Contents

List of Tables and Figures / xi

Foreword / xiii

ANN CAVOUKIAN

Acknowledgments / xvii

List of Abbreviations / xix

Introduction: On the Politics of Access to Information / 1

MIKE LARSEN AND KEVIN WALBY

Part 1: Access to Information, Past and Present

1 Sustaining Secrecy: Executive Branch Resistance to Access to Information in Canada / 35

ANN REES

2 Access Regimes: Provincial Freedom of Information Law across Canada / 68

GARY DICKSON
Part 2: Behind Closed Doors – Security and Information Control

3 Flying the Secret Skies: Difficulties in Obtaining Data on Canadian Airport Security Screening Tests Following 9/11 / 97
   JIM BRONSKILL

4 Access to Information in an Age of Intelligenced Governmentality / 115
   WILLEM DE LINT AND REEM BAIDI

5 Accessing Dirty Data: Methodological Strategies for Social Problems Research / 142
   YAVAR HAMEED AND JEFFREY MONAGHAN

Part 3: Access to Information and Critical Research Strategies

6 The Freedom of Information Act as a Methodological Tool: Suing the Government for Data / 169
   MATTHEW G. YEAGER

7 “He who controls the present, controls the past”: The Canadian Security State’s Imperfect Censorship under the Access to Information Act / 194
   STEVE HEWITT

8 Beyond the Blue Line: Researching the Policing of Aboriginal Activism Using Access to Information / 209
   TIA DAFNOS

9 Accessing the State of Imprisonment in Canada: Information Barriers and Negotiation Strategies / 234
   JUSTIN PICHÉ

10 Accessing Information on Streetscape Video Surveillance in Canada / 261
    SEAN P. HIER

Part 4: Dispatches from the Fourth Estate – Access to Information and Investigative Journalism

11 Access, Administration, and Democratic Intent / 287
    FRED VALLANCE-JONES
Contents

12 Access to Information: The Frustrations – and the Hope / 314
   David McKie

13 The Quest for Electronic Data: Where Alice Meets Monty Python
   Meets Colonel Jessep / 335
   Jim Rankin

Postscript / 358
   Suzanne Legault

List of Contributors / 363

Index / 370
Tables and Figures

Tables
0.1 Canadian access to information regimes / 10
0.2 Selected international access to information laws / 14
9.1 Informal information requests, 2009 / 240
9.2 Formal information requests, 2009 / 243
9.3 Informal information requests, 2010 / 248
9.4 Scope of ongoing prison capacity expansion in Canada / 250
11.1 Extensions under the Access to Information Act, by fiscal year / 291
11.2 Number of extension complaints filed with the Information Commissioner of Canada, by agency, 2005-06 and 2008-09 / 292
11.3 Access to information requests received and fees collected by the federal government and the provinces, where available / 305
11.4 Average fees for requests for personal information and general records under the Ontario provincial and municipal acts / 306

Figures
8.1 Department of National Defence e-mail correspondence, 31 May 2007 / 225
11.1 Letter to reporter Jim Bronskill from Department of Justice Canada, 4 June 2009 / 293
11.2 Memo from Sébastien Togneri calling on ATIP manager to “unrelease” records, 27 July 2009 / 300
Foreword

ANN CAVOUKIAN

“We do not now and never will accept the proposition that the business of the public is none of the public’s business.”

These were the words of Ontario Attorney General Ian Scott when he introduced the province’s first Freedom of Information law in 1985. They are words to remember for they underline the single, trenchant argument in favour of having freedom of information (FOI) or access to information (ATI) laws, namely, that for far too long, in jurisdictions around the world, governments appear to have accepted the proposition that the business of the public is none of the public’s business.

As unacceptable as that may sound, this is not a new issue. Although the first ATI law was passed in Sweden in 1766, it was not an idea that caught on quickly. The next such law was not passed for another 187 years, this time in Finland in 1953. At that point the ball started rolling, with the United States following suit in 1966. Today some seventy-eight countries have laws supporting the public’s right to request and receive information from their governments. The fact that many of these countries, in Eastern Europe and South and Central America, have emerged from totalitarian regimes and are passing these laws as part of that emergence shows how fundamental a principle of democracy is the public’s right to know what government organizations are doing.
Here in Canada, the federal government passed the *Access to Information Act* in 1983 and since then every province and territory has introduced its own law. Since 1997, I have been the Information and Privacy Commissioner for the province of Ontario, overseeing the operation of the FOI and privacy laws introduced by Ian Scott. I believe passionately that citizens must be allowed to participate in the democratic process, and that in order to do so they must have timely access to the information held by their governments – essentially their own information.

In my time as commissioner, I have experienced enough setbacks and victories to understand that even in the fairest and most democratic societies, the road to information access makes for a long and bumpy ride. That is why this book is such a welcome addition to the literature on this subject. All of the contributors make it clear that although we have come a long way regarding access to information, we still have a long way to go.

In 1997, Supreme Court of Canada Justice Gérard La Forest spoke eloquently of the fundamental importance of access to information in a democracy in the case of *Dagg v. Canada (Minister of Finance)*:

> The overarching purpose of access to information legislation, then, is to facilitate democracy. It does so in two related ways. It helps to ensure first, that citizens have the information required to participate meaningfully in the democratic process, and secondly, that politicians and bureaucrats remain accountable to the citizenry. Parliament and the public cannot hope to call the government to account without an adequate knowledge of what is going on.

One of the frustrations for those of us in the business of upholding and promoting better access to information is the incongruence between what is stated and what is acted upon by our elected leaders. In 2004, Ontario Premier Dalton McGuinty echoed the words of Ian Scott in a memorandum to ministers and deputy ministers: “Our government should ensure that information requested of it should continue to be made public unless there is a clear and compelling reason not to do so.” As my 2008 annual report to the Ontario legislature makes clear, I applauded the Premier’s words and Ontario for achieving commendable results in providing timely responses to access requests. Ontario has also recently expanded its access laws to include publicly funded universities, announced plans to make the expense accounts of public officials available, and extended FOI to publicly funded hospitals.

Unfortunately, this commitment to the principle of access does not extend to the federal government. Despite promises to enhance government ac-
countability, the federal Justice Minister has rejected recent recommendations of the House of Commons committee on access to information, privacy, and ethics that were aimed at improving access to information. Across Canada, the default position for far too many government agencies is to withhold information if at all possible.

We need look no further than the case of Maher Arar, the details of which are well known to most Canadians. The federal government refused to make public the so-called evidence against Mr. Arar, on the grounds of “national security.” In the wake of Mr. Justice Dennis O’Connor’s commission of inquiry into the affair, we now know that the real reason had far less to do with national security than with covering up bureaucratic incompetence. When a fundamental democratic value like public access to information can be set aside by the highest levels of government in order to disguise incompetence, and freedom of information can be obstructed through false claims of national security, we all need to ask ourselves – and our governments – how this reflects upon the nature of our democracy.

When we began passing FOI laws in this country, we collectively bought into the notion that government must be open, transparent, visible, accountable, and citizen-driven. Our governments accepted that the public perception and understanding of information sharing had changed – that receiving information from government should no longer be viewed as an occasional privilege that citizens were granted but rather as a right that they had been accorded under the laws of this land, one that they had every right to exercise.

Freedom of information is really about freedom, the preservation and advancement of which should be at the heart of all that we do. It is frustrating that books such as this still need to be published and hopefully read. But the fact that they are being published and read – and I would strongly encourage all Canadians to read this one – is a good sign. The road may indeed be a long one, and it may be bumpy along the way, but with every mile travelled and every obstacle overcome, our values are secured and our democracy is strengthened. May it grow steadily and may it in turn strengthen our freedom and liberty.

LEGISLATION CITED

CASE CITED
We would like to thank our contributors for their insights, commitment, and support. It has been a privilege to work collaboratively with so many active members of Canada’s access community. We thank Jessica Ross for providing research assistance. We would also like to thank the anonymous reviewers who provided us with thorough feedback on the manuscript, as well as Randy Schmidt, Ann Macklem, and the editorial staff at UBC Press for seeing us smoothly through the review and production processes.

