as to better ensure judges make rules within an informed environment.

With a better understanding of the capacity of courts and legislatures to reform their governing processes, I concluded by considering the merits of an alternative rule-making paradigm for criminal procedure: administrative governance. This recently rejuvenated idea suggests that agencies would be better situated to craft efficient and coherent rules. Even if the reforms to the litigation process advocated in Chapter Six were adopted, administrative agencies would likely still provide more efficient and coherent rules than would courts and legislatures. Changing rule-making paradigms nevertheless comes with the risk that agencies would undercut civil liberties, as courts are typically required to show significant deference to agency-made rules. In the Canadian context, this should give rise to serious reservations about the desirability of adopting an administrative approach to criminal procedure rules.

Given these concerns, I contend that agencies ought to craft detailed criminal procedure rules but still be subject to strong form judicial review. This arrangement allows the proposed criminal procedure agency to use its expertise to craft rules with relatively few barriers, thereby ensuring that the rules adopted would be coherent and keep up with digital technologies. With detailed descriptions of these rules and their rationales, as well as external help processing adjudicative and systemic facts relevant to searches of digital technologies, courts would be well-situated to conduct informed judicial review of criminal procedure rules implicating digital technologies. Although this approach may prove more costly, it deserves to be situated as one of the various options for reform of criminal procedure rule-making in the digital age.

II. Criminal Procedure and Institutional Reform

The analysis and prescriptions offered in my dissertation have been restricted to the realm of criminal procedure and digital technologies. In so doing, I have relied upon a bright line distinction between what is and is not too complex for legislative and judicial rulemaking: digital technologies. It is possible that the line ought not be drawn this way. Although privacy and digital technologies are arguably the worst instance of this problem, many, if not all, areas relating to policing require a sophisticated understanding of complex empirical evidence to craft informed, timely, and even-handed rules. It is questionable whether the adversarial and legislative processes will consistently yield reliable and coherent rules for many of the same reasons outlined throughout my dissertation. If so, it is arguable that my proposed model for governing criminal procedure rules implicating digital technologies ought to be expanded to encompass the entire field of criminal procedure.

There is nevertheless a case to be made for restraint when proposing broad and novel reforms to a field of law. Although the United Kingdom has adopted administrative rulemaking

for crafting a broad range of criminal procedure rules,[1] it is imprudent to assume that such an approach could be transplanted to the Canadian or American context. It is therefore best to hive off the most problematic field of criminal procedure for institutional reform—digital technologies—and leave broader reforms to be assessed at a later date. If the Canadian experience governing digital technologies in the criminal procedure context were to benefit from the institutional framework proposed herein, I would not hesitate to expand the administrative/judicial approach beyond the field of digital technologies.

[1] See the *Police and Criminal Evidence Act*, (1984) § 67; *Police and Criminal Evidence Act 1984 (PACE) Codes of Practice*, online: <https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice>.

Bibliography

I. Articles

Akamine, Tatsuya. "Proposal for a Fair Statutory Interpretation: E-mail Stored in a Service Provider Computer Is Subject to an Interception Under the Federal Wiretap Act" (1999) 7 Journal of Law and Policy 519.

Alarie, Benjamin and Andrew Green. "Interventions at the Supreme Court of Canada: Accuracy, Affiliation, and Acceptance" (2010) 48 Osgoode Hall Law Journal 381.

Allan, Trevor. "Constitutional Rights and Common Law" (1991) 11 Oxford Journal of Legal Studies 453.

Amar, Akhil. "Fourth Amendment First Principles" (1994) 107 Harvard Law Review 757.

Amsterdam, Anthony. "Perspectives on the Fourth Amendment" (1974) 58 Minnesota Law Review 349.

Anckar, Carsten. "On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research" (2008) 11:5 International Journal of Social Research Methodology 389.

Azarian, Reza. "Potentials and Limitations of Comparative Method in Social Science" (2011) 1 International Journal of Humanities and Social Science 113.

Balla, Steven and Benjamin Daniels. "Information Technology and Public Commenting on Agency Regulations" (2007) 1 Regulation and Governance 46.

Barnett, Randy and Evan Bernick, "The Letter and the Spirit: A Unified Theory of Originalism" (2018) 107 Georgetown Law Journal 1.

Blitz, Marc. "Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Trades Image and Identity" (2004) 82 Texas Law Review 1349.

Bamberger, Kenneth & Dierdre Mulligan. "Privacy on the Books and on the Ground" (2011) 63 Stanford Law Review 247.

Bankston, Kevin and Ashkan Soltani. "Tiny Constables and the Cost of Surveillance: Making Cents Out of *United States v. Jones*" (2014) 123 Yale Law Journal 1.

Bar-Gill, Oren and Barry Friedman. "Taking Warrants Seriously" (2012) 106 Northwestern University Law Review 1609.

Breglio, Nola. “Leaving FISA Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance” (2003) 113 Yale Law Journal 179.

Breyer, Stephen. “Our Democratic Constitution” (2002) 77 New York University Law Review 245.

Calabresi, Guido. “The Exclusionary Rule” (2002) 26 Harvard Journal of Law and Public Policy 111.

Cate, Fred. “The Changing Face of Privacy Protection in the European Union and the United States” (1999) 33 Indiana Law Review 173.

Cavoukian, Ann. “Privacy, Transparency, and the Rule of Law: Critical to Preserving Freedom and Liberty” (2005) 19 National Journal of Constitutional Law 193.

Chan, Gerald. “Life After Vu: Manner of Computer Searches and Search Protocols” (2014) 67 Supreme Court Law Review 433.

Chari, Raj, Gary Murphy, and John Hogan. “Regulating Lobbyists: A Comparative Analysis of the United States, Canada, Germany and the European Union” (2007) 78 The Political Quarterly 422.

Clancy, Thomas. “The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures” (1995) 25 University of Memphis Law Review 483.

Cloud, Morgan. “The Fourth Amendment during the Lochner Era: Privacy, Property, and Liberty in Constitutional Theory” (1996) 48 Stanford Law Review 555.

Cockfield, Arthur. “Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance” (2003) 29 Queen's Law Journal 364.

Coglianese, Cary. “Citizen Participation in Rule-Making: Past, Present, and Future” (2006) 55 Duke Law Journal 943.

Collier, David. “The Comparative Method” in Ada Finifter, *Political Science: The State of the Discipline II* (Washington: American Political Science Association, 1993).

Consovoy, William. “The Rehnquist Court and the End of Constitutional *Stare Decisis*: Casey, Dickerson and the Consequences of Pragmatic Adjudication” (2002) Utah Law Review 53.

Coughlan, Steve and Marc Corbet, “Nothing Plus Nothing Equals . . . Something? A Proposal for FLIR Warrants on Reasonable Suspicion” (2005) 23 CR (6th) 239.

Coughlan, Steven. “Telus: Asking the Right Questions About General Warrants” (2013) 100 CR (6th) 290.

Crespo, Andrew. “Regaining Perspective: Constitutional Criminal Adjudication in the U.S. Supreme Court” (2016) 100 Minnesota Law Review 1985.

Crespo, Andrew. “Systemic Facts: Toward Institutional Awareness in Criminal Courts” (2016) 129 Harvard Law Review 2049.

Cuéllar, Mariano-Florentino. “Rethinking Regulatory Democracy” (2005) 57 Administrative Law Review 411.

“Data Mining, Dog Sniffs, and the Fourth Amendment” (2014) 128 Harvard Law Review 691.

Davies, Simon. “Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity” in (eds) Phillip Agre and Marc Rotenberg, *Technology and Privacy: The New Landscape* (Cambridge: MIT Press, 1997).

Davies, Thomas. “Recovering the Original Fourth Amendment” (1999) 98 Michigan Law Review 547.

Davis, Kenneth Culp. “An Approach to Problems of Evidence in the Administrative Process” (1942) 55 Harvard Law Review 364.

Davis, Kenneth Culp. “An Approach to Legal Control of the Police” (1974) 52 Texas Law Review 703.

Dempsey, James. “Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy” (1997) 8 Alberta Law Journal of Science and Technology 65.

Dixon, Rosalind. “The Supreme Court of Canada, Charter Dialogue, and Deference” (2009) 47 Osgoode Hall Law Journal 235.

Dodek, Adam. “Omnibus Bills: Constitutional Constraints and Legislative Liberations” (2017) 48 Ottawa Law Review 1.

Donohue, Laura. “The Fourth Amendment in a Digital World” (2016) 71 New York University Annual Survey of American Law 553.

Dripps, Donald. “Criminal Procedure, Footnote Four, and the Theory of Public Choice; Or, Why Don't Legislatures Give a Damn About the Rights of the Accused?” (1993) 44 Syracuse Law Review 1079.

Dripps, Donald. “Constitutional Theory for Criminal Procedure: *Dickerson*, *Miranda*, and the Continuing Quest for Broad-but-Shallow” (2001) 43 William and Mary Law Review 1.

Epstein, Richard. “The Legal Regulation of Genetic Discrimination: Old Responses to New Technology” (1994) 74 Boston University Law Review 1.

Eskridge, William and Lauren Baer. "The Continuum of Deference: Supreme Court Review of Agency Statutory Interpretations from Chevron to Hamdan" (2008) 96 Georgetown Law Journal 1083.

Fairburn, Michal. "Twenty-Five Years in Search of a Reasonable Approach" (2008) 40 Supreme Court Law Review 55.

Fehr, Colton. "Cell Phone Searches Incident to Lawful Arrest: A Case Comment on the Ontario Court of Appeal's Decision in *R v Fearon*" (2014) 60 Criminal Law Quarterly 343.

