


edited by

Philip E. Agre and Marc Rotenberg



**Technology and Privacy:  
The New Landscape**

---

# Technology and Privacy: The New Landscape

---

# Technology and Privacy: The New Landscape

edited by Philip E. Agre and Marc Rotenberg

The MIT Press  
Cambridge, Massachusetts  
London, England

© 1997 Massachusetts Institute of Technology

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from the publisher.

Set in Sabon by The MIT Press.

Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Technology and privacy : the new landscape / edited by Philip E. Agre and Marc Rotenberg.

p. cm.

Includes bibliographical references and index.

ISBN 0-262-01162-x (alk. paper)

1. Computer security. 2. Data protection. 3. Privacy, Right of. I. Agre, Philip. II. Rotenberg, Marc.

QA76.9.A25T43 1997

323.44'83—dc21

97-7989

CIP

---

# Contents

- Preface vii
- Introduction 1
- 1 **Beyond the Mirror World: Privacy and the Representational Practices of Computing** 29  
Philip E. Agre
  - 2 **Design for Privacy in Multimedia Computing and Communications Environments** 63  
Victoria Bellotti
  - 3 **Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?** 99  
Colin J. Bennett
  - 4 **Privacy-Enhancing Technologies: Typology, Critique, Vision** 125  
Herbert Burkert
  - 5 **Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity** 143  
Simon G. Davies
  - 6 **Controlling Surveillance: Can Privacy Protection Be Made Effective?** 167  
David H. Flaherty
  - 7 **Does Privacy Law Work?** 193  
Robert Gellman
  - 8 **Generational Development of Data Protection in Europe** 219  
Viktor Mayer-Schönberger

<b>9</b>	<b>Cryptography, Secrets, and the Structuring of Trust</b>	<b>243</b>
	David J. Phillips	
<b>10</b>	<b>Interactivity As Though Privacy Mattered</b>	<b>277</b>
	Rohan Samarajiva	
	List of Contributors	311
	Index	313

---

## Controlling Surveillance: Can Privacy Protection Be Made Effective?

David H. Flaherty

There is wide-ranging theoretical and empirical support for the importance of personal privacy in our respective lives, but there is some disagreement among nation states about how best to implement the protection of privacy of individuals in the public and private sectors. Instead of simply thinking about the issue and trying to develop some kind of theory about how best to proceed, my interest during the last 20 years has been to observe the kinds of significant privacy problems that have emerged in advanced industrial societies and then seek to monitor, through case studies, the various approaches of “regulatory” bodies, with widely varying powers, as they try to fashion solutions for the challenges to individual privacy that continue to surface.

Most of what I have learned was published in my 1989 book *Protecting Privacy in Surveillance Societies*,<sup>1</sup> which examined the workings of national and state data-protection agencies in the Federal Republic of Germany, Sweden, France, Canada, and the United States. As I am both an academic (at the University of Western Ontario) and a consultant on privacy policy, my findings and recommendations were very much shaped by direct observation of data protectors at work in many countries and by an examination of what they wrote, and what was said and written about them, in scholarly and journalistic circles. It is an understatement to say that examining the functioning of such small, important bureaucracies was a significant learning experience for me. But I do not think that it ever came into my consciousness that I would be given an opportunity to do such work myself in Canada.

In the 1990s I became interested in trying my hand at implementing privacy protection officially. Canada has had the post of federal Privacy

Commissioner since 1977; this post is filled through a political process dominated by the prime minister's office. Some of the provinces have similar posts. Quebec has had a Commission on Access to Information since 1982, but its members are also selected by the government of the day in what I would also describe as a political process.

In 1988, Ontario advertised for an Information and Privacy Commissioner and then allowed a select committee of the legislature to make the choice, subject to legislative approval. In 1991, when this post was open, I was not selected. In July 1993, however, also on the basis of a public competition, I became the first Information and Privacy Commissioner for the Province of British Columbia, which has a population of just under 4 million and is the third largest of the Canadian provinces (after Ontario and Quebec).

My provincial counterparts in Quebec, Ontario, and Alberta are both Privacy Commissioners and Freedom of Information Commissioners. These positions are still separate at the federal level, although there has been misguided agitation for their integration. (In my view, the sheer physical expanse of Canada necessitates separate commissioners to promote these competing interests effectively, especially since the staffing and budgets of the federal offices are comparatively small.) Canada is in fact unique in formulating laws and enforcement mechanisms, together, both for greater openness and accountability for general information in society and for the protection of the personal information of the citizenry. In the first instance, this process emulates of Sweden and the United States, but, especially compared to the latter, Canada is much more advanced on the implementation side of the ledger; that is, there is someone in charge of making the law work for citizens. Americans usually have to sue in the courts to achieve access to information or protection of their privacy when they encounter obstacles or practices that they consider objectionable.