Royalties from *Brokering Access* have been donated to the BC Civil Liberties Association, in recognition of their sustained commitment to human rights, transparency, and government accountability.
Abbreviations

AFN  Assembly of First Nations
ART  Aboriginal Relations Team [Ontario Provincial Police]
ATI  access to information
ATIA Access to Information Act [Canada]
CADORS Civil Aviation Daily Occurrence Reporting System [Transport Canada]
CAIRS Coordination of Access to Information Requests System [Canada]
CATSA Canadian Air Transport Security Authority
CCAPS Community, Contract, and Aboriginal Policing Services [RCMP]
CCCS Coordinating Committee for Community Safety [London, Ontario]
CCTV closed-circuit television
CFIA Canadian Food Inspection Agency
CFNCIU Canadian Forces National Counter-Intelligence Unit
CIA Central Intelligence Agency [US]
CIC Citizenship and Immigration Canada
CNA Canadian Newspaper Association
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPC</td>
<td>Commission for Public Complaints Against the RCMP</td>
</tr>
<tr>
<td>CSC</td>
<td>Correctional Service of Canada</td>
</tr>
<tr>
<td>CSIS</td>
<td>Canadian Security Intelligence Service</td>
</tr>
<tr>
<td>CYFN</td>
<td>Council of Yukon First Nations</td>
</tr>
<tr>
<td>DEA</td>
<td>Drug Enforcement Administration [US]</td>
</tr>
<tr>
<td>DFO</td>
<td>Department of Fisheries and Oceans [= Fisheries and Oceans Canada]</td>
</tr>
<tr>
<td>DND</td>
<td>Department of National Defence [Canada]</td>
</tr>
<tr>
<td>ERT</td>
<td>Emergency Response Team [Ontario Provincial Police]</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation [US]</td>
</tr>
<tr>
<td>FIPPA</td>
<td>Freedom of Information and Protection of Privacy Act [Canadian provinces/territories]</td>
</tr>
<tr>
<td>FOI</td>
<td>freedom of information</td>
</tr>
<tr>
<td>FOIA</td>
<td>Freedom of Information Act [US]</td>
</tr>
<tr>
<td>IBET</td>
<td>Integrated Border Enforcement Team [RCMP]</td>
</tr>
<tr>
<td>ICT</td>
<td>information and communications technology</td>
</tr>
<tr>
<td>INAC</td>
<td>Indian and Northern Affairs Canada</td>
</tr>
<tr>
<td>INSET</td>
<td>Integrated National Security Enforcement Team [RCMP]</td>
</tr>
<tr>
<td>ITAC</td>
<td>Integrated Threat Assessment Centre [Canada]</td>
</tr>
<tr>
<td>LAC</td>
<td>Library and Archives Canada</td>
</tr>
<tr>
<td>LPS</td>
<td>London Police Service</td>
</tr>
<tr>
<td>LVMAC</td>
<td>Lions Video Monitoring Advisory Committee [Sudbury, Ontario]</td>
</tr>
<tr>
<td>MAF</td>
<td>Management Accountability Framework [Canada]</td>
</tr>
<tr>
<td>MCSCS</td>
<td>Ministry of Community Safety and Correctional Services [Ontario]</td>
</tr>
<tr>
<td>MFIPPA</td>
<td>Municipal Freedom of Information and Protection of Privacy Act [Ontario]</td>
</tr>
<tr>
<td>MLA</td>
<td>Member of the Legislative Assembly</td>
</tr>
<tr>
<td>NADDIS</td>
<td>Narcotics and Dangerous Drugs Information System [US Drug Enforcement Administration]</td>
</tr>
<tr>
<td>NGO</td>
<td>non-governmental organization</td>
</tr>
<tr>
<td>NSCI</td>
<td>National Security Criminal Investigations [RCMP]</td>
</tr>
<tr>
<td>NSG</td>
<td>National Security Group [Department of Justice Canada]</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Name</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>OIC</td>
<td>Office of the Information Commissioner of Canada</td>
</tr>
<tr>
<td>OIPC</td>
<td>Office of the Information and Privacy Commissioner [Ontario]</td>
</tr>
<tr>
<td>OMS</td>
<td>Offender Management System [Correctional Service of Canada]</td>
</tr>
<tr>
<td>OPC</td>
<td>Office of the Privacy Commissioner of Canada</td>
</tr>
<tr>
<td>OPI</td>
<td>Office of primary interest</td>
</tr>
<tr>
<td>OPP</td>
<td>Ontario Provincial Police</td>
</tr>
<tr>
<td>PCO</td>
<td>Privy Council Office</td>
</tr>
<tr>
<td>PERT</td>
<td>Provincial Emergency Response Team [Ontario]</td>
</tr>
<tr>
<td>PMO</td>
<td>Prime Minister’s Office</td>
</tr>
<tr>
<td>PSC</td>
<td>Public Safety Canada</td>
</tr>
<tr>
<td>SIRC</td>
<td>Security Intelligence Review Committee [Canada]</td>
</tr>
<tr>
<td>TRU</td>
<td>Tactics and Rescue Unit [Ontario Provincial Police]</td>
</tr>
<tr>
<td>VMAC</td>
<td>Video Monitoring Advisory Committee [Sudbury, Ontario]</td>
</tr>
</tbody>
</table>
BROKERING ACCESS
Introduction
On the Politics of Access to Information

MIKE LARSEN AND KEVIN WALBY

This book focuses on the workings of access to information (ATI) regimes in Canada. It explores the laws and practices that provide members of the public with the means to exercise a “right to know” about the work of government agencies. It also investigates the ways these same laws and practices act to maintain and legitimize secrecy, and the ways in which they are subverted and circumvented in the interests of information control. A key argument that appears throughout this volume is that access regimes emerge as sites of contestation situated between the public pursuit of transparency and the culture of secrecy in government. The various chapters engage with the politics of access at the level of policy and at the level of practice, where interactions between requesters and professional access brokers take place, negotiations ensue, and techniques of opacity are used.

Every citizen and permanent resident in Canada has the right to request information from federal, provincial, and municipal government agencies. At the federal level, under the Access to Information Act (ATIA), this involves submitting a written request and a cheque for $5 to the access to information office at the agency in question. The ATIA came into force in 1983; the provinces and territories have adopted their own legislation, in the form of combined freedom of information (FOI) and privacy protection laws. There are municipal equivalents too. Most government agencies are listed as entities subject to the federal ATIA or to FOI acts at provincial and municipal levels.¹
*Brokering Access* presents essays written by sociologists, journalists, and ATI advocates and professionals. Its purpose is to assess conceptual, political, and practical issues regarding the role played by ATI in government today, and how ATI can become part of a critical methodological strategy. Exploring the relationship between information, governance, secrecy, and security, the following chapters examine how ATI requests are crafted, how the request process is negotiated, how government employees bury the textual traces of their work, and how ATI results become part of media reporting. We hope that this volume facilitates dialogue between the researchers, investigative journalists, administrators, and policy makers who are presently shaping the Canadian ATI community.

Our thoughts on ATI/FOI developed through our use of ATI in research on policing and national security in Canada (Larsen and Piché 2009; Piché and Walby 2010; Walby 2009; Walby and Larsen 2012; Walby and Monaghan 2010; Walby and Monaghan 2011). It struck us that the broader conceptual issues concerning ATI in Canada had yet to receive their due in sociology and political science. Most social scientists in Canada view ATI as something journalists use to break a big story rather than as a tool that can be utilized to produce qualitative and longitudinal data about government practices (Walby and Larsen 2012). Why, we wondered, are scholars with research interests similar to ours reluctant to use ATI? How can social scientists rethink research methods by incorporating ATI as a tool?

Several books have focused on government secrecy (see Bok 1989; Demac 1984; Helms 2003; Theoharis 1998), although few explore the relationship between secrecy and ATI in Canada; those that do focus on the federal level, overlooking provincial and municipal frameworks. The most thorough examination of ATI is *Blacked Out* (2006), by Alasdair Roberts. Roberts’s research examines the role that political interference and bureaucratic resistance have played in delaying sensitive requests filed by journalists or political parties. Similar “information policing” operates at provincial levels (see Roberts 1999, 2002a, 2002b, 2004). Other than the work of Roberts, however, there is little literature on ATI processes in Canada. Recent contributions (such as Kinsman and Gentile 2010) are beginning to address the gap, but more conceptual work is needed. *Brokering Access* supplements Roberts’s path-breaking analysis in four ways. First, we emphasize a two-pronged approach to ATI requests, using them systematically to seek out substantive information about the “backstage” of government practices while simultaneously studying ATI processes themselves as sites of information gatekeeping. Second, we include a consideration of provincial- and
municipal-level ATI requests (see Chapters 2, 8, 9, and 10). Third, we include voices from numerous communities that have a stake in ATI, such as information advocates, ATI professionals, and investigative journalists. Fourth, we focus on policing, security, and war, as these areas are characterized by contestations over secrecy.