Fehr, Colton and Jared Biden. "Divorced from (Technological) Reality: A Response to the Supreme Court of Canada's Reasons in *R v Fearon*" (2016) 20 Canadian Criminal Law Review 93.

Fenrich, William. "Common Law Protection of Individuals' Rights in Personal Information" (1996) 65 Fordham Law Review 951.

Fine, Jordan. "Leaving Dumb Phones Behind: A Commentary on the Warrantless Searches of Smart Phone Data Granted in *R v Fearon*" (2015) 13 Canadian Journal of Law and Technology 171.

Friedman, Barry and Maria Ponomarenko. "Democratic Policing" (2015) 90 New York University Law Review 1827.

Friedman, David. "Privacy and Technology" (2000) 17 Social Philosophy & Policy 186.

Gilbert, Daphne, Ian Kerr, and Jena McGill. "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers" (2006) 51 Criminal Law Quarterly 469.

Godbout, Jean-Francois. "Parliamentary Politics and Legislative Behaviour" in Luc Turgeon et al., eds, *Comparing Canada: Methods and Perspectives on Canadian Politics* (Vancouver: UBC Press, 2014) 171.

Gold, Alan. '"If the Shoe Fits…and Wonderfully so': Part VI of the *Criminal Code* Should be Applied to Digital Communications" (2016) 28 CR (7th) 44.

Gormley, Ken. "One Hundred Years of Privacy" (1992) Wisconsin Law Review 1335.

Gotlieb, Calvin. "Privacy: A Concept Whose Time has Come and Gone" in (eds) David Lyon & Elia Zuriek, *Computers, Surveillance, and Privacy* (Minneapolis: University of Minnesota Press, 1996).

Guarda, Dalla. "Digital Encryption and the Freedom from Self-incrimination: Implications for the Future of Canadian Criminal Investigations and Prosecutions" (2014) 61 Criminal Law Quarterly 119.

Gustafson, Kaaryn. “The Criminalization of Poverty” (2009) 99 Journal of Criminal Law & Criminology 643.

Henschel, Marcy. “Obtaining Records of Cell Phone Calls and Text Messages” (Paper delivered at the Federation of Law Societies of Canada 42nd National Criminal Law Program, Edmonton Alberta, July 2015) [unpublished].

Hogg, Peter and Allison Bushell. “The Charter Dialogue between Courts and Legislatures (Or Perhaps the Charter of Rights Isn’t Such a Bad Thing After All)” (1997) 35 Osgoode Hall Law Journal 75.

Hogg, Peter, Allison Bushell Thornton, and Wade Wright. “Charter Dialogue Revisited – Or ‘Much Ado About Metaphors’” (2007) 45 Osgoode Hall Law Journal 1.

Hopper, Benjamin. “Amici Curiae at the United States Supreme Court and the Australian High Court: A Lesson in Balancing Amicability” (2017) 51 John Marshall Law Review 81.

Howell, Beryl. “Seven Weeks: The Making of the USA-PATRIOT Act” (2004) 72 George Washington Law Review 1145.

Herbert, Ian. “Where Are We with Location Tracking: A Look at the Current Technology and the Implications on Fourth Amendment Jurisprudence” (2011) 16 Berkeley Journal of Criminal Law 442.

Jacobi, Tonja. “The Law and Economics of the Exclusionary Rule” (2011) 87 Notre Dame Law Review 585.

Jacobs, James and Dimitra Blitsa. “Sharing Criminal Records: The United States, the European Union, and Interpol Compared” (2008) 30 Loyola of Los Angeles International & Comparative Law Review 125.

Jacobs, James and Tamara Crepet. “The Expanding Scope, Use, and Availability of Criminal Records” (2008) 11 New York University Journal of Legislation and Public Policy 177.

Jacobsen, Kristen. “Game of Phones, Data Isn’t Coming: Modern Mobile Operating System Technology and Its Chilling Effect On Law Enforcement” (2017) 85(2) George Washington Law Review 566.

Jansen, Nils. “Comparative Law and Comparative Knowledge” in Mathias Reimann and Reinhard Zimmermann, eds, *The Oxford Handbook of Comparative Law* (Oxford: Oxford University Press, 2006) 305.

Kearney, Joseph and Thomas Merrill. “The Influence of Amicus Curiae Briefs on the Supreme Court” (2000) 148 University of Pennsylvania Law Review 743.

Kerr, Orin. "Internet Surveillance Law After the USA Patriot Act: The Big Brother that Isn't" (2003) 97 Northwestern University Law Review 607.

Kerr, Orin. "Lifting the 'Fog' of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law" (2003) 54 Hastings Law Journal 805.

Kerr, Orin. "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution" (2004) 102 Michigan Law Review 801.

Kerr, Orin. "Congress, the Courts, and New Technologies: A Response to Professor Solove" (2005) 74 Fordham Law Review 779.

Kerr, Orin. "Ex Ante Regulation of Computer Search and Seizure" (2010) 96 Virginia Law Review 1241.

Kerr, Orin. "The Mosaic Theory of the Fourth Amendment" (2012) 111 Michigan Law Review 311.

Klarman, Michael. "The Puzzling Resistance to Political Process Theory" (1991) 77 Vandervort Law Review 747.

Kozel, Randy. "*Stare Decisis* as Judicial Doctrine" (2010) 67 Washington & Lee Law Review 411.

Lah, Frederick. "Are IP Addresses 'Personal Identifiable Information'?" (2008) 4:3 I/S: A Journal of Law & Policy for the Information Society 681.

Lash, Kurt. "The Cost of Judicial Error: Stare Decisis and the Role of Normative Theory" (2014) 89 Notre Dame Law Review 2189.

Lee, Cynthia. "Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness Analysis" (2012) 81 Mississippi Law Journal 1133.

Lee, Thomas. "*Stare Decisis* in Historical Perspective: From the Founding Era to the Rehnquist Court" (1999) 52 Vanderbilt Law Review 647.

Lerner, Craig. "The Reasonableness of Probable Cause" (2003) 81 Texas Law Review 951.

Lerner, Craig. "Legislators as the 'American Criminal Class': Why Congress (Sometimes) Protects the Rights of Defendants" (2004) 101 University of Illinois Law Review 599.

Levinson, Daryl. "Making Government Pay" (2000) 67 University of Chicago Law Review 345.

Levenson, Justin, Mark Bennett, and Koichi Hioki. "Judging Implicit Bias: A National Empirical Study of Judicial Stereotypes" (2017) 69 Florida Law Review 63.

Lijphart, Arend. “Comparative Politics and Comparative Method” (1971) 65 The American Political Science Review 682.

Lijphart, Arend. “The Comparable-Cases Strategy in Comparative Research” (1975) 8:2 Comparative Political Studies 158.

Macey, Jonathan. “Transaction Costs and the Normative Elements of the Public Choice Model: An Application to Constitutional Theory” (1988) 74 Virginia Law Review 471.

Maclin, Tracey. “The Central Meaning of the Fourth Amendment” (1993) 35 William & Mary Law Review 197.

Maclin, Tracey. “What Can Fourth Amendment Doctrine Learn from Vagueness Doctrine” (2001) 3 University of Pennsylvania Journal of Constitutional Law 398.

Magotiaux, Susan. “Out of Sync: Section 8 and Technological Advancements in Supreme Court Jurisprudence” (2015) 71 Supreme Court Law Review 501.

Mashaw, Jerry. “Public Law and Public Choice: Critique and Rapprochement” in Daniel Farber and Anne O’Connell, eds, *Research Handbook on Public Choice and Public Law* (Cheltenham: Edward Elgar Publishing Ltd, 2010) at 30.

Massicotte, Louis. “Omnibus Bills in Theory and Practice” (2013) 36 Canadian Parliamentary Review 13.

Mayeda, Graham. “My Neighbour’s Kid Just Bought a Drone…New Paradigms for Privacy Law in Canada” (2015) 35 National Journal of Constitutional Law 59.

Mazza, Stephen. “Taxpayer Privacy and Tax Compliance” (2003) 51 University of Kansas Law Review 1065.

McGowan, Carl. “Rule-Making and the Police” (1972) 70 Michigan Law Review 659.

McIntyre, Joshua. “Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information” (2011) 60 DePaul Law Review 895.

Meares, Tracey. “Programming Errors: Understanding the Constitutionality of Stop-and-Frisk as a Program, Not an Incident” (2015) 82 University of Chicago Law Review 159.

Meehan, Eugene, Marie-France Major, and Thomas Slade. “Getting In, Getting Heard, Getting Practical: Intervening in Appellate Courts Across Canada” (2017) 46 The Advocates’ Quarterly 261.

Merrill, Thomas. “Does Public Choice Theory Justify Judicial Activism After All?” (1997) 21 Harvard Journal of Law & Public Policy 219.

Monaghan, Henry "*Stare Decisis* and Constitutional Adjudication" (1988) 88 Columbia Law Review 723.

Morgan, Charles. "Employer Monitoring of Employee Electronic Mail and Internet Use" (1999) 44 McGill Law Journal 849.

Morissette, Yves-Marie. "The Exclusion of Evidence Under the *Canadian Charter of Rights and Freedoms*: What To Do and What Not To Do" (1984) 29 McGill Law Journal 521.

Murphy, Erin. "The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions" (2013) 111 Michigan Law Review 485.

Nadler, Janice. "No Need to Shout: Bus Sweeps and the Psychology of Coercion" (2002) 202 Supreme Court Review 153.

Orr Larsen, Allison. "The Trouble with Amicus Facts" (2014) 100 Virginia Law Review 1757.

Owsley, Brian. "The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in its Electronic Surveillance" (2013) 16 Journal of Constitutional Law 1.