In this chapter I propose to ignore, for the most part, the freedom-of-information side of my work in British Columbia, which involves the exercise of regulatory power in decision making on specific cases, and to concentrate on what primarily interested me in the writing of my 1989 book: how to try to control surveillance by making data protection effective in the public sector. Although I am more than three years into a six-year mandate as Commissioner, I want to reexamine the conclusions to



my book by testing my academic findings against my practical experience. I do so fully cognizant of the risks of egocentrism's being the primary theme of what follows. I hope that by being self-critical and by giving fair play to my critics I can avoid wallowing in excessive self-admiration. I also acknowledge, in advance, that any model of data protection is much affected by the personality of the commissioner, the political culture of a particular jurisdiction, and the state of the local economy. Good times are better for data protection than bad times.

I would suggest that a cynical legislature, wanting to offer only the illusion of data protection, should not in the future select a privacy commissioner who knows anything about his or her duties at the time of selection, since there is a significant learning curve for any new appointee, especially if the office is new. Based on my 20 years of research and consulting activities concerning the protection of privacy, I knew in particular that I had to adopt a proactive approach to the advocacy side of my work (the "privacy watchdog" role), which continues to be a big surprise to politicians and to the bureaucrats who actually run government in the trenches. "What is Flaherty trying to do to us?" has been a not-uncommon response by the government in power and by the public service to my advocacy role and my media statements on privacy issues. Just as the bureaucracy is having to learn to live with freedom of information and with privacy protection, so we have been learning how to live with one another and to appreciate our varying responsibilities. I have not suffered from a lack of invited and volunteer tutors.

### **The Need for Data-Protection Laws**

As I noted in *Protecting Privacy in Surveillance Societies*, "the existence of data protection laws gives some hope that the twenty-first century will not be a world in which personal privacy has been fully eroded by the forces promoting surveillance."<sup>2</sup> This debate has been handily won by the pro-privacy side of the equation, at least in most advanced industrial societies. It is now an odd Western nation, state, or province that does not have explicit laws for controlling the collection, use, retention, and disclosure of personal information in both the public and the private sector.

In the 1980s I was still somewhat cautious about fully endorsing the need for data-protection laws. The deregulation movement led by Margaret Thatcher and Ronald Reagan was in full flood, and the American resistance to regulatory intervention of this type was also flourishing (with interventionism being ahistorically viewed as some kind of un-American activity, a kind of first step toward a socialist state). But advances in the development and application of information technology since the mid 1980s, almost bewildering in their scope and pace, have lent considerable urgency to the argument that government's and the private sector's rapid adoption and application of numerous forms of surveillance technology require a watchdog mechanism and a set of statutory rules for fair information practices. Data matching, photo radar, digital photographs, criminal-record checks, and pharmacy prescription profiling systems are some local examples that spring to mind. As I wrote in 1989, "the critical issue is how best to strengthen data protection in the face of strong, sustained, countervailing pressures for surveillance."<sup>3</sup>

In fact, my experience in British Columbia is that the pressures for surveillance are almost irresistible for an office such as mine. The bureaucrats and the legislature are under intense pressures to reduce costs, to promote efficiency, and to spend public money wisely. Surveillance technology appears to be a neutral, objective process that must be wielded as a weapon, or at least a tool, against welfare cheats (targeting all those on income assistance), sex offenders (targeting all those who work with children through criminal-record checks), and photo radar (monitoring all cars and photographing the license plates of speeders).

I also notice considerable pressure in British Columbia for the rationalization of identity checking of applicants for government benefits, whether for income assistance, health care, or drivers' licenses, on the basis of what is euphemistically called a "common registry." This registry appears to be the first step toward the development of a national data bank, which has figured in the nightmares of US privacy advocates since the 1960s. The fact that such technological applications are so apparently achievable drives these seeming imperatives among legislators, functionaries, and the taxpaying public. One consequence will be a full-fledged surveillance state. I really fear that such a result is almost impossible to prevent in the long term, whatever the prodigious efforts of data protectors and their allies.