The chapters of *Brokering Access* are critical in tone, reflecting the frustrations of experienced researchers and transparency advocates who work within a Canadian ATI regime that is widely recognized as being outmoded, out of step with international trends, and subject to systemic delays (see Beeby 2011; Chase 2011; Hazel and Worthy 2010; Tromp 2008). This tone reflects a working personality characterized by a determination to work both within and against a flawed system. One thread connecting the chapters is a belief in ATI as a means of producing information of public interest. The corollary to this position is an implicit normative commitment to transparency in government as a public good (see Loader and Walker 2007). That the potential of ATI to facilitate transparency is often unrealized or deliberately inhibited is cause for concern, and this is an issue that the contributors to this volume take up in the form of critical accounts of opacity in government. Several contributors also remark on the need for comprehensive law reform. The 2011 Federal Court of Appeal decision that the Harper Conservatives have too often severed information in ways that contravene the *ATIA* was a progressive step. Our sense, however, is that broad law reform will come to fruition only as the result of agitation by an organized social movement. Certainly there are numerous committed and very active ATI and transparency advocates across the country; the question is how they can work together, and what key issues to focus on in mobilizing for an overhauled access regime in Canada.

One note on terminology is required before moving ahead. Although we use “ATI” to refer to requests at the federal level and “FOI” to refer to requests at the provincial and municipal levels, we insist on the phrase “access to information” over “freedom of information” to define the general process. Ideas of accountability, transparency, openness, and freedom can distract from understanding the complicated process of using ATI. “Freedom of information” is a prescriptive term reflecting the aspirations of the right-to-know movement, which calls for proactive disclosure of the vast majority of public sector information, with minimal interference in the form of redaction, delay, and exemption. By contrast, “access to information” more accurately describes the mediated processes that characterize the administration of the right to know in practice. Bok (1989) dismisses
the notion of a “right to know” itself as quixotic, since it glosses the intermediary actors and stages involved in the release, transmission, and acquisition of information, and risks implying a duty to inform that does not exist. The public, she argues, does not have a right to information, “but at best to access to information; and not to all information, but only to some” (258). ATI processes have numerous built-in governance mechanisms, from the design of software to the response tactics of ATI coordinators, in addition to the limitations associated with current ATI laws. Some of the factors shaping ATI are tangible and visible – published guidelines and the precedents set by court decisions in cases of contested access, for example – while others, as Thomas (2010a, 15) notes, are submerged in “the overlapping political and administrative cultures of government.” What we have is a legal regime that allows for mediated record retrieval, which we refer to as brokered access. Access laws simultaneously facilitate transparency and circumscribe its limits.

The Live Archive and the Spectrum of Disclosure
Information plays a key role in all governance processes and government agencies. Numerous social scientists have pointed to how governments rely on information about people, places, and resources (see Dandeker 1990; Foucault 1980; Giddens 1985; Higgs 2001; Maynard 2009). In Canada, when scholars write about government, they often refer to federal, provincial, and municipal agencies charged with providing essential services in various jurisdictions. Government and the “state” are often conflated, and it is difficult not to invoke the notion of the “state” despite its shortcomings as a concept. For all the effort put into trying to define the “state” (compare Miliband 1973 with Poulantzas 1972, or Curtis 1995 with Rose and Miller 1992), social scientists still do not fully understand the work of political administration, for reasons we will elaborate on.

Abrams (1988) paints a picture of naïve sociologists who try to scrutinize the “state” but mistakenly study a preconceived idea of it because they have no data about what government agencies do. The suggestion here is that the state “is a spurious object of sociological concern” (63). There is no “state” as such; a quick scroll down the list of departments to which one can submit an ATI request at the federal level alone suggests that we are dealing with a multitude of networked government agencies, each with specific missions, which also have a degree of autonomy from one another. Social scientists cannot say that they study state formation or government if they do not
develop an empirical understanding of what happens from day to day in government agencies. It is the manifold knowledge practices of government agencies that we must learn about in order to conduct a sociology of political administration.

Theorizing the state in general obscures otherwise knowable internal and external relations of political and governmental agencies. Where we part from Abrams (1988) is his suggestion that to escape from reification of the state we must resist what Elias (1987) has called the “retreat of sociologists into the present.” It is not only historical documents that allow the internal and external relations of governmental agencies to become knowable. There is what we call the live archive (Walby and Larsen 2011), mounds of text detailing how governments do what they do, added to every day by civil servants, which we get at using ATI. Records pertaining to government policy and practices are created, stored, modified, and circulated – intra- and inter-institutionally, transnationally, and between sectors. Increasingly, this “deepening pool of information” (Roberts 2006, 218) is given structure through Electronic Document and Records Management Systems, a process that produces a new layer of organizational metadata (see Thomas 2010b). The networks between government agencies, the connections between different branches of the same government agencies, and the governance of citizens by these agencies are all enacted by texts. It is this textual trail we must investigate. The live archive is a dynamic system; it changes as researchers engage with it, so part of the ATI research process is to chronicle these changes in how ATI coordinators and other civil servants work with texts. The systematic use of ATI as a means of data production should involve critical reflections on the politics and practices of information brokering.

Information is always situated in a political context. The ability to access information and the power to control access to it depend in many ways on one’s position in organizational hierarchies. The kind of information we discuss in this book is textual. Texts are the means by which government bureaucracies organize and communicate (Smith 1999). The idea of an information society (see Bell 1974; Webster 1995) also signals the importance of texts to understanding contemporary governance. Other commentators (e.g., Castells 1996; Poster 1990) have theorized the trend towards network governance and the pivotal role of information in government agencies today. Although governments have always relied on information about their citizenry, the role of information has shifted with the rise of so-called
e-government. E-government is about supplying information (see Gil-Garcia, Chun, and Janssen 2009) as well as the careful management of disclosures. Information management requires new infrastructures of hardware and software. The move towards information management in government means that we should conceptualize “information as the primary input to, and product of, government activity” (Gil-Garcia, Chun, and Janssen 2009, 3). Information management also influences how governments interact with citizens. Workers are now expected to have information and communications technology (ICT) skills and also to manage more “sensitive” information, which requires an understanding of formal policy and a familiarity with the informal, unwritten “rules of the game” for handling and disclosing information” (Thomas 2010b, 16).

Access to information confers a legal right to seek access to materials not already a matter of the public record. Yet the creation of formal information retention and disclosure mechanisms does not mandate government officials to be more accountable or transparent per se. The concept of accountability itself is the subject of considerable debate. Whitaker and Farson (2009, 4) suggest that a heuristic understanding of accountability is that “A is accountable to B when A is obliged to inform B about A’s actions (or inactions) and decisions, to justify them as appropriate and proper and, in the case of misconduct, to suffer sanction.” They are quick to note that this straightforward understanding belies the complexity of the concept; it makes more sense to speak of multiple and overlapping accountabilities that differ in their focus, intensity, and effects. Whitaker and Farson (2009, 6) also note that “processes of accountability might seem to imply a relationship of power or influence over those held to account [but] accountability importantly offers legitimacy to those persons or organizations held accountable.”

From an accountability standpoint, the significance of the information that is disclosed is often, though not necessarily, tied to the means of disclosure. We find it useful to imagine a spectrum of means of disclosure. A mechanism’s location on this spectrum is dependent upon the degree of control over the scope and timing of disclosure it affords to government officials. At the end of the spectrum characterized by maximum information control, we find coordinated and voluntary releases of official information. The opposite end of the spectrum, characterized by minimum official control over disclosure, is occupied by whistleblower exposés featuring the revelation of “dirty data” (see Marx 1984) and the mass publication of involuntarily leaked records. ATI mechanisms are located near the middle of
the spectrum, in a zone defined by *rules*. They facilitate an uneven form of accountability, but also facilitate secrecy through exemption and provide a source of rhetorical legitimacy for governments.

By contrast, the work of the whistleblowing agency WikiLeaks is characterized by the transgression of rules governing information control and disclosure. Although information leaks are not the subject of this book, the broad impact of the WikiLeaks phenomenon is worth considering. As Slavoj Žižek notes, WikiLeaks represents a radical departure both from regulated disclosure processes and from what he characterizes as traditional investigative journalism, which remains tied to the logic of the bourgeois press: “Its [the bourgeois press’s] ideology not only controls what you say, but even how you can violate what you are allowed to say. You [WikiLeaks founder and editor Julian Assange] are not just violating the rules. You are changing the very rules [governing] how we were allowed to violate the rules. This may be the most important thing you can do” (Democracy Now! 2011).