Paciocco, David. "Proof and Progress: Coping with the Law of Evidence in a Technological Age" (2013) 11:2 Canadian Journal of Law and Technology 181.

Packer, Herbet. "Two Models of the Criminal Process" (1964) 113 University of Pennsylvania Law Review 1.

Parsons, Christopher. "Unpacking the Potential Costs of Bill C-30" (2012) 9:6 Canadian Privacy Law Review 57.

Parsons, Christopher. "Stuck on the Agenda: Drawing Lessons from the Stagnation of 'Lawful Access' Legislation in Canada" in Michael Geist, ed, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (Ottawa: University of Ottawa Press, 2015) 257.

Penney, Steven. "Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach" (2007) 97 Journal of Criminal Law and Criminology 477.

Penney, Steven. "Updating Canada's Communications Surveillance Laws: Privacy and Security in the Digital Age" (2008) 12 Canadian Criminal Law Review 115.

Penney, Steven. "Searches of Digital Devices Incident to Arrest: *R v Fearon*" (2014) 23 Constitutional Forum 1.

Penney, Steven. "The Digitization of Section 8 of the *Charter*: Reform or Revolution?" (2014) 67 Supreme Court Law Review 505.

Penney, Steven. "'Mere Evidence'? Why Customs Searches of Digital Devices Violate Section 8 of the *Charter*" (2016) 49:2 University of British Columbia Law Review 485.

Penney, Steven and Dylan Gibbs. "Law Enforcement Access to Encrypted Data: Legislative Responses and the *Charter*" (2017) 63 McGill Law Journal 201.

Ponsford, Matthew. "The Lawful Access Fallacy: Voluntary Warrantless Disclosures, Customer Privacy, and Government Requests for Subscriber Information" (2017) 15 Canadian Journal of Law and Technology 153.

Pomerance, Renee. "Flirting with Frankenstein: The Battle between Privacy and our Technological Monsters" (2016) 20 Canadian Criminal Law Review 149.

Posner, Eric and Adrian Vermeule. "Crisis Governance in the Administrative State: 9/11 and the Financial Meltdown of 2008" (2009) 76 University of Chicago Law Review 1613.

Posner, Richard. "The Right of Privacy" (1978) 12 Georgia Law Review 393.

Post, Robert. "Three Concepts of Privacy" (2001) 89 Georgetown Law Journal 2087.

Quigley, Tim. "*R. v. Fearon*: A Problematic Decision" (2015) 15 CR (7^{th}) 281.

Raigrodski, Dana. "Reasonableness and Objectivity: A Feminist Discourse of the Fourth Amendment" (2008) 17 Texas Journal of Women and the Law 153.

Rachlinski, Jeffrey, Sherri Lynn Johnson, Andrew Wistrich, and Chris Guthrie. "Does Unconscious Racial Bias Affect Trial Judges?" (2009) 84 Notre Dame Law Review 1195.

Reamey, Gerald. "When 'Special Needs' Meet Probable Cause: Denying the Devil Benefit of Law" (1992) 19 Hastings Constitutional Law Quarterly 340.

Renan, Daphna. "The Fourth Amendment as Administrative Governance" (2016) 68 Stanford Law Review 1039.

Renan, Daphna. "The FISC's Stealth Administrative Law" in Zachary Goldman and Samuel Rascoff, eds, *Global Intelligence Oversight: Governing Security in the Twenty-First Century* (Oxford: Oxford University Press, 2016) 121.

Roach, Kent. "Dialogic Judicial Review and its Critics" (2004) 23 Supreme Court Law Review 49.

Roach, Kent. "Dialogue or Defiance: Legislative Reversals of Supreme Court Decisions in Canada and the United States" (2006) 4 International Journal of Constitutional Law 347.

Sartori, Giovanni. "Comparing and Miscomparing" (1991) 3 Journal of Theoretical Politics 243.

Scanlan, Daniel. “Issues in Digital Evidence and Privacy: Enhanced Expectations of Privacy and Appellate Lag Times” (2012) 16 Canadian Criminal Law Review 301.

Schuck, Christina. “A Search for the Caselaw to Support the Computer Search Guidance in *United States v. Comprehensive Drug Testing*” (2012) 16 Lewis & Clark Law Review 741.

Schwartz, Paul. “Privacy and Democracy in Cyberspace” (1999) 52 Vanderbilt Law Review 1609.

Schwartz, Randy. “*Criminal Update:* The Online Crime Act (Bill C-13) and New Police Search Powers”, (Paper delivered during Webinar presented by Osgoode Hall Law School, May 11, 2015) [unpublished].

Shapiro, Martin. “Administrative Law Unbounded: Reflections on Government and Governance” (2001) 8 Indiana Journal of Global Legal Studies 369.

Simmons, Omari. “Picking Friends from the Crowd: Amicus Participation as Political Symbolism” (2009) 42 Connecticut Law Review 185.

Simmons, Ric. “Can Winston Save Us from Big Brother? The Need for Judicial Consistency in Regulating Hyper-Intrusive Searches” (2003) 55 Rutgers Law Review 547.

Simmons, Ric. “Ending the Zero-Sum Game: How to Increase the Productivity of the Fourth Amendment” (2013) 36 Harvard Journal Law & Public Policy 449.

Singhal, Anjali. “The Piracy of Privacy? A Fourth Amendment Analysis of Key Escrow Cryptography” (1996) 7 Stanford Law and Policy Review 189.

Sitaraman, Ganesh and Ingrid Wuerth. “The Normalization of Foreign Relations Law” (2015) 128 Harvard Law Review 1897.

Sklansky, David. “The Fourth Amendment and Common Law” (2000) 100 Columbia Law Review 1739.

Sklansky, David. “Quasi-Affirmative Rights in Constitutional Criminal Procedure” (2002) 88 Vanderbilt Law Review 1229.

Sklansky, David. “Too Much Information: How Not to Think About Privacy and the Fourth Amendment” (2014) 102 California Law Review 1069.

Sklansky, David. “Two More Ways Not to Think about Privacy and the Fourth Amendment” (2015) 82 The University of Chicago Law Review 223.

Slane, Andrea and Lisa Austin, “What’s in a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations” (2011) 57 Criminal Law Quarterly 486.

Slobogin, Christopher. “Why Liberals Should Chuck the Exclusionary Rule” (1999) 1999 University of Illinois Law Review 363.

Slobogin, Christopher. “Rehnquist and Panvasive Searches” (2013) 82 Mississippi Law Journal 307.

Slobogin, Christopher. “Policing as Administration” (2016) 165 University of Pennsylvania Law Review 91.

Small Jr, Joseph and Robert Burgoyne. “Criminal Prosecutions Initiated by Administrative Agencies: the FDA, the Accardi Doctrine and the Requirement of Consistent Agency Treatment” (1987) 78 Journal of Criminal Law & Criminology 87.

Smith, Peter. “How Different are Originalism and Non-Originalism?” (2011) 62 Hastings Law Journal 707.

Smith, Stephen. “The *Carpenter* Chronicle: A Near-Perfect Surveillance” (2018) 132 Harvard Law Review 205.

Solove, Daniel. “The Darkest Domain: Deference, Judicial Review, and the Bill of Rights” (1999) 84 Iowa Law Review 941.

Solove, Daniel. “Digital Dossiers and the Dissipation of Fourth Amendment Privacy” (2002) 75 California Law Review 1083.

Solove, Daniel. “Fourth Amendment Codification and Professor Kerr’s Misguided Call for Judicial Deference” (2005) 74 Fordham Law Review 747.

Solove, Daniel and Chris Hoofnagle. “A Model Regime of Privacy Protection” (2006) University of Illinois Law Review 357.

Solove, Daniel. “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy” (2007) 44 San Diego Law Review 745.

Stack, Kevin. “Interpreting Regulations” (2012) 111 Michigan Law Review 355.

Stigler, George. “An Introduction to Privacy in Economics and Politics” (1980) 9 Journal of Legal Studies 623.

Strahilevitz, Lior. “Reunifying Privacy Law” (2010) 98 California Law Review 2007.

Stribopoulos, James. “Lessons from the Pupil: A Canadian Solution to the American Exclusionary Rule” (1999) 22 Boston College International & Comparative Law Review 77.

Stribopoulos, James. “In Search of Dialogue: The Supreme Court, Police Powers, and the *Charter*” (2005) 31 Queen’s Law Journal 1.

Stribopoulos, James. “Packer’s Blind Spot: Low Visibility Encounters and the Limits of Due Process versus Crime Control” in François Tanguay-Renaud & James Stribopoulos, eds, *Rethinking Criminal Law Theory: New Canadian Perspectives in the Philosophy of Domestic, Transnational and International Criminal Law* (Oxford: Hart Publishing, 2012) 193.

Stuntz, William. “Warrants and Fourth Amendment Remedies” (1991) 77 Virginia Law Review 881.

Stuntz, William. “Implicit Bargains, Government Power, and the Fourth Amendment” (1992) 44 Stanford Law Review 553.

Stuntz, William. “Privacy’s Problem and the Law of Criminal Procedure” (1995) 93 Michigan Law Review 1016.

Stuntz, William. “The Substantive Origins of Criminal Procedure” (1995) 105 Yale Law Journal 393.

Stuntz, William. “The Pathological Politics of Criminal Law” (2001) 100 Michigan Law Review 505.

Stuntz, William. “Local Policing after the Terror” (2002) 111 Yale Law Journal 2137.

Sundby, Scott. “Everyman's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?” (1994) 94 Columbia Law Review 1751.

Sunstein, Cass. “Foreword: Leaving Things Undecided” (1996) 110 Harvard Law Review 6.

Sunstein, Cass and Adrian Vermeule, “Interpretations and Institutions” (2003) 101 Michigan Law Review 885.