Thus, my stated ambition in 1989 of “protecting the personal privacy of individuals to the fullest extent possible in a democratic society”<sup>4</sup> seems to be increasingly problematic. Neither government nor the private sector really likes the privacy business, whatever it is, because it gets in the way of their continuing to do business as usual with personal information. (Here I am referring to the government as a collectivity rather than as specific individuals with human concerns: I find it tedious to be told, repeatedly, by those practicing the systemic invasion of privacy how much they value privacy in their own lives. Getting government officials to think as human beings, with families and friends, is an ongoing challenge for data protectors.)

Concern for privacy comes to be perceived as an unnecessary barrier to what is regarded by most legislators in governing parties, and by some taxpayers, as clearly rational behavior. Hence the value, in my opinion, of having data-protection laws and officials in place. They are at least a temporary barrier to what others naturally perceive as progress in dealing with some problem of the moment that seems to require fixing. The “fix-it” solution is even more software, systems, record linkages, and advanced surveillance technology. These trends place data protectors in the awkward and unpleasant position of at least appearing to resist multiple forms of progress—but that is what they and their staffs are paid to do.

### **Defining Privacy Interests to Limit Surveillance**

It is no particular surprise that legislators in British Columbia, as elsewhere, did not heed my advice to define privacy interests more adequately in legislation as a guide to limiting surveillance.<sup>5</sup> I conclude that those who draft legislation must in fact throw up their hands in bewilderment at such a prospect, if they have indeed ever been invited to tackle the thorny issue of defining privacy. Only philosophers continue to bemuse themselves with this important activity, it would appear, while individual authors parade their ingenuity with increasingly obscure, and obscuring, definitions.<sup>6</sup>

I have had no more success at focusing legislative efforts on articulating the central privacy interests that require protection. However, let me say, immodestly, that among the most useful features of my book are

several tables that seek to summarize the “privacy interests of individuals in information about themselves”<sup>7</sup> and “data protection principles and practices for government information systems.”<sup>8</sup> The latter table originated as an *aide memoire* as I attempted to track the most appealing features of extant laws and major legal decisions. A number of them, including the principles of informational self-determination, publicity, transparency, finality, data trespass, and the right to be forgotten (all admirable products of European thinking and lawmaking), do not appear explicitly in the BC Freedom of Information and Protection of Privacy Act. My conscious goal has been to promote these principles and practices on the local scene by reprinting the two tables in the introduction to my first annual report for 1993–94, referring to them in our Investigative Report No. P95-005, March 31, 1995, and generally discussing these broad measures to protect privacy in my ongoing media relations and public education efforts in the province. The “right to be forgotten” figured in one of my recent orders (Order No. 58-1995, October 12, 1995, p. 7).

I wrote in 1989 that “protection of privacy should also remain largely a nonlegal activity in most areas of human existence, meaning that even when data-protection laws exist, individuals have to rely to a considerable extent on their own efforts, such as refusing to give out personal information, in order to limit unwanted surveillance.”<sup>9</sup> In old and new ways, data protection, in my considered view, remains largely a matter of raising consciousness at various levels of society. Despite my ongoing efforts to act as the privacy watchdog for the province, I regularly end my interactions with the general public, on radio talk shows in particular, by encouraging every listener to be their own privacy watchdog by controlling what they choose to disclose to outsiders and by monitoring what they are being asked to disclose. More and more people appear to be prepared to say that a request for their personal information is none of anyone’s business. A more privacy-conscious public service means that privacy-impact statements for proposed legislation are prepared at an appropriate time in the annual legislative calendar without my office’s always having to intervene to stimulate such an activity in the first place. The several times that this has happened in British Columbia, especially through the good offices of the Ministry of Health, are an ongoing sign of progress in data protection.

In classic liberal fashion, I emphasized in my book the need to balance privacy against competing values and legitimate governmental purposes.<sup>10</sup> My efforts to appear balanced to consumers of my research strike me as naive in retrospect: the striking of balance within government is so much against the privacy interests of individuals that it is a wonder we have any privacy left once governments get through doing what is good for each and every one of us. What is good for government is always thought by those in government to be good for the public at large.

I emphasized in 1989 the importance of minimizing data collection in order to reduce intrusion into private lives.<sup>11</sup> I am more than ever convinced that this is a central concept in debates over privacy and its preservation. Personal information must be collected and shared only if there is a demonstrated need for it in the first place. As a “culture of privacy” begins to impinge more on the operating consciousness of the hundreds of thousands of persons working for public bodies subject to the BC Freedom of Information and Protection of Privacy Act, I find modest evidence of a self-initiated process of questioning why certain data should be collected. Among other things, we have succeeded in ending the collection of the Social Insurance Number, a unique personal identifier, in at least a dozen settings, including its use as a customer control number by BC Hydro.<sup>12</sup> On the other hand, we have also accepted the explanations of the BC Gaming Commission as to why it feels compelled to collect so much personal information about the people associated with applications for licenses to run gambling establishments.