*New York Times* editor-in-chief Bill Keller (2011, 3), whose newspaper was eager to capitalize on WikiLeaks’s work, describes the organization as “a secretive cadre of anti-secrecy vigilantes.” Keller (2011, 4) also notes that “by the end of the year, the story of this wholesale security breach had outgrown the story of the actual contents of the secret documents, and had generated much breathless speculation that something – journalism, diplomacy, life as we knew it – had profoundly changed forever.” Precisely by transgressing them, the WikiLeaks disclosures revealed the scope of the rules governing the political management of information by governments. Keller’s use of “wholesale security breach” to describe the disclosures is illustrative of the extent to which information control has become a central component of contemporary security politics (tellingly, US Vice President Joseph Biden described Assange as a “high tech terrorist”).

This book is concerned with the same regimes of secrecy and politics of information control exposed by WikiLeaks, but our focus here is on everyday practices of transparency and opacity and the nature of the rules governing access.

**A Short History of the Debate over ATI in Canada**

Now that we have set the conceptual scene, we can get to the details of ATI. Canada has long operated with the British Westminster system of government, which offers little opportunity for citizens to learn about what officials are up to. Throughout most of the twentieth century in Canada, even if a person was allowed standing to view documents under the *Official Secrets
Act, the “government [could] always assert its Crown privilege to deny access” (Rankin 1977, 12). Most courts would without question abide by a ministerial decision to veto information release. Thomas (1973, 160) suggested that Canada’s “bureaucracy is sheltered from parliamentary control and supervision by the doctrines of Cabinet and Ministerial responsibility.” Bazillion (1983, 382) likewise argued that “administrative secrecy is endemic in the Canadian political system, for reasons that are largely historical.” One reason for secrecy is that ministers bear sole responsibility for department operations. Ministerial control in Canada has been reinforced by current Prime Minister Stephen Harper, who has intervened to prevent ministerial assistants from communicating with the media.

Whereas the United States enacted freedom of information legislation in 1966, there were delays in implementing ATI in Canada (see Table 0.1). A private member’s bill recommending ATI was introduced in 1965. Conservative MP Gerald Baldwin introduced similar bills every year between 1969 and 1974. The October Crisis of 1970, with its allegations and revelations of police misconduct, was another step towards access. In June 1977, the Liberal government issued a Green Paper titled Legislation on Public Access to Government Documents. The Green Paper starts with the metaphor of a football huddle. These football players make a decision about an action to pursue in private, it is argued, because not to do so destroys the team’s ability to enact the plan. This is the justification for barring access to cabinet confidences. “The Green paper frequently takes refuge in the convention of ministerial responsibility,” argues Rankin (1977, 136).

A few years later, the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police was struck, headed by Justice D.C. McDonald. The commission published two reports (Security and Information in 1979 and Freedom and Security under the Law in 1981) arguing that the Official Secrets Act needed to be curtailed and used only in espionage cases. Then Joe Clark’s Conservative government introduced draft ATI legislation as Bill C-15 in October 1979. Trudeau’s Liberals replaced the Conservatives in February 1980, however, and in July of that year the Liberals introduced Bill C-43. The bills were similar. The two-tier system of appealing to an information commissioner and then Federal Court was introduced by Bill C-15 and is still part of the Access to Information Act today. Bill C-43 also introduced stringent exemptions concerning third-party information. Mandatory exemptions for cabinet documents were introduced at the final hour. One argument against ATI by numerous government officials was “maintenance of cabinet solidarity” (Bazillion 1980, 151). A second argument
was that “the anonymity of public servants in a parliamentary system must be protected so that they may advise their ministers fully, frankly, and in confidence without involving themselves in the political process” (151). Riley (1977, 13) argued that ATI had “become a bit of a merry-go-round in Parliament.”

Academics commented on these developments even before the law was passed. There was debate between Donald Rowat and K.W. Knight in the Canadian Journal of Economics and Political Science. An advocate of ATI, Rowat (1965, 480) questioned the information practices of Canada’s federal government. He argued that Canada should adopt the publicity rule since it lets the “public have a chance to criticize and discuss proposals before decisions are made” (492). Knight (1966) responded that there would be practical limits to conferring a right to request information, arguing that “the civil servant may feel, too, that he [sic] must avoid placing on record anything which is likely to offend or cut across the interests of any individual or group in the community” (78). “Many officials, faced with open access, would seek to avoid completely the risks arising from the putting of pen to paper,” he argued (79). Sadly, many of Knight’s predictions have come true. Many in public administration see ATI as an unwelcome imposition on government. For example, Donald Savoie (2003, 213), a proponent of the “traditional bargain” between anonymous career public servants operating in secret and providing advice to politically accountable ministers, has argued that ATI legislation contributes to a risk-averse culture in government, and that it “inhibits public servants from committing frank advice to paper for fear of embarrassing their ministers or compromising their political neutrality.”

Access to information is a fairly new animal in some liberal democratic nation-states (see Table 0.2). It was only in 2000 that Britain moved towards a statutory right of access to official records. Numerous other countries have adopted ATI as a so-called accountability measure. For instance, Arko-Cobbah (2008) assesses some of the limits of access to information in post-apartheid South Africa. South Africa’s Promotion of Access to Information Act from 2000 has been called one of the most progressive pieces of ATI legislation in the world. Yet there have been challenges in declassifying documents from the apartheid era, and reports of non-compliance. Where ATI laws have been implemented, differences arise concerning rules for re-daction, the definition of personal information (which is also addressed in privacy law), third-party status, statutory compliance timelines, and the rate of charging schemes (Birkinshaw 1999). Access to information takes on a
<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Title of access law(s)</th>
<th>Year of adoption</th>
<th>Cost per request (initial)</th>
<th>Access commissioner</th>
<th>Commissioner has order-making power?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada (federal)</td>
<td>• Access to Information Act (ATIA)</td>
<td>1983</td>
<td>$5 for request</td>
<td>Information Commissioner of Canada</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• Privacy Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Newfoundland and Labrador</td>
<td>Access to Information and Protection of Privacy Act (ATIPPA)</td>
<td>Freedom of Information Act of 1981 replaced by ATIPPA, 2005</td>
<td>$5 for request + 2 hours search time, $15 per hour after; $0.25 per page for copies; “actual cost” for other formats</td>
<td>Information and Privacy Commissioner of Newfoundland and Labrador</td>
<td>No</td>
</tr>
<tr>
<td>Prince Edward Island</td>
<td>Freedom of Information and Protection of Privacy Act (FOIPPA)</td>
<td>2002</td>
<td>Free for personal information, copy fees apply; $5 for public records + $10 per half-hour search time and computer time + copy and associated costs</td>
<td>Information and Privacy Commissioner of Prince Edward Island</td>
<td>Yes</td>
</tr>
<tr>
<td>New Brunswick</td>
<td>Right to Information and Protection of Privacy Act</td>
<td>Right to Information Act, 1978 repealed and replaced in 2010</td>
<td>$5 for request + 2 hours search time, $15 per half-hour after; $0.25 per page for copies</td>
<td>Access to Information and Privacy Commissioner of New Brunswick</td>
<td>No</td>
</tr>
<tr>
<td>Province</td>
<td>Act</td>
<td>Act History</td>
<td>Request and Copy Fees</td>
<td>Appeal Officer</td>
<td>Access Required</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Nova Scotia</td>
<td>• Freedom of Information and Protection of Privacy Act (FOIPOP)</td>
<td>1977 replaced by FOIPOP in 1994</td>
<td>$5 for request; $15 per hour may be charged for compiling; $0.20 per page for copies + various format fees</td>
<td>Review Officer</td>
<td>No</td>
</tr>
<tr>
<td>Québec</td>
<td>An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information</td>
<td>1982</td>
<td>Free request; copy fees only</td>
<td>Commission d'accès à l'information (5 commissioners and 1 chair)</td>
<td>Yes</td>
</tr>
<tr>
<td>Ontario</td>
<td>• Freedom of Information and Protection of Privacy Act (FIPPA)</td>
<td>1987</td>
<td>$5 for request, personal or otherwise; copy and additional search time fees apply</td>
<td>Information and Privacy Commissioner of Ontario</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>• Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manitoba</td>
<td>• Freedom of Information and Protection of Privacy Act (FIPPA)</td>
<td>1997</td>
<td>Free for FIPPA application + 2 hours search time, $15 per hour after; copy fees apply</td>
<td>Access and Privacy Division of Manitoba Ombudsman</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• Personal Health Information Act (PHIA)</td>
<td></td>
<td></td>
<td>Information and Privacy Adjudicator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Municipal Government Act</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>Title of access law(s)</td>
<td>Year of adoption</td>
<td>Cost per request (initial)</td>
<td>Access commissioner</td>
<td>Commissioner has order-making power?</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>------------------</td>
<td>--------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Saskatchewan</td>
<td>• <em>Freedom of Information and Protection of Privacy Act</em> (FOIP)</td>
<td>1992</td>
<td>Free for personal information but copy fees may apply; first 2 hours free, $15 per hour after</td>
<td>Information and Privacy Commissioner of Saskatchewan</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• <em>Local Authority Freedom of Information and Protection of Privacy Act</em> (LAFOIP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alberta</td>
<td>• <em>Freedom of Information and Protection of Privacy Act</em> (FOIP)</td>
<td>1995</td>
<td>$25 for request</td>
<td>Information and Privacy Commissioner of Alberta</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>• <em>Health Information Act</em> (HIA)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>British Columbia</td>
<td><em>Freedom of Information and Protection of Privacy Act</em> (FIPPA)</td>
<td>1993</td>
<td>Free for personal information and search time up to 3 hours, $30 per hour after; copy fees apply</td>
<td>Information and Privacy Commissioner for British Columbia</td>
<td>Yes</td>
</tr>
<tr>
<td>Territory</td>
<td>Access to Information and Privacy Protection Act (ATIPP) (an amended form of the NWT act)</td>
<td>Year</td>
<td>Fee Structure</td>
<td>Access to Information and Privacy Commissioner of</td>
<td>No</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
<td>----</td>
</tr>
<tr>
<td>Nunavut</td>
<td>NWT ATIPP adopted under the Nunavut Act 1999, pending new legislation</td>
<td></td>
<td>Free for personal information, with possible copy fees; $25 fee per request for public records</td>
<td>Commissioner of Nunavut</td>
<td></td>
</tr>
<tr>
<td>Northwest Territories</td>
<td>Access to Information and Protection of Privacy Act (ATIPP)</td>
<td>1996</td>
<td>Free for personal information; $25 for other</td>
<td>Information and Privacy Commissioner of the Northwest Territories</td>
<td></td>
</tr>
<tr>
<td>Yukon</td>
<td>Access to Information and Protection of Privacy Act (ATIPP)</td>
<td>1984</td>
<td>Free request; retrieval and processing fees $25 per hour + copying expenses over $10</td>
<td>Information and Privacy Commissioner of the Yukon</td>
<td></td>
</tr>
</tbody>
</table>
### TABLE 0.2