Sunstein, Cass and Thomas Miles. “Do Judges Make Regulatory Policy? An Empirical Investigation of Chevron” (2006) 73 University of Chicago Law Review 823.

Swire, Peter. “*Katz* is Dead: Long Live *Katz*” (2004) 102 Michigan Law Review 904.

Thompson, Anthony. “Stopping the Usual Suspects: Race and the Fourth Amendment” (1999) 74 New York University Law Review 956.

Turgeon, Luc. “Introduction” in Luc Turgeon et al., eds, *Comparing Canada: Methods and Perspectives on Canadian Politics* (Vancouver: UBC Press, 2014) 3.

Warren, Samuel and Louis Brandeis. “The Right to Privacy” (1890) 4 Harvard Law Review 193.

Wasserstrom, Silas and Louis Michael Seidman. "The Fourth Amendment as Constitutional Theory" (1988) 77 Georgia Law Journal 19.

Weiden, David. "Judicial Politicization, Ideology, and Activism at the High Courts of the United States, Australia, and Canada" (2011) 64 Political Research Quarterly 335.

White, Jarrod. "E-Mail@Work.Com: Employer Monitoring of Employee E-Mail" (1997) 48 Alabama Law Review 1079.

Williamson, Jillian and Kelsey Sitar. "Placing Proper Restraints on the General Warrant: Searching of Data Storage Devices Following Lawful Seizure" (2015) 15 Canadian Criminal Law Review 57.

II. Books

Chen, Brian. *Always On: How the iPhone Unlocked the Anything-Anytime-Anywhere Future—and Locked Us In* (Boston: Da Capo Press, 2012).

Coughlan, Steven. *Criminal Procedure*, 2nd ed (Toronto: Irwin Law, 2012).

Cox, Gary and Mathew McCubbins. *Legislative Leviathan: Party Government in the House* (Berkeley: University of California Press, 1993).

Docherty, David. *Legislatures* (Vancouver: UBC Press, 2005).

Downs, Anthony. *An Economic Theory of Democracy* (New York: Harper, 1957).

Ely, John Hart. *Democracy and Distrust* (Cambridge: Harvard University Press, 1980).

Epstein, David and Sharyn O'Halloran. *Delegating Powers: A Transaction Cost Politics Approach to Policy Making Under Separate Powers* (Cambridge: Cambridge University Press, 1999).

Farber, Daniel and Anne O'Connell, eds. *Research Handbook on Public Choice and Public Law* (Cheltenham: Edward Elgar Publishing Ltd, 2010).

Ferguson, Gerry. *Global Corruption: Law, Theory & Practice*, 3rd ed (Victoria: University of Victoria Press, 2018).

Fontana, James and David Keeshan, *The Law of Search & Seizure in Canada*, 8th ed (Markham: Lexis Nexis, 2010).

Fontana, James and David Keeshan, *The Law of Search & Seizure in Canada*, 9th ed (Toronto: Lexis Nexis, 2015).

Frickey, Philip and Daniel Farber. *Law and Public Choice: A Critical Introduction* (Chicago: University of Chicago Press, 1992).

Harten, Gus Van, et al. *Administrative Law: Cases, Text, and Materials*, 7th ed (Toronto: Emond, 2015).

Hogg, Peter. *Constitutional Law of Canada* (Toronto: Thomson Reuters Canada, 2009).

Hubbard, Robert, Peter Brauti, and Scott Fenton. *Wiretapping and Other Electronic Surveillance: Law and Procedure*, Looseleaf (Aurora: Canada Law Book Inc, 2005).

Husa, Jaako. *A New Introduction to Comparative Law* (Portland: Hart Publishing, 2015) at 71.

Hutchinson, Scott and Michael Bury, *Search and Seizure Law in Canada*, loose-leaf (updated 1 January 2018).

Israel, Jerold and Wayne Lafave. *Criminal Procedure in a Nutshell*, 5th ed (1993).

Komesar, Neil. *Imperfect Alternatives: Choosing Institutions in Law, Economics, and Public Policy* (Chicago: University of Chicago Press, 1994).

Lafave, Wayne, Jerold Israel, and Nancy King. *Criminal Procedure*, 3rd ed (St. Paul: West Group, 2000).

Lafave, Wayne. *Search and Seizure*, 4th ed (2004).

Lawson, Philippa. *Moving towards a Surveillance Society: Proposals to Expand "Lawful Access" in Canada* (Vancouver: British Columbia Civil Liberties Association, 2012).

Leigh, Leonard. *Police Powers in England and Wales*, 2nd ed (London: Butterworths, 1985).

Lessig, Lawrence. *Code and Other Laws of Cyber Space* (Harvard: Basic Books, 1999).

Lessig, Lawrence. *Code: Version 2.0* (New York: Basic Books, 2006).

Mathen, Carrisma. *Courts Without Cases: The Law and Politics of Advisory Opinions* (Oxford: Hart, 2019).

Mayhew, David. *Congress: The Electoral Connection* (New Haven: Yale University Press, 1974).

Mueller, Denis. *Public Choice III* (Cambridge: Cambridge University Press, 2003).

Packer, Herbet. *The Limits of the Criminal Sanction* (Stanford: Stanford University Press, 1968).

Penney, Steven, Vincenzo Rondinelli, and James Stribopoulos, *Criminal Procedure in Canada* (Toronto: Lexis Nexis, 2018).

Przeworski, Adam and Henry Teune. *The Logic of Comparative Social Inquiry* (New York: John Wiley, 1970).

Roach, Kent. *Due Process and Victims' Rights: The New Law and Politics of Criminal Justice* (Toronto: University of Toronto Press, 1999).

Roach, Kent. *The Supreme Court on Trial: Judicial Activism or Democratic Dialogue* (Toronto: Irwin Law, 2001).

Scanlan, Daniel. *Digital Evidence in Criminal Law* (Aurora: Canada Law Book, 2011).

Slobogin, Christopher. *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* (Chicago: University of Chicago Press, 2007).

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

Solove, Daniel. *Understanding Privacy* (Harvard: Harvard University Press, 2008).

Solove, Daniel. *Nothing to Hide: The False Trade-off between Privacy and Security* (New Haven: Yale University Press, 2011).

Stephen Brooks, Douglas Koopman, and Matthew Wilson, *Understanding American Politics*, 2nd ed (Toronto: University of Toronto Press, 2013).

Stretton, Hugh. *The Political Sciences: General Principles of Selection in Social Science and History* (London: Routledge, 1969).

Stuart, Don. *Charter Justice in Canadian Criminal Law*, 6th ed (Toronto: Carswell, 2014).

Tanovich, David. *The Colour of Justice: Policing Race in Canada* (Toronto: Irwin Law, 2006).

Taslitz, Andrew and Margaret Paris. *Constitutional Criminal Procedure* (1997).

Vermeule, Adrian. *Judging Under Uncertainty: An Institutional Theory of Legal Interpretation* (Harvard: Harvard University Press, 2006).

Vermeule, Adrian. *Law's Abnegation: From Law's Empire to the Administrative State* (Cambridge: Harvard University Press, 2016).

III. Jurisprudence

(i) Canadian

A (Re), 2017 SKPC 90, 142 WCB (2d) 685.

Application for a General Warrant pursuant to S.487.01 of the Criminal Code, Re, 2002 SKPC 11, 52 WCB (2d) 517.

Attorney-General for Manitoba v Manitoba Egg and Poultry Association et al., [1971] SCR 689, 19 DLR (3d) 169.

Canada (Attorney General) v Bedford, 2013 SCC 72, [2013] 3 SCR 1101.

Canada (Minister of Citizenship and Immigration) v Vavilov, 2019 SCC 65.

Doré v Barreau du Québec, 2012 SCC 12, [2012] 1 SCR 395.

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

Keating v Nova Scotia (Attorney General), 2001 NSSC 85, 194 NSR (2d) 290.

Marcotte v Canada (Deputy A.G.), [1976] 1 SCR 108, 19 CCC (2d) 257.

Ontario (Ministry of the Attorney General) v Law Society of Upper Canada, [2010] OJ No 2975 (ONSC).

R c Bordage, 146 CCC (3d) 549, [2000] JQ No 2045 (QBCA).

R c Doucet, 18 CR (6th) 103, [2003] JQ No 18497.

R c Solomon (1992), 77 CCC (3d) 264, 16 CR (4th) 193.

Re C.(S.), 2006 ONCJ 343, 71 WCB (2d) 241.

Reference re Remuneration of Judges of the Provincial Court, [1998] 1 SCR 3, 155 DLR (4th) 1.

Reference re ss. 193 and 195.1(1)(C) of the Criminal Code (Man.), [1990] 1 SCR 1123, 68 Man R (2d) 1.

Reference re Workers' Compensation Act, 1983 (Nfld.) (Application to intervene), [1989] 2 SCR 335, 76 Nfld & PEIR 185.

Re Subscriber Information, 2015 ABPC 178, 123 WCB (2d) 553.

R v Araujo, 2000 SCC 65, [2000] 2 SCR 992.

R v Backhouse (2005), 194 CCC (3d), 28 CR (6th) 31.

R v Bahr, 2006 ABPC 360, 434 AR 1.

R v Beauchamp (2008), 58 CR (6th) 177, 171 CRR (2d) 358 (OSCJ).

R v Beitel, 2011 ONSC 5394, 243 CRR (2d) 296.

R v Belcourt, 2015 BCCA 126, 322 CCC (3d) 93.

R v Bishop, 2007 ONCJ 441, 75 WCB (2d) 258.

R v Braudy, [2009] OJ No 347, 81 WCB (2d) 561.