**Selected international access to information laws**

<table>
<thead>
<tr>
<th>Country</th>
<th>Title of access law</th>
<th>Year adopted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sweden</td>
<td>Freedom of the Press Act</td>
<td>1766/1945/1976c</td>
</tr>
<tr>
<td>United States</td>
<td>Freedom of Information Act</td>
<td>1966</td>
</tr>
<tr>
<td>France</td>
<td>Law on Access to Administrative Documents</td>
<td>1978</td>
</tr>
<tr>
<td>Australia</td>
<td>Freedom of Information Act</td>
<td>1982</td>
</tr>
<tr>
<td>New Zealand</td>
<td>Official Information Act</td>
<td>1982</td>
</tr>
<tr>
<td>Philippines</td>
<td>Code of Conduct and Ethical Standards for Public Employees</td>
<td>1987</td>
</tr>
<tr>
<td>Spain</td>
<td>Law on Rules for Public Administration</td>
<td>1992</td>
</tr>
<tr>
<td>Ukraine</td>
<td>Law on Information</td>
<td>1992</td>
</tr>
<tr>
<td>Ireland</td>
<td>Freedom of Information Act</td>
<td>1997</td>
</tr>
<tr>
<td>Thailand</td>
<td>Official Information Act</td>
<td>1997</td>
</tr>
<tr>
<td>Israel</td>
<td>Freedom of Information Law</td>
<td>1998</td>
</tr>
<tr>
<td>South Africa</td>
<td>Promotion of Access to Information Act</td>
<td>2000</td>
</tr>
<tr>
<td>Pakistan</td>
<td>Freedom of Information Ordinance 2002</td>
<td>2002</td>
</tr>
<tr>
<td>Zimbabwe</td>
<td>Access to Information and Privacy Protection Act (AIPPA)</td>
<td>2002</td>
</tr>
<tr>
<td>Angola</td>
<td>Law on Access to Administrative Documents</td>
<td>2002</td>
</tr>
<tr>
<td>Croatia</td>
<td>Act on the Right of Access to Information</td>
<td>2003</td>
</tr>
<tr>
<td>Turkey</td>
<td>Law on Right to Information</td>
<td>2003</td>
</tr>
<tr>
<td>India</td>
<td>Right to Information Act</td>
<td>2005</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Freedom of Information Act</td>
<td>2005</td>
</tr>
<tr>
<td>China</td>
<td>People’s Republic of China Ordinance on Openness of Government Information (OGI Regulations)</td>
<td>2008</td>
</tr>
<tr>
<td>Chile</td>
<td>Law on Access to Public Information</td>
<td>2008</td>
</tr>
<tr>
<td>Russia</td>
<td>Law on Providing Access to Information on the Activities of State Bodies and the Bodies of Local Self Government</td>
<td>2009</td>
</tr>
</tbody>
</table>
different tenor in each country. Byrne (2003), for instance, discusses how the focus on “transparency” in the former Soviet bloc means something different than in western nation-states due to vestiges of the communist apparatus.

The events of 11 September 2001 led to substantial changes for ATI in Canada and the United States. As Relyea (2009, 315) argues, “these events prompted rethinking, as well as continuing concern, about ... the public availability of information [deemed to be] of potential value to terrorists for either the commission of their acts or forewarning them of ways of their being detected.” The Federal Advisory Committee Act (FACA) and the Critical Infrastructure Information Act (CIIA) were passed as part of the Homeland Security Act of 2002; both led to greater secrecy. The CIIA prohibits the disclosure of “critical infrastructure information” by the Department of Homeland Security (Shapiro and Steinzor 2006, 124). Numerous groups filed ATI requests after 9/11 only to see these denied unjustifiably. The Coalition of Journalists for Open Government were vocally defiant (Kirtley 2006).

All this raises questions about whether Canada is modelling itself after the US in the post-9/11 quest for continental security. Anti-terrorism has a digital infrastructure – it depends on up-to-the-second intelligence accessible in numerous sites (Roy 2005). This requires “interoperability,” or the ability to share information across space and time. Post-9/11, Canada was accused by Homeland Security directors of having an outdated digital

<table>
<thead>
<tr>
<th>Country</th>
<th>Title of access law</th>
<th>Year adopted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Liberia</td>
<td>Freedom of Information Act</td>
<td>2010</td>
</tr>
<tr>
<td>Nigeria</td>
<td>Freedom of Information Bill</td>
<td>2011</td>
</tr>
</tbody>
</table>

Notes: Access provisions can take a variety of forms: stand-alone legislation, administrative regulations, and/or jurisprudence and constitutional rights. The following are some examples.

a These countries have constitutional provisions for access to information or high court rulings that a right to information is necessary to the interpretation of certain constitutional rights.

b While China’s OGI Regulations, the Philippine Code of Conduct and Ethical Standards for Public Employees, and the Pakistani Freedom of Information Ordinance 2002 are not acts, they do provide some legal basis for rights to information.

c Sweden’s Freedom of the Press Act (1766) is the world’s first freedom of information act. The dates indicate the enactment and two major amendments.
infrastructure. It responded by creating Public Safety and Emergency Preparedness Canada (now Public Safety Canada) soon after. Reflecting on the post-9/11 context, Pozen (2010, 266) offers a theory of government secrecy, with secrets being organized “on a continuum running from maximally opaque to maximally intelligible.” The “depth” of a given secret is determined by the number of people within government who know the secret, the types of actors who are in the know, and the extent of the secret known by each of these actors (see Hinson 2010). Deep secrets are the province of a small group of authorized knowers, and they correspond to the Rumsfeldian concept of “unknown unknowns” – things that we don’t know that we don’t know. Shallow secrets, by contrast, are those things that we know that we don’t know. A given secret can be simultaneously shallow and deep, relative to different audiences, and its depth can change over time, given the expansion of the network of actors “in the know” and the proliferation of the textual trail.