R v Boudreau-Fontaine, 2010 QCCA 1108, 93 WCB (2d) 47.

R v Brousseau, 2010 ONSC 6753, 264 CCC (3d) 562.

R v Caslake, [1998] 1 SCR 51, 121 CCC (3d) 97.

R v Cater, 2012 NSPC 2, 312 NSR (2d) 242.

R v Cheung, 100 CCC (3d) 441, 1995 CarswellBC627 (BCSC).

R v Cody, 2007 QCCA 1276, 228 CCC (3d) 331.

R v Cole, 2012 SCC 53, [2012] 3 SCR 34.

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

R v Comeau, 2018 SCC 15, [2018] 1 SCR 342.

R v Chehil, 2013 SCC 49, [2013] 3 SCR 220

R v Croft, 2013 ABQB 640, 573 AR 339.

R v Cross, 2007 CanLII 64141 (ONSC).

R v Cuttell, 2009 ONCJ 471, [2009] OJ No 4053.

R v Daniels, 2004 NLCA 73, 242 Nfld & PEIR 290.

R v Dhillon, 2013 BCSC 869, 106 WCB (2d) 503.

R v Doiron, 2007 NBCA 41, 315 NBR (2d) 205.

R v Doiron, [2007] SCCA No 413.

R v Dragos (2009), 200 CRR (2d) 227, [2009] OJ No 4045 (SCJ).

R v Duarte, [1990] 1 SCR 30, 53 CCC (3d) 1.

R v Edwards (ONSC), [1999] OJ No 3819, 44 WCB (2d) 45.

R v Edwards and Brown, 2014 ONSC 6323, 118 WCB (2d) 67.

R v Evans, [1996] 1 SCR 8, 131 DLR (4th) 654.

R v Fearon, 2010 ONCJ 645, [2010] OJ No 5745.

R v Fearon, 2013 ONCA 106, 296 CCC (3d) 331.

R v Fearon, 2014 SCC 77, [2014] 3 SCR 621.

R v Fegan (1993), 13 OR (3d) 88, 80 CCC (3d) 356 (ONCA).

R v Ferguson, 2008 SCC 6, [2008] 1 SCR 96.

R v Finnikin, 2009 CanLii 82187 (ONSC).

R v Franko, 2012 ABQB 282, 541 AR 23.

R v Friers, 2008 ONCJ 740, [2008] OJ No 5646.

R v Giles, 2007 BCSC 1147, 77 WCB (2d) 469.

R v Godoy, 33 OR (3d) 445, 115 CCC (3d) 272 (ONCA).

R v Godoy, [1999] 1 SCR 311, 168 DLR (4th) 257.

R v Golden, 2001 SCC 83, [2001] 3 SCR 679.

R v Gomboc, 2010 SCC 55, [2010] 3 SCR 211.

R v Grandison, 2016 BCSC 1712, 342 CCC (3d) 249.

R v Grant, 2009 SCC 32, [2009] 2 SCR 353.

R v Griffith (1988), 44 CCC (3d) 63, 49 CRR 323 (Ont Dist Crt).

R v Ha, 2009 ONCA 340, 245 CCC (3d) 546.

R v Hackert, [1997] OJ No 6384 (Ont Gen Div).

R v Hackert, [2000] OJ No 3495, 2000 CarswellOnt 3325 (ONCA).

R v HG, 2005 QCCA 1160, [2005] JQ No 17665.

R v Hiscoe, 2011 NSPC 84, 310 NSR (2d) 142.

R v Hiscoe, 2013 NSCA 38, 297 CCC (3d) 35.

R v Howell, 2011 NSSC 284, 313 NSR (2d) 4.

R v Jones, 2011 ONCA 632, 107 OR (3d) 241.

R v Jones, 2015 SKPC 29, 468 Sask R 264.

R v Jones, 2017 SCC 60, [2017] 2 SCR 696.

R v Khan, 2014 ONSC 5664, 122 WCB (2d) 259.

R v Khiamal (1990), 83 Alta LR (2d) 359, 106 AR 246 (ABQB).

R v Kuitenen, 2001 BCSC 677, 45 CR (5th) 131.

R v Kwok, [2008] OJ No 2414, 78 WCB (2d) 21 (ONCJ).

R v Liew, 2012 ONSC 1826, [2012] OJ No 1365.

R v Lubovac (1989), 52 CCC (3d) 551, 1989 CarswellAlta 791 (ABCA).

R v Largie, 2010 ONCA 548, 101 OR (3d) 561.

R v Largie, [2010] SCCA No 460.

R v Little, 2009 CanLII 41212, [2009] OJ No 3278.

R v Lucas, 2014 ONCA 561, 121 OR (3d) 303.

R v Lucas, [2014] SCCA No 461.

R v Manley, 2011 ONCA 128, 269 CCC (3d) 40.

R v Mann, 2012 BCSC 1247, CRR (2d) 49.

R v Mann, 2014 BCCA 231, 310 CCC (3d) 143.

R v Marakah, 2017 SCC 59, [2017] 2 SCR 608.

R v McNeice, 2010 BCSC 1544, 91 WCB (2d) 178.

R v McNeice, 2013 BCCA 98, [2013] BCWLD 4244.

R v Mohammed, [2007] OJ No 700, 152 CRR (2d) 129 (ONSC).

R v Morelli, 2010 SCC 8, [2010] 1 SCR 253.

R v Nguyen, 2004 BCSC 76, 20 CR (6th) 151.

R v Nguyen, 2005 ABQB 403, 379 AR 202.

R v Nin (1985), 34 CCC (3d) 89, 1985 CarswellQue 278 (Que CSP).

R v Otchere-Badu, 2010 ONSC 1059, 87 WCB (2d) 29.

R v Pangman, 2000 MBQB 85, 147 Man R (2d) 93.

R v Panko, 52 CR (6th) 378, [2007] OJ No 3826.

R v Panko, 2010 ONCA 660, 276 OAC 49.

R v Penna, [1997] BCJ No 3014, 1997 CarswellBC 2914 (BCSC).

R v Perkins, 2013 ONSC 1807, 105 WCB (2d) 694.

R v Plant, [1993] 3 SCR 281, 84 CCC (3d) 203.

R v Polius, (2009), 196 CRR (2d) 288, 84 WCB (2d) 343.

R v Rayworth, [1999] OJ No 5289, 45 WCB (2d) 291.

R v Rogers Communications, 2016 ONSC 70, 128 OR (3d) 692.

R v SAB, 2003 SCC 60, [2003] 2 SCR 678.

R v Saeed, 2016 SCC 24, [2016] 1 SCR 518.

R v Sampson, [1983] 45 Nfld & PEIR 32 (NFCA).

R v Samson (1983), 45 Nfld & PEIR 32, 132 APR 32 (Nfld CA).

R v Smith, (unreported, December 19, 2003, BCSC 119747).

R v Sonne, 2012 ONSC 1463, 100 WCB (2d) 414.

R v Spencer, 2009 SKQB 341, 361 Sask R 1.

R v Spencer, 2011 SKCA 144, 377 Sask R 280.

R v Spencer, 2014 SCC 43, [2014] 2 SCR 212.

R v Stillman, [1997] 1 SCR 607, 144 DLR (4th) 193.

R v Talbot, 2017 ONCJ 814, 140 OR (3d) 104.

R v Talbot, 2018 CarswellOnt 5328.

R v T & T Fisheries, [2005] PEIJ No 74, 2005 CarswellPEI 71.

R v Telus Communications Co., 2013 SCC 16, [2013] 2 SCR 3.

R v Telus Communications Company, 2015 ONSC 3964, 122 WCB (2d) 281.

R v TGH, 2014 ONCA 460, 120 OR (3d) 581.

R v Tessling, 2004 SCC 67, [2004] 2 SCR 432.

R v Thompson, [1990] 2 SCR 1111, 73 DLR (4th) 596.

R v Trapp, 2009 SKPC 5, 330 Sask R 169.

R v Trapp, 2011 SKCA 143, 377 Sask R 246.

R v Tse, 2008 BCSC 906, [2008] BCJ No 1766.

R v Tse, 2012 SCC 16, [2012] 1 SCR 531.

R v Vu, 2011 BCCA 536, 285 CCC (3d) 160.

R v Vu, 2013 SCC 60, [2013] 3 SCR 657.

R v Ward, 2008 ONCJ 355, 79 WCB (2d) 129.

R v Ward, 2012 ONCA 660, 112 OR (3d) 321.

R v Watts, 2000 BCPC 191, [2000] BCJ No 2721.

R v Weir, 2001 ABCA 101, 281 AR 333.

R v Whitman-Langille, [2004] QJ No 14164.

R v Wilson, [2009] OJ No 1067, 2009 CarswellOnt 2064 (ONSC).

R v Wise, [1992] 1 SCR 527,70 CCC (3d) 193.

R v Wong, [1990] 3 SCR 36, 60 CCC (3d) 460.

Schachter v Canada, [1992] 2 SCR 679, 93 DLR (4th) 1.

Transmission Data Recorder Warrant, Re, 2015 ONSC 3072, 254 ACWS (3d) 76.

United States of America v Equinix Inc, 2013 ONSC 193, 104 WCB (2d) 848.

Young v Canada, [2010] NJ No 389, 91WCB (2d) 452.

(ii) American

AFL-CIO v Donovan, 757 F2d 330 (DC Cir 1985).

Berger v New York, 388 US 41 (1967).

California v Ciarolo, 476 US 207 (1986).

United States v Carolene Products Company, 304 US 144 (1938).

Carpenter v United States, 819 F 3d 880 (2016).

Carpenter v United States, 16 S Ct 402 (2018).

Chimel v United States, 395 US 752 (1969).