Much of the information in the live archive is clustered at the shallow end of the spectrum. Other information is classified as secret, and subject to official efforts to increase control over its dissemination (see Chapter 4). The circulation of secret information within and between networks increases the likelihood that it will become more knowable to others. Relatively shallow and accessible records often reference other documents, such that sustained research using ATI can reduce the depth of secret practices. Yet the flow of information between agencies can be an impediment to formal ATI processes, as multiple stakeholders are often consulted prior to the release of records, creating delays and backlogs (see Walby and Larsen 2011).

There are barriers that accompany access law. In Canada, successive Information Commissioners have reported on systemic issues facing the federal access regime (on access regimes, see Chapter 2). Access loopholes caused by broad exemption clauses in ATI laws, quasi exemptions (see Chapter 11) such as chronic delays, and prohibitive fee estimates are efforts to keep decisions “off the record” and disconnected from the live archive. Each chapter in this book engages with the limitations of ATI. While we support the notion that ATI can facilitate democratic accountability, we conceptualize ATI as a field of contestation, a site for struggles over what can be known about government actions.

Our position as users of access law and as proponents of increased government transparency is that the federal access regime is in need of major law reform. The problem facing the Canadian access regime is not a lack of well-researched, principled solutions to current dilemmas or detailed plans
for ATI modernization. Instead, the problem exists at the level of implementation. Successive governing parties have capitalized on the rhetoric of transparency while presiding over a dysfunctional ATI regime and refusing to undertake comprehensive reform efforts. The dysfunctionalities of the current ATI framework are by no means reducible to problems with the law; as we discuss below, “techniques of opacity” are tied to political and administrative cultures. Nonetheless, the federal access law anchors the access regime and defines its scope and limitations. It is hard to imagine a meaningful solution to problems such as chronic delays and denials without a new act. There is no shortage of ideas for law reform, including mandatory periodic review of the legislation; the granting of order-making powers to the Information Commissioner; radical limitations on cabinet confidence exemptions; limitations on exemptions, extensions, and consultation-related delays; clearer guidelines for the delegation of authority for ATI decisions; and commitments to principles of open government. Translating these ideas into a legislative mandate will require an organized social movement that can effectively connect moments of secrecy and opacity to the (dys) functioning of the ATI regime.

Bureaucracy and Information Brokers
ATI can provide social scientists with a more nuanced understanding of how government agencies do what they do. Yet access is contingent on the intensity of “information management” in any government agency, the political contentiousness of the request, the limits of the Canadian ATI law and oversight mechanisms, and the complexities of requester-agency interactions and request wording. Thus, ATI is a source of both opportunity and constraint for the researcher (Gentile 2009). We use the term “access brokering” to describe the range of interactions involved in the filing and processing of ATI requests. Access brokering is an interactive, mediated process. Several factors are key. The effective framing of initial requests, such that the language used fits closely with the specialized jargon of government agencies, is crucial. Understanding this process and the actors, interests, and technologies involved is not simply a means to the end of gaining information. “Brokering” itself is an important subject of inquiry (Walby and Larsen 2012).

Users of ATI mechanisms often interact with ATI analysts many times over the life cycle of a request; these encounters can involve the negotiation of request wording and scope, discussions about time extensions and delays, and contestation over the accessibility of records. Inexperienced requesters
can find themselves talked into making concessions that drastically alter the outcome/disclosure. Questions such as “Can we interpret this part of your request to mean xyz?” or “Can I ask why you are looking for this information?” can help coordinators to assist requesters, but they can also steer requests away from more contentious texts. Experienced users of ATI requests are not immune to this steering. When the brokering process results in opacity, this may not reflect a commitment to keeping certain records secret but instead may signal an access regime that is disproportionately concerned with procedural measurements of compliance. A brokering process that narrows a request so as to render it manageable within a deadline avoids the production of a “deemed refusal” statistic – the primary unit of measurement for many access oversight processes (see Thomas 2010a). The invocation of extension clauses and the chronic delays that characterize some ATI regimes contribute to decisions to restrict the date range or complexity of requests. An understanding of government information management processes, careful request follow-up, and the asking of probing questions by ATI researchers can lead to more effective brokering.

This complex process of brokered access raises questions about the powers and activities of government ATI analysts and coordinators. Former Assistant Information Commissioner of Canada Bruce Mann (1986) argued that access coordinators represent the “meat in the sandwich,” occupying a role unlike any other in the federal government. The uniqueness of this role is due to the position of the ATI coordinator within the “pyramidal hierarchy of government,” where the coordinator maintains “multiple working relationships” of both a hierarchical and lateral nature (580). According to Mann, ATI coordinators are positioned between a suspicious requesting public and a distrustful bureaucracy, and are further positioned in a confrontational role with oversight bodies such as the Office of the Information Commissioner. By foregrounding the competing interests in play within and between government agencies, however, Mann creates a certain distance between ATI coordinators and the agencies in which they are embedded.

Brokering access is political and, at present, inextricably linked to the management of public perceptions through government communications efforts. In using the metaphor of brokerage, we do not mean to imply that analysts and coordinators occupy the neutral position of a mediator or the proverbial honest broker between two parties with competing claims. For this to be the case, we would have to ignore the location of ATI workers within government agencies as well as the influence of overarching cultures of secrecy on the information disclosure process (Hazell and Worthy 2010).
We would also have to make assumptions about the neutrality of access law itself, including that it effectively operates according to a principle of presumptive disclosure and that it empowers ATI workers to apply balancing tests when disclosure is contested. And we would have to ignore inequalities in the exercise of power between the two parties – the requester and the government – whose interests are being brokered.

This is not the picture we paint. We use the term “brokering” to highlight the contingent and mediated nature of the ATI process, to foreground the position of ATI workers as the point of contact between the requesting public and government agencies, and to recognize the role that discretion and negotiation play. We are not implying that ATI workers possess a uniform set of motivations that serve to inhibit access, or that they necessarily work to advance secrecy. Our interest is in the position that ATI workers occupy within the machinery of government. We could just as easily speak about negotiated access, mediated access, or the gatekeeping of information within a secretive system. Access coordinators certainly play a gatekeeping role, not only through the negotiations that characterize access brokering but also through the discretionary application of exemption clauses under the ATIA. Journalist Dean Beeby (2011) argues that “overworked [ATI] bureaucrats largely focus on the technical application of legal loopholes to withhold information,” a position that echoes the perspectives of many of the contributors to this book. In the federal access regime, high rates of personnel turnover, coupled with the lack of a full devolution of authority from senior departmental bureaucrats to access coordinators, mean that ATI offices are unable to develop the institutional memory or independence that would enable them to operate as the proverbial meat in Mann’s information sandwich. Willem de Lint (2003, 386), in his study of police as brokers of access to sites and individuals, argues that knowledge work and the negotiation of access “cannot simply be decoupled from the question of ‘for whom?’ or ‘in whose interests?’” These questions are central to the study of access brokering and ATI as well.

The brokering of access also has a technological component. The quintessential image of an access-brokered document remains the white page with blacked-out sections of redacted text. In Canada, the hands-on production of blacked-out texts is becoming a thing of the past, as more government agencies switch to specialized software systems such as ATIPflow and the more advanced AccessPro Case Management. While the “where, when, and why” of redaction are established by discretion, law, and, at the federal level, regulations issued by the Treasury Board, agencies are free to
develop in-house policies around the “how” of redaction. This has led to an uneven access field, with many of the large agencies using state-of-the-art software and others not. These new programs, developed by the Ottawa-based software company Privasoft to meet the needs of Canada’s access regime, allow for the real-time management and tracking of all aspects of the ATI process, from filing to the tasking of requests to offices of primary interest (OPIs), to standardized correspondence, to redaction – which now appears as blank white space – and release package approval. They also offer tools for the stonewalling of sensitive requests through amber lighting and red filing. Amber lighting refers to the tagging of a request or a requester as politically contentious. Red filing refers to requests that are stonewalled by the minister or by the Prime Minister’s Office, who receive a weekly inventory of tagged requests.

Roberts (2005) contends that internal routines and technological developments ensure that ATI laws do not effectively break down governmental secrecy. Arguing that “special procedures for handling politically sensitive requests are commonplace in major departments” (4), Roberts discusses the way government departments try to mitigate the potential fallout of disclosing information. Over half of the requests in some departments (the Department of National Defence, for example) are amber lighted. Media lines and house cards are then prepared prior to the release of request packages so government spokespersons can field questions. There are various other techniques that ATI officers use to stall or stunt requests, some specific to certain types of agencies. The Canadian Security Intelligence Service (CSIS) ATI office has a policy of citing the sections of the ATIA it has invoked to exempt or redact information in a release package, but refusing to indicate which portion of the document the exemption clause has been applied to. This is explained as necessary to protect national security, lest unauthorized knowers glean information about state secrets by using exemption clauses as clues to missing content. Our favourite response from CSIS is, “We neither confirm nor deny the existence of such records.”

We use the term “techniques of opacity” to encompass the range of formal and informal attributes of access regimes that can effectively inhibit timely and comprehensive access to information. Some techniques of opacity stem directly from ATI law, in the form of exemption and redaction clauses. Others are more informal. Rigid and narrow interpretations of requests and efforts to steer requesters away from particular parts of the live archive through negotiation are techniques of opacity, for example. Many of the contributors to this book express frustration over the systemic delays
that characterize the Canadian access regime. The chronic delay problem certainly constitutes a technique of opacity, in that it inhibits timely access. In Canada, techniques of opacity are enshrined in access laws, institutional cultures, and technology. In Chapter 11, Fred Vallance-Jones describes the routine failure of ATI regimes to realize their own ideals of disclosure as the product of a range of “quasi exemptions.”

In making sense of opacity, we have found it useful to draw on the work of Ericson (2007), who argues that western societies have come to be governed through the problem of uncertainty. This shift in focus has caused many agencies to reorganize their work around precautionary measures and the identification and pre-emption of potential sources of harm or insecurity. We suggest that the idea of governing – and governing through – uncertainty and the ascendance of precautionary logics are helpful in thinking about the politics of ATI in the contemporary context. From the perspective of government, ATI mechanisms are often viewed as a pervasive source of uncertainty and political risk (see Savoie 2003; Thomas 2010b). Requests that seek potentially embarrassing records can destabilize carefully crafted and centrally controlled messaging efforts (see Roberts 2006), with unpredictable results. Seen in this light, the range of techniques of opacity employed by access brokers, the creation of communications products in anticipation of the publication of ATI records, and the broader cultures of secrecy within governments emerge as attempts to manage uncertainty, pre-empt surprises, and consolidate control. The intersection of this preoccupation with uncertainty and the ongoing expansion of the information society creates a paradox in which the circulation of information within the live archive is simultaneously a source of power and a potential source of insecurity for government agencies. As Ericson (2007, 217) notes, “the problem of uncertainty creates the urge to hunker down, avoid risk, and limit the freedom of others in the name of security.” It is this defensive hunkering down that has given rise to a federal ATI regime in Canada that is “sluggish, unresponsive and obstructionist” (Chase 2011).

Yet not all delays with ATI stem from the government agencies supplying the information. Drapeau (2009) has commented on the inability of the Office of the Information Commissioner (OIC) to investigate complaints concerning non-compliance, leading some government departments to exploit this impotence (see also Roberts 2002b; Rosner 2008). Information Commissioner Robert Marleau, who served from 2006 to 2009, is credited with spearheading a compliance campaign based on a business model of managing OIC investigations. Drapeau, however, accuses Marleau of
replacing knowledgeable OIC executives with new assistant commissioners with no expertise. Drapeau claims that more emphasis has been placed on the OIC ATI report cards, without any teeth being given to OIC enforcement.

To circumvent these techniques of opacity and to deal with complications stemming from OIC management of the federal access regime, researchers should consider ATI research as part of an information production feedback loop. The production and circulation of information within the live archive is shaped by an awareness of the potentiality of its release through ATI (see Chapter 8 of this book). ATI offices routinely inform government officials of the content of requests, and this information can influence changes in substantive practices and in the production of talking points and media lines. We find it fruitful to file requests for records pertaining to the management of previous requests. Adopting this stance demands a heightened commitment to reflexivity by the ATI researcher, and raises questions about how ATI requests as a form of data production can supplement existing social scientific research strategies.

Coda: Access to Information as a Tool for Critical Social Science

The access to information process appears to have a tenuous relationship with the social sciences (Walby and Larsen 2011, 2012). There is a prejudgment among most scholars that ATI requests are something used by journalists and lawyers, which means that systematic ATI research is an underdeveloped methodological approach in the social sciences. Those who wish to incorporate ATI into their research tend to learn through trial and error.

Haggerty (2004) has compared the knowledge production of social scientists and journalists. He suggests that journalists are comparatively free from the scrutiny of research ethics protocols that stifle researchers in social science. Academic research is often “comparatively less robust and critical than investigative journalism that can and does ‘name names’” (409). There is a need for social scientists to break away from “the path of least institutional resistance” (413) or letting ethical review boards govern the topics and methods of our research. There are clear rationales for using ATI/FOI instead of and in addition to conventional research methods. Journalists prefer ATI data because interviews with public officials are unreliable by comparison. If our goal in using ATI is to understand how government agencies do what they do, even the experience of being amber lighted, red filed, and stonewalled is important to write about (see Chapter 8).
On the Politics of Access to Information

ATI/FOI can play a key data production role in reinvigorating critical social science. Used systematically and with attention to key moments of reflexivity, ATI/FOI can provide researchers with invaluable access to backstage government texts. Additionally, and crucially, by treating the ATI/FOI process itself as an object of research, as opposed to an unexamined means to an end, we can study the interplay between practices of secrecy and information management in government agencies (Walby and Larsen 2012). We want this book to push social scientists beyond studying rhetoric and towards muckraking sociology. What we have called the live archive needs to be opened up. We are not suggesting that ATI can provide a “true” account of government – the results of ATI requests are more like acquiring small pieces of an always-shifting puzzle. There is a time and place for studying official discourse (Burton and Carlen 1979), but we also need access to the kinds of “dirty data” (Marx 1984) that are out there if we want a more comprehensive picture of the internal and external relations of political and governmental agencies.

Overview of the Chapters

This book is organized into four thematic sections. Part 1 sets the stage with two chapters on the history of ATI mechanisms and key features of ATI in Canada today.

In Chapter 1, Ann Rees argues that political opposition to access among party leaders and senior civil servants is the central problem facing ATI in Canada. This state of affairs is tied to the makeup of the ATIA, which includes broad exemption clauses for cabinet confidences and other sensitive executive branch records. Rees argues that the ATIA is as much about the codification of secrecy as it is about the facilitation of transparency, particularly given the ascendancy of security as a motif in government. Despite the political, legal, and bureaucratic forces operating to reduce transparency, Rees argues that ATI is essential to democracy. She concludes with several recommendations intended to rebalance the current equation of state secrecy and public interest access.

In Chapter 2, Gary Dickson, Information and Privacy Commissioner of Saskatchewan, provides an account of the historical development of provincial ATI laws in Canada. He makes a valuable contribution to the literature on ATI in Canada, which has predominantly focused on the federal level. Dickson introduces the concept of “access regime,” which encompasses the various legal, bureaucratic, oversight, and political mechanisms, actors, and decisions that collectively shape ATI in a given jurisdiction. Focusing on
Introduction

provincial access regimes, he identifies the factors that contribute to the unevenness of access across Canada.

Part 2 contains three chapters on security and information control. These chapters examine the use of security as an organizing framework for government activity, concomitant with moves to entrench mechanisms of secrecy and techniques of opacity, and the idea of “dirty data” (see Marx 1984).

Chapter 3, by journalist Jim Bronskill, explores the securitization of Canadian airport security screening tests in the post-9/11 context. Reconfigurations of security politics have led to this information being considered extremely sensitive. Bronskill discusses his efforts to obtain information about aviation security, the nature of the opposition he has encountered, and the ways in which government actors have gone about framing this material as a source of risk and a subject of secrecy. The chapter then addresses the implications of the securitization of information, discussing what this trend poses for ATI in Canada.

In Chapter 4, Willem de Lint and Reem Bahdi build on the theme of the securitization of information by providing an account of information control in the Canadian national security field. The unchecked flow of information is viewed by national security agencies as a source of risk. Opposition to this flow takes the forms of discourses of exceptionalism, efforts to procure public trust against a dynamic media backdrop, and attempts to challenge the loyalties of those who would contest secrecy. De Lint and Bahdi argue that efforts to consolidate information control also produce opportunities for resistance and contestation.