Doe v DiGenova, 642 F Supp 624 (DDC 1986) (VA records).

Florida v Riley, 488 US 445 (1989).

Groh v Ramirez, 540 US 551 (2004).

Guest v Leis, 255 F 3d 325 (6th Cir 2001).

Hudson v Michigan, 547 US 586 (2006).

Illinois v Krull, 480 US 340 (1987).

In re Kufkin, 255 BR 204 (Bankr. ED Tenn 2000).

Janus v American Federation of State, County, and Municipal Employees, Council 31 et al., 585 US 1 (2018).

Katz v United States, 389 US 347 (1967).

Kyllo v United States, 533 US 27 (2001).

Lopez v United States, 373 US 427 (1963).

Mapp v Ohio, 367 US 643 (1961).

Marvin v United States, 732 F 2d 669 (8th Cir 1984).

McKamey v Roach, 55 F 3d 1236 (6th Cir 1995).

Minnesota v Dickerson, 508 US 366 (1993).

Motor Vehicle Mfrs. Ass'n v State Farm Mut. Auto. Ins. Co., 463 US 29 (1983).

Murray v United States, 487 US 533 (1988).

Nix v Williams, 467 US 431 (1984).

Nowicki v Comm'r, 262 F 3d 1162 (11th Cir 2001).

O'Connor v Ortega, 480 US 709 (1987).

Oliver v United States, 466 US 170 (1984).

Olmstead v United States, 277 US 438 (1928).

Ontario v Quon, 560 US 746 (2010).

Planned Parenthood of Southeastern Pennsylvania v Casey, 505 US 893 (1992).

Price v Turner, 260 F 3d 1144 (9th Cir 2001).

Re Askin, 47 F3d 100 (1995).

Riley v California, 134 S Ct 2473 (2014).

Scott v United States, 436 US 128 (1978).

Smith v Maryland, 442 US 735 (1979).

State v Mubita, 188 P 3d 867 (Idaho 2008).

Stoner v California, 376 US 483 (1964).

Terry v Ohio, 392 US 1 (1968).

Tri-State Generation & Transmission Ass'n v Envtl. Quality Council, 590 P2d 1324 (Wyo 1979).

Tyler v Berodt, 877 F 2d 705 (8th Cir 1989).

United States v Baker, 221 F 3d 438 (3d Cir 2000).

United States v Biasucci, 786 F 2d 504 (2d Cir 1986).

United States v Bobo, 477 F 2d 974 (4th Cir 1973).

United States v Botelho, 360 F Supp 620 (1973).

United States v Bunnell, No CRIM.02-13-B-S, 2002 WL 981457.

United States v Caceres, 440 US 741 (1979).

United States v Cafero, 473 F 2d 489 (3d Cir 1973).

United States v Cox, 449 F 2d 679 (10th Cir 1971).

United States v *Cuevas-Perez*, 640 F 3d 272 (2011).

United States v Davis, 657 F Supp 2d 630 (D Md 2009).

United States v Davis, 690 F 3d 226 (4th Cir 2012).

United States v Dorais, 241 F 3d 1124 (9th Cir 2001).

United States v Dunn, 480 US 294 (1987).

United States v Edgar, 82 F 3d 499 (1st Cir 1996).

United States v Elliott, 676 F Supp 2d 431 (D Md 2009).

United States v Falls, 34 F 3d 674 (8th Cir 1994).

United States v Gorshkov, No CR00-550C, 2001 (WD Washington, 23 May 2001).

United States v Hambrick, 55 F Supp 2d 504 (1999).

United States v Herring, 555 US 135 (2009).

United States v Jones, 132 S Ct 945 (2012).

United States v Karo, 468 US 705 (1984).

United States v Kennedy, 81 F Supp 2d 1103 (2000).

United States v Kirschenblatt, 16 F 2d 202 (1926).

United States v Knotts, 460 US 276 (1983).

United States v Koyomejian, 970 F 2d 536 (9th Cir 1992).

United States v Lyons, 992 F 2d 1029 (10th Cir 1993).

United States v Martinez, 498 F 2d 464 (6th Cir 1974).

United States v Matlock, 415 US 164 (1974).

United States v McNulty (In re Askin), 47 F 3d 100 (4th Cir 1995).

United States v Michaelian, 803 F 2d 1042 (9th Cir 1986).

United States v Microsoft Corporation, 253 F 3d 34 (2001).

United States v Miller, 425 US 435 (1976).

United States v Nixon, 418 US 683 (1974).

United States v Orlando, 281 E3d 586 (6th Cir 2002).

United States v Payner, 447 US 727 (1980).

United States v Place, 462 US 696 (1983).

United States v Rabinowitz, 339 US (1950).

United States v Ramsey, 503 F 2d 524 (7th Cir 1974).

United States v R. Enters., Inc., 498 US 292 (1991).

United States v Ross, 456 US 798 (1982).

United States v Scarfo, 180 F Supp 2d 572 (DNJ 2001).

United States v Sholola, 124 F 3d 803 (7th Cir 1997).

United States v Sklaroff, 506 F 2d 837 (5th Cir 1975).

United States v Smith, 978 F 2d 171 (5th Cir 1992).

United States v Thomas, 613 F 2d 787 (10th Cir 1980).

United States v Torres, 751 F 2d 875 (7th Cir 1984).

United States v Tortorello, 480 F 2d 764 (2d Cir 1973).

United States v Wellons, 32 F 3d 117 (4th Cir 1994).

United States v Whitaker, 474 F 2d 1246 (3d Cir 1973).

United States v White, 401 US 745 (1971).

Utah v Strieff, 136 US 2056 (2016).

Wang v United States, 947 F2d 1400 (9th Cir 1991).

Webb v Goldstein, 117 F Supp 2d 289 (EDNY 2000).

Word v United States, 604 F 2d 1127 (8th Cir 1979).

Wyoming v Houghton, 526 US 295 (1999).

Zurcher v Stanford Daily, 436 US 547 (1978).

IV. Legislation

(i) Canadian

(A) Statutes

An Act to amend the Criminal Code, the Crown Liability and Proceedings Act and the Radiocommunication Act (Bill C-109), 1993, c 40.

Canadian Charter of Rights and Freedoms, being schedule B to the Canada Act 1982 (UK), 1982, c11.

Criminal Code of Canada, RSC 1985, c C-46.

Interpretation Act, RSC 1985, c I-21.

Personal Information Protections and Electronic Documents Act, SC 2000, c 5.

Privacy Act, RSC 1985, c P-21.

Securities Act, RSO 1990, c S.5.

Supreme Court Act, RSC 1985, c S-26.

Response to the Supreme Court of Canada Decision in R. v. Tse Act, SC 2013, c. 8.

Rules of the Supreme Court of Canada, SOR/2002-156.

(B) Bills

Bill C-2, *An Act to Amend the Criminal Code and the Make Consequential Amendments to Other Acts*, 2005, c 32, s 6.

Bill C-13, *An Act to amend the Criminal Code (capital markets fraud and evidence gathering)*, SC, 2004, c 3.

Bill C-13, *An Act to Amend the Criminal Code (criminal procedure, language of the accused, sentencing and other amendments)*, 2008, c 18.

Bill C-13, "An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act", 41st Parl, 2nd Sess, No 25 (27 November 2013).

Bill C-13, *Protecting Canadians from Online Crime Act*, SC 2014, c 31.

Bill C-15A, *An Act to Amend the Criminal Code and to Amend Other Acts*, 2002, c 13.

Bill C-27, *An Act to amend the Criminal Code (identity theft and related misconduct)*, SC, 2009, c 28.

Bill C-30, "An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts", 41st Parl, 1st Sess, 2012.

Bill C-46, "An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act", 40th Parl, 2nd Sess, 2009.

Bill C-47, "An Act regulating telecommunications facilities to support investigations", 40th Parl, 2nd Sess, 2009.

Bill C-50, "An Act to amend the Criminal Code (interception of private communications and related warrants and orders)", 40th Parl, 3rd Sess, 2010.

Bill C-51, "An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act", 40th Parl, 3rd Sess, 2010.

Bill C-52, "An Act regulating telecommunications facilities to support investigations", 40th Parl, 3rd Sess, 2010.

Bill C-59, *An Act to amend the Criminal Code (unauthorized recording of a movie)*, SC, 2007, c 28.

Bill C-74, "An Act regulating telecommunications facilities to facilitate the lawful interception of information transmitted by means of those facilities and respecting the provision of telecommunications subscriber information", 1st Sess, 38th Parl, 2005.

(C) Debates

"Bill C-15A, An Act to amend the Criminal Code and to amend other Acts", *House of Commons Debates*, 37th Parl, 1st Sess, No 137 (3 May 2001).

"Bill C-15A, An Act to Amend the Criminal Code and to Amend other Acts", *House of Commons Debates*, 37th Parl, 1st Sess, No 97 (18 October 2001).

"Bill C-46, An Act to amend the Criminal Code (capital markets fraud and evidence-gathering", *House of Commons Debates*, 37th Parl, 2nd Sess, No 129 (29 September 2003; 8 October 2003; 03 November 2003; 05 November 2003).

*"*Bill C-46, An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act", *House of Commons Debates*, 40th Parl, 2nd Sess, No 100 (26 October 2009; 27 October 2009).

"Bill C-47, An Act regulating telecommunications facilities to support investigations", *House of Commons Debates*, 40th Parl, 2nd Sess, No 101 (27 October 2009).

"Bill C-109, An Act to amend the Criminal Code, the Crown Liability and Proceedings Act and the Radiocommunication Act", *House of Commons Debates*, 34th Parl, 3rd Sess, No 13 (26 February 1993).

"Bill C-109, An Act to amend the Criminal Code, the Crown Liability and Proceedings Act and the Radiocommunication Act", *House of Commons Debates*, 34th Parl, 3rd Sess, No 14 (30 April 1993).

(ii) American

(A) Statutes

Administrative Procedure Act, 5 USC § 553(b)(3).

Cable and Communication Act, 47 USC § 551.

Cable Communications Policy Act, 47 USC § 55.

Driver's Privacy Protection Act, 18 USC § 2721(c).

Electronic Communications Privacy Act, 18 USC § 2701.

Fair Credit Reporting Act, 15 USC § 1681.

Family Education Right to Privacy Act, 20 USC § 1232g.

Federal Rules of Criminal Procedure, 28 USC §§ 2072, 2074.

Federal Wiretap Act, 18 USC § 2520.

Health Insurance Portability and Accountability Act, 29 USC §§ 1181-1183.

Pen Register and Trap and Trace Devices Act, 18 USC §§ 3121-27.

New Deal's Communications Act, 47 USC § 605.

Privacy Act, 5 USC § 552a.

Privacy Protection Act, 42 USC § 2000aa.

Right to Financial Privacy Act, 12 USC §§ 3401-3422.

Stored Communications Act, 18 USC § 2701-12.

Temporary Assistance to Needy Families Act, 2 USC § 608(a)(9).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 50 USC § 1801-62.

Video Privacy Protection Act, 18 USC § 2710.

Wiretap Act, 18 US Code §§ 2510-22 (1968).

(B) Bills

Criminal Code Revision Act of 1981, HR 1647, 97th Cong, 1st Sess 297-98 (Feb 4, 1981).

Electronic Surveillance Act of 1984, HR 6343, 98th Cong, 2d Sess 5-6 (Oct 1, 1984).

(C) Debates

HR 5285, 96th Cong, 1st Sess, in 125 Cong Rec 25955 (Sept 24, 1979) (statement of Representative Robert Drinan).

HR 933, 97th Cong, 1st Sess, in 127 Cong Rec 514, 518 (Jan 19, 1981) (statement of Representative Ted Weiss).

S 1207, 96th Cong, 1st Sess, in 125 Cong Rec 22668 (Aug 3, 1979) (statement of Senator Carl Levin).

Hearing on Privacy in Electronic Communications before the Subcommittee on Patents, Copyrights and Trademarks of the Senate Committee on the Judiciary, 98th Cong, 2d Sess 12 (1984) (statement of HW William Caming, Senior Counsel, AT&T).

Video and Library Privacy Protection Act of 1988: Joint Hearing Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. *on the Judiciary and the Subcomm. on Tech. & the Law of the S. Comm. on the Judiciary,* 100th Cong. 123-50 (1989).

1984: Civil Liberties and the National Security State, Hearings before the Sub- committee on Courts, Civil Liberties, and the Administration of Justice of the House Committee on the Judiciary, 98th Cong, 2d Sess 150 (1984) (testimony of US Magistrate Judge James Carr).

(iii) United Kingdom

Police and Criminal Evidence Act, (1984) § 67 [United Kingdom].

Police and Criminal Evidence Act 1984 (PACE) Codes of Practice, online: <https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice> [United Kingdom].

V. Other

American Bar Association, "16-402" (26 January 2018), online: <https://www.americanbar.org/groups/public_education/publications/preview_home/2017_2018_briefs/16-402/>.

Apple, "iOS Security: iOS 11", (January 2018), online: <https://www.apple.com/business/docs/iOS/Security_Guide.pdf>.

Arellano, Nestor. "Small ISPs Foresee Cost Burden in 'Lawful Access' Bills" *ITBusiness* (27 June 2011), online: <https://www.itbusiness.ca/news/small-isps-foresee-cost-burden-in-lawful-access-bills/16419>.

Bartlett, Bruce. "How Congress Used to Work: The Deep Roots of Republicans' Failure on Capitol Hill", *Politico Magazine* (4 April 2017), online: <https://www.politico.com/magazine/story/2017/04/how-congress-used-to-work-214981>.

Belsey, Bill. "Cyberbullying: A Real and Growing Threat" *ATA Magazine* (Fall 2007) 14.

Brown, Jesse. "Slacktivism Defeats Lawful Access" *Maclean's* (21 September 2011) online: <http://www.macleans.ca/society/technology/slacktivism-defeats-lawful-access/>.

Burns, Ian. "B.C. Budget Boosts Legal Aid Funding but it's still 'Woefully Underfunded,' Women's Equality Group says" *The Lawyer's Daily* (26 February 2018), online: <https://www.thelawyersdaily.ca/articles/5971/b-c-budget-boosts-legal-aid-funding-but-it-s-still-woefullyunderfunded-women-s-equality-group-says>.

Canadian Wireless Telecommunications Association, "Re: Consultation on a Licensing Framework for Mobile Broadband Services (MBS) — 700 MHz Band" *Canadian Radio-television Telecommunications Commissioner* (22 June 2012), online: <https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/DGSO-002-12-comments-CWTA-submissions.pdf/$FILE/DGSO-002-12-comments-CWTA-submissions.pdf>.

CBC News, "Harper Government Should Adopt Liberal Bill on Surveillance: MP" *CBC News* (29 March 2007), online: <http://www.cbc.ca/m/touch/canada/story/1.635923>.

CBC News, "Government Moving to Access Personal Info, Sparking Privacy Fears" *CBC News* (12 September 2007), online: <www.cbc.ca/news/technology/govern- ment-moving-to-access-personal-info-sparking-privacy-fears-1.631075>.

CBC News, "Privacy Watchdog Reiterates Lawful Access Concerns" *CBC News* (27 October 2011), online: <www.cbc.ca/news/technology/privacy-watchdog- reiterates-lawful-access-concerns-1.996304>.

Centre for Constitutional Studies, "The Reference Procedure: The Government's Ability to Ask the Court's Opinion", online: <https://ualawccsprod.srv.ualberta.ca/>.

Chan, Gerald. "What Does Telus Say About Retrospective Seizures of Private Communications?" For the Defence Magazine Vol 34:4 (28 October 2013).

Council of Europe, "Details of Treaty No 185: Convention on Cybercrime", ETS No 185 (23 November 2001), online: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

Department of Justice, "Summary of Submissions to the Lawful Access Consultation", (Ottawa: 7 January 2015), online: <http://www.justice.gc.ca/eng/cons/la-al/sum-res/faq.html>.

Department of Justice, "About the Anti-Terrorism Act" (26 July 2017), online: <http://www.justice.gc.ca/eng/cj-jp/ns-sn/act-loi.html>.

Doherty, Eamon. "The Need for a Faraday Bag" *ForensicMag* (21 February 2014) online: <https://www.forensicmag.com/article/2014/02/need-faraday-bag>.

Electronic Privacy Information Centre, "Riley v California", online: <https://epic.org/amicus/cell-phone/riley/>.

Electronic Privacy Information Centre, "United States v Jones", online: <https://epic.org/amicus/jones/>.

Forcese, Craig. “Politicized Judicial Appointments & the Absence of Checks and Balances” *Public Law Blog* (28 May 2014).

Gallagher, Sean. “Memory that Never Forgets: Non-Volatile DIMMs Hit the Market” *Arstechnica* (4 April 2013), online: <https://arstechnica.com/information-technology/2013/04/memory-that-never-forgets-non-volatile-dimms-hit-the-market/>.

Geist, Michael. “Ottawa finds public no pushover in snooping law” *The Toronto Star* (30 October 2006) EO3.

Geist, Michael. “Public Safety Canada Quietly Launches Lawful Access Consultation” *Michael Geist* (blog), (11 September 2007), online: <www.michael- geist.ca/content/view/2228/99999/>.

Goetz, David and Gérald Lafrenière, “Legislative History of Bill C-15A” (30 September 2002), online: <http://publications.gc.ca/Collection-R/LoPBdP/LS/371/371c15a-e.htm>.

Google, “Android 7.1 Compatibility Definition” (21 June 2017), online: <http://source.android.con/compatibility/7.1/android-7.1-cdd.pdf>.

Government of Canada, “Canada Completes Ratification of Convention on Cybercrime” (8 July 2015), online: <https://www.canada.ca/en/news/archive/2015/07/canada-completes-ratification-convention-cybercrime.html>.

Goodyear, Sheena. “Digital Divide: Is high-speed internet access a luxury or a right?” *CBC News* (9 February 2016).

Harris, Kathleen. “Supreme Court Chief Justice says Legal Aid ‘Essential’ to Fair Justice System” *CBC News* (20 June 2019), online: < https://www.cbc.ca/news/politics/supreme-court-chief-justice-wagner-1.5182657?fbclid=IwAR1Opazt3YIkzw2pwk3wJ-GrmZgpMSVYO2YYDzxpMbdi_cUYUfNd1MQmVo4>.

House of Commons, “Legislative Process”, Government of Canada, online: <https://www.ourcommons.ca/About/Compendium/LegislativeProcess/c_g_legislativeprocess-e.htm>.

Joseph, Patricia. “A TheCourt.ca Exclusive Interview: R v Spencer One Year Later” *TheCourt.ca* (24 September 2015), online: <http://www.thecourt.ca/a-thecourt-ca-exclusive-interview-r-v-spencer-one-year-later/>.

Kerr, Orin. “Apple’s Dangerous Game”, *The Washington Post* (19 September 2014), < https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game/>.

Kline, Jesse. “Vic Toews Draws Line on Lawful Access: You’re with Us, or the Child Pornographers” *National Post* (14 February 2012), online: <http://nationalpost.com/opinion/vic-toews-draws-line-on-lawful-access-youre-with-us-or-the-child-pornographers>.