Chapter 5, by Yavar Hameed and Jeffrey Monaghan, focuses on strategies for push-back against information control. Their goal is to advance a social problems research agenda informed by opposition to injustice by gaining access to dirty data: “information which is kept secret and whose revelation would be discrediting or costly in terms of various types of sanctioning” (Marx 1984, 79). Hameed and Monaghan discuss strategies for getting at dirty data, unpacking these approaches through two case studies. Monaghan’s experience using civil litigation to gain access to data otherwise denied under ATI and Privacy Act requests has yielded significant results. In contrast, Hameed, working on the case of Abousfian Abdelrazik, has found that litigation can lead to a defensive tightening of information control, as evidenced by a comparison of pre- and post-litigation flows of information. The chapter argues for the use of multiple methods in search of disparate pieces of a puzzle that can later be combined.
Part 3 includes five chapters that illustrate how the use of ATI as a method of data production in the social sciences can assist in understanding government practices. Each chapter includes an account of techniques of opacity and a discussion of the formal and informal tactics that can be used to push back and obtain data. Chapter 6, by Matthew Yeager, discusses the merits of ATI requests as components of a research methodology. He focuses on request follow-through, complaints, and civil litigation as components of a conflict criminology approach. Originally published in the Canadian Journal of Criminology and Criminal Justice in 2006 and reprinted here with permission, this chapter represents one of the first pieces of Canadian criminological scholarship to focus on ATI. Yeager has revised the piece to include reflection on his recent experiences with suing the government for data. By responding to the denial of access by taking information brokering to its logical (and legal) extreme, Yeager argues that elite and state interests control disclosure.

In Chapter 7, historian Steve Hewitt reflects on eighteen years of using the ATI in research on the Canadian security state. He reviews the exemption and redaction clauses used to withhold information from researchers, and considers the relationship between these exclusionary practices and broader political agendas. One of the strategies that Hewitt employs is to seek access to records that are held by multiple agencies, and to compare the release packages and note the differential redacting of information. Hewitt moves on to discuss the implications of the existence of multiple versions of the same document for historical researchers and the ongoing trend towards reduced disclosure of security-related material, even of a historical nature.

In Chapter 8, Tia Dafnos discusses her research on the policing of Canadian Aboriginal activism using ATI. Outlining the access barriers and forms of opposition she has encountered, she reviews the successes and failures she has experienced using ATI to conduct research on the policing of the reclamation of Caledonia and the blockades of Tyendinaga. Dafnos observes that the policing of Aboriginal activism is characterized by an awareness of the potentiality of ATI requests, which in turn has shaped information management practices at the agencies in question. Her chapter is informed by a normative commitment to transparency as a means of ensuring accountability in public policing.

In Chapter 9, Justin Piché discusses his use of multi-jurisdictional formal and informal ATI requests in a study of contemporary Canadian prison
expansion. He recounts a three-stage research strategy that moved from the collection and analysis of publicly available information to a series of informal requests, and finally to the filing of federal ATI and provincial FOI requests. He discusses the various brokering processes he has developed, and the techniques of opacity that he encountered. The chapter concludes by considering the policing of criminological knowledge through access restrictions, and the importance of transparency for informed participatory politics.

Chapter 10, by Sean Hier, continues the discussion of methods. Hier’s focus is the development of policy concerning streetscape surveillance cameras in Canada. Through the cultivation of informal relationships with government managers (essentially the individuals who would be considered the offices of primary interest in a formal ATI request), he gained access to extensive sets of documents. The analysis of these texts has contributed to a more nuanced understanding of the forces influencing streetscape surveillance, enabling the revision of hypotheses developed during earlier phases of the research project and providing insights into the role of the privacy sector in streetscape video surveillance policy diffusion. Hier concludes by contrasting the tendency of researchers to adopt a conflict approach to ATI methods (see Chapter 6) with an argument for informal rapport building.

Many ATI researchers in the social sciences have been influenced by investigative journalists, who have helped shape the Canadian access regime by publishing the results of ATI research and challenging denials through litigation. Part 4 of this book includes chapters from some of Canada’s most prominent journalistic users of ATI. Given the fluid format of contemporary news media and the push towards instant reporting, timeliness of access emerges as a key issue. For journalists, access delayed is access denied.

Chapter 11, by Fred Vallance-Jones, is based on an exploration of what he describes as quasi exemptions – regulatory provisions within ATI laws beyond formal exemption clauses that can be used to block or delay the release of information. Disregard for statutory time limits for the processing of requests emerges as the most prominent quasi exemption, but prohibitive processing fees are also discussed. Based on interviews with veteran users of ATI, Vallance-Jones discusses the tensions between openness and secrecy as well as the implications of barriers at the bureaucratic, oversight, and legal levels. He argues that the current focus on incremental administrative reforms will not address quasi exemptions, and that legislative reform is necessary.
In Chapter 12, the Canadian Broadcasting Corporation’s David McKie argues that the Canadian federal access regime currently faces endemic issues that arise from its organization. McKie argues that the absence of political will to enact reforms or enforce compliance is the central problem facing the Canadian access community. The chapter is based on a case study of ATI research and reporting in the context of the 2008 Ontario listeriosis crisis. McKie notes the ways in which endemic access problems contributed to the media’s inability to convey information to the public in a timely fashion. Despite the pitfalls, reporting using ATI enables journalists to break stories of great public worth. The chapter concludes by exploring key resources and strategies for research success.

Chapter 13, by Jim Rankin of the Toronto Star, elaborates on lessons learned through data-based investigative reporting, and speaks directly to both journalistic and academic audiences. This chapter explores the idea that access to information is actively opposed by government agencies that have vested interests in the preservation of exclusive control over information. Rankin argues that ATI researchers must develop a particular skill set to effectively broker access, suggesting that proactive approaches based on knowledge of information management systems and persistent follow-up with ATI analysts are necessary. The chapter closes with reflections on the relationship between data-based journalism – currently the province of a small cadre of reporters – and traditional news media structures, and the prospects of moving towards an online, interactive reporting format.

ACKNOWLEDGMENTS

We thank the anonymous reviewers at UBC Press, as well as Sean Hier and Chris Hurl.

NOTES

1 One of the flaws with the Canadian federal ATI regime is that government departments and agencies can be brought under its authority only by being added to Schedule I of the Access to Information Act. This must be done either at the time that an agency’s own enabling legislation is created or amended, or in an omnibus fashion, as occurred following the passage of the Federal Accountability Act (2006). There is no presumption of inclusion, which means that some government agencies and Crown corporations “fly under the radar” of the act.

2 One of the only revelations as it concerns the pre-emptive information policing in government departments comes from Kelly (2006), who discusses his work as a government employee under the Mike Harris government in Ontario. Kelly discusses systematic methods of obstructing requests. First, requests can be obstructed by
taking a literal reading of request wording instead of helping to facilitate the search. It is easy to respond that “no such records exist” when a literal reading of the request is taken; only the provided key words are searched for. Second, Kelly discusses the way that cabinet briefing notes are covered under “Advice to Minister” or “closed meeting” clauses. Third, orders were given to destroy information. Twice, Kelly writes, he was advised to destroy all documents concerning Ipperwash and the murder of Dudley George by the Ontario Provincial Police.

3 Relyea (2009) argues that, similar to Canada, when ATI was introduced in the United States there were few government agencies that supported it. The Canadian provinces beat the federal government to the punch with regard to access law (see Rowat 1982, 177). Nova Scotia became the first jurisdiction in the British Commonwealth to establish a public right of access when in 1977 it passed a Freedom of Information Act. New Brunswick followed in 1978.

4 One of us filed a request with the RCMP for “documents and records” related to information-sharing arrangements between partners of the Integrated Security Unit in charge of the 2010 G20 Summit. The analyst in charge noted that the request was broad in scope and, for the sake of avoiding delays, recommended that its wording be amended to seek memoranda and letters of understanding only. This proposal sounded expedient, and was accepted. The RCMP responded by noting that no such MOUs or formal letters existed, closing the file.

REFERENCES


On the Politics of Access to Information


Sample Material © 2012 UBC Press

**LEGISLATION CITED**

*Promotion of Access to Information Act No. 2 of 2000* (South Africa).