Krugel, Lauren. “Alberta Defence Lawyers Demand Boost to Legal Aid Funding” *The Globe and Mail* (17 April 2018), online: <https://www.theglobeandmail.com/canada/alberta/article-calgary-defence-lawyers-group-demands-boost-to-legal-aid-funding/>.

Kyonka, Nicholas. “Telcos Object to Industry Department’s ‘Lawful Intercept’ Proposal for 700 MHz Band,” *Wire Report* (9 July 2012), online: <www. thewirereport.ca/news/2012/07/09/telcos-object-to-industry-department’s- ‘lawful-intercept’-proposal-for-700-mhz/25496>.

Law Reform Commission of Canada, *Electronic Surveillance*, Working Paper No 47 (Ottawa: 1986).

Liberal Party of Canada, “Don’t Let Harper Read Your Emails” (2013), online: <http://petition.liberal.ca/online-privacy-surveillance-lawful-access-bill-c30-liberal-amendment/>.

Liptak, Adam. “The Polarized Court” *New York Times* (May 10 2014).

Logan, Shawn. “Defence Lawyers Say Legal Aid ‘Neglected and Degraded’ in Alberta” *Calgary Herald* (30 April 2018), online: <http://calgaryherald.com/news/local-news/defence-lawyers-says-legal-aid-suffering-from-funding-crisis-in-alberta>.

McKenna, Barrie. “Corrupt Canada? We’re Small Time Compared to the US” *Globe and Mail* (10 October 2010).

Mercury News, “EU data protection chief warns against anti-terrorism plans”, *Mercury News* (26 September 2005).

Nicol, Julia and Dominique Valiquet, *Legislative Summary of Bill C-13: An Act to Amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act* (28 August 2014), online: <https://lop.parl.ca/Content/LOP/LegislativeSummaries/41/2/c13-e.pdf>.

Noack, Rick. “America’s Supreme Court Picks are Highly Politicized: They Don’t Have to be that Way” *Washington Post* (February 1 2017).

“Office of the Information and Privacy Commissioner of Alberta”, online: <https://www.oipc.ab.ca/>.

Office of the Privacy Commissioner of Canada, “Response to the Government of Canada's ‘Lawful Access’ Consultations” (May 2005), online: <http://www.priv.gc.ca/information/research-recherche/sub/ sub_la_050505_e.asp>.

Office of the Privacy Commissioner of Canada, "What an IP Address Can Reveal About You" (May 2013), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/>.

Office of the Privacy Commissioner of Canada, "Statement from the Privacy Commissioner of Canada regarding Bill C-13" (28 November 2013), online: <http://www.priv.gc.ca/media/nr-c/2013/s-d_131128_e.asp>.

Office of the Privacy Commissioner of Canada, "Who we are", online: <https://www.priv.gc.ca/en/about-the-opc/who-we-are/>.

Open Media, "Stop Online Spying" *OpenMedia* (2013), online: <https://openmedia.org/en/ca/look-back-our-stop-spying-campaign-against-canadas-bill-c-30>.

Pascrell, Bill. "Why is Congress so Dumb?", *Washington Post* (11 January 2019), online: <https://www.washingtonpost.com/news/posteverything/wp/2019/01/11/feature/why-is-congress-so-dumb/>.

Payton, Laura. "Internet Privacy Experts raise Concerns over Crime Bill" *CBC News* (9 August 2011), online: <http://www.cbc.ca/news/politics/internet-privacy-experts-raise-concerns-over-crime-bill-1.1090482>.

Payton, Laura. "'Tell Vic Everything Tweets' Protest Online Surveillance" *CBC News* (16 February 2012), online: <http://www.cbc.ca/news/politics/tell-vic-everything-tweets-protest-online-surveillance-1.1187721>.

Payton, Laura. "Toews Steps Back from Child Pornographers Comment," *CBC News* (16 February 2012), online: <www.cbc.ca/news/politics/ toews-steps-back-from-child-pornographers-comment-1.1127817>.

Payton, Laura. "Government Killing Online Surveillance Bill" *CBC News* (11 February 2013), online: <http://www.cbc.ca/news/politics/government-killing-online-surveillance-bill-1.1336384>.

Penney, Steven. "Fear the Fearon? Searches of Digital Devices Incident to Arrest" Webcast (6 February 2015) online: <https://ualawccsprod.srv.ualberta.ca/index.php/webcasts/811-fear-the-fearon-searches-of-digital-devices-incident-to-arrest-professor-steven-penney>.

Pinto, Lindsey. "NDP Leader Responds to StopSpying.ca Campaign" *OpenMedia* (25 May 2012), online: <https://openmedia.org/en/ndp-leader-responds-stopspyingca-campaign>.

Privacy Commissioners of Ontario, Alberta, British Columbia, "RE: Police Chiefs Speak out" *Information and Privacy Commissioner of Ontario* (7 November 2012), online: <http://www.ipc.on.ca/ english/About-Us/Whats-New/Whats-New-Summary/?id=263>.

Proussalidis, Daniel. “Magnotta to be Charged with Criminal Harassment of PM” *Winnipeg Sun* (1 June 2012), online: <http://winnipegsun.com/2012/06/01/internet-snooping-bill-would-be-helpful-in-lin-case-toews/wcm/ad158458-2a17-463f-904d-716cae0de5c6>.

Public Safety and Emergency Preparedness Canada, “Legislation to Modernize Investigative Techniques Introduced Today,” *Government of Canada* (15 November 2005).

Schiesser, Tim. “Guide to Smartphone Hardware: Memory and Storage” *Neowin* (12 March 2012), online: <https://www.neowin.net/news/guide-to-smartphone-hardware-37-memory-and-storage>.

Schmidt, Sarah and Jason Fekete. “Vic Toews will ‘Entertain Amendments’ to Online Surveillance Bill” (15 February 2012), online: <https://nationalpost.com/news/canada/protecting-children-from-internet-predators-act-vic-toews>.

Shaw, Erin and Dominique Valiquet. *Legislative Summary of Bill C-30: An Act to Enact the Investigating and Preventing Criminal Electronic Communications Act and to Amend the Criminal Code and other Acts* (15 February 2012), online: <https://lop.parl.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?ls=c30&Parl=41&Ses=1&source=library_prb&Language=E>.

Southey, Tabatha. “Bill C-13 is about a lot more than Cyberbullying” *Globe and Mail* (6 December 2013), online: <https://www.theglobeandmail.com/opinion/columnists/maybe-one-day-revenge-porn-will-be-have-no-power/article15804000/>.

Stoddart, Jennifer et al., “Letter to Public Safety Canada from Canada's Privacy Commissioners and Ombudspersons on the Current 'Lawful Access' proposals” (9 March 2011), online: <http://www.priv.gc.ca/ media/nr-c/2011/let_110309_e.asp>.

Stone, Geoffrey. “Our Politically Polarized Supreme Court?” *The Huffington Post* (November 25 2014).

Stone, Laura. “Conservatives Kill Internet Surveillance Bill C-30”, *iPOLITICS* (11 February 2013), online: <www.ipolitics.ca/2013/02/11/conservatives-kill-internet-surveillance-bill-c-30>.

Stribopoulos, James. “Peeking in Cyberspace’s Backdoor” *Toronto Star* (12 July 2009).

“Summary of Submissions to the Lawful Access Consultation” (16 April 2003), online: <http://canada.justice.gc.ca/eng/cons/la-al/sum-res/6.html>.

Svensson, Peter. “Smartphones now Outsell ‘Dumb’ Phones” *Newshub* (28 April 2013), online: <http://www.newshub.co.nz/technology/smartphones-now-outsell-dumb-phones-2013042912>.

Tweedie, Steven. “The World’s First Smartphone, Simon, was Created 15 Years before the Iphone” *Tech Insider* (14 June 2015), online: <http://www.businessinsider.com/worlds-first-smartphone-simon-launched-before-iphone-2015-6>.

United States Department of Justice, "Electronic Communications Privacy Act of 1986 (ECPA)", online: <https://www.it.ojp.gov/PrivacyLiberty/authorities/statutes/1285>.

Valiquet, Dominique. "Bill C-74: Modernization of Investigative Techniques Act: Backgrounder" (21 December 2005), online: <https://lop.parl.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?lang=F&ls=c74&Parl=38&Ses=1&source=library_prb>.

Valiquet, Dominique. "Telecommunications and Lawful Access: I. The Legislative Situation in Canada" (Canada: Library of Parliament, 2006), online: <http://www.parl.gc.ca/Content/LOP/ResearchPublications/prb0565-e.html>

Valiquet, Dominique. *Legislative Summary of Bill C-47: Technical Assistance for Law Enforcement in the 21st Century Act* (28 July 2009), online: <https://lop.parl.ca/About/Parliament/LegislativeSummaries/Bills_ls.asp?language=E&ls=c47&source=library_prb&Parl=40&Ses=2>.

Wessler, Nathan "The Supreme Court's Ground breaking Privacy Victory for the Digital Age", *ACLU* (22 June 2018), online: <https://www.aclu.org/blog/privacy-technology/ location-tracking/supreme-courts-groundbreaking-privacy-victory-digital-age>.

Wielaard, Robert. "Data Retention Bill Divides EU Countries" *SFGate.com* (8 September 2005).

Yahoo News, "U.K. sets out case for data logs to fight terror", *Yahoo News* (*Reuters*) (7 September 2005).

Appendix "A" for Chapters Two and Three

Appendix "A" may be found at the following url:

https://docs.google.com/spreadsheets/d/1oAwZ0uxkx0G7PiRsQVDpWkM_ui43KtdRcJPo64o5PTk/edit#gid=0