### **The Need for Data-Protection Agencies**

In 1992 the legislature of British Columbia, led by a newly elected New Democratic Party, created the Office of the Information and Privacy Commissioner in imitation of the Ontario and Quebec models. Alberta, under a very conservative premier who has substantially cut back government services, imitated British Columbia in 1995. Thus, all the most populous provinces in Canada now have data-protection agencies.

I need to separate my support for such initiatives, both in theory and in practice, from my criticisms of how privacy commissioners actually go about their work, since these are quite different matters. In my judgment,

the best evidence of the need for privacy-protection bodies is the sorry state of data protection in the US, where only a few of the states have equivalents of the Canadian agencies. Those brave souls in New York, Connecticut, Minnesota, and Hawaii work valiantly within the executive branch to promote freedom of information and privacy, but they lack independence, financial and human resources, and political clout. What they have accomplished gives some sense of what is needed and of what is possible in a market-driven capitalistic society that treats personal information as simply one more tradable commodity.

The United States suffers from a lack of an ongoing, institutionalized body of specialized privacy expertise directly available to all levels of government. The small network of talented US privacy advocates, including lawyers in private practice, cannot compensate adequately for this lacuna. It is demoralizing to watch admirable organizations like the Electronic Privacy Information Center (EPIC) have to bring lawsuits to accomplish privacy-protection goals that are rarely recognized in the federal and state legislative arenas. Although there is a clear role for litigation in the implementation model for any such law, it should not have to be the first recourse for concerned or affected citizens, who can rarely afford such a luxury as suing the government.

Although my office has encountered resistance to its data-protection work, one of our considerable accomplishments in a geographically limited area has been to bring our existence to the direct attention of policymakers, senior politicians, policy analysts, and other public servants, at least in the central government. Whatever they may think of our actual work, they are aware that we exist. My proactive advocacy role on privacy issues has surprised them, I think, because the provincial Ombudsman and Auditor General function somewhat differently than the commissioner and because neither of them has regulatory power. They may identify problems, and they may make recommendations; however, because I have the authority to make binding decisions in access-to-information cases, my “recommendations” carry considerable weight in achieving compromise solutions on privacy policy (unless, of course, the legislature decides to move ahead with its plans anyway—e.g., by implementing a province-wide system of criminal-record checks to uncover pedophiles with criminal records). But I am not part of the hierarchy of

public service, and some senior bureaucrats have trouble accepting that I cannot be controlled, in the traditional sense, for the sake of specific political or administrative agendas (even though informal pressures of that sort exist).

I wrote in 1989 that data protection “requires significant modification in information-handling practices.”<sup>13</sup> I also thought that data protectors always encountered significant resistance from one organization or another. I can honestly say that I have not met or felt such overt resistance, especially on the privacy side of my work, although this may be due to a lack of perception or of sensitivity on my part. The most significant resistance has come from the Ministry of Human Resources, which has an enthusiasm for data matching. We have not found examples of significant bad actors who require numerous remonstrances; perhaps the “bad guys” are still hiding from us. This presumably happy situation is explained in part by the fact that we are still in the honeymoon phase of our relationship with government and in part by BC’s relatively robust economy. Budget cutbacks, which are now beginning, will have an impact on the capacity of my office to accomplish its statutory tasks. We will have to concentrate on our core activities, which include mediating requests for review of access requests, investigating complaints, giving policy advice to public bodies, conducting site visits as a form of auditing, and engaging in media relations and public education.

I still like my 1989 formulation that “data protection commissioners or agencies are an alarm system for the protection of privacy.”<sup>14</sup> Our tools include oversight, auditing, monitoring, evaluation, expert knowledge, mediation, dispute resolution, and the balancing of competing interests.<sup>15</sup> Thus, I continue to believe that “data protectors are specialists in articulating privacy interests on a systematic basis on behalf of the public and in applying fair information practices.”<sup>16</sup>

The risk side of the equation is that we will “simply become agents for legitimating information-collection activities and new information technology.”<sup>17</sup> We may act only “as shapers of marginal changes in the operating rules”<sup>18</sup> for instruments of public surveillance, losing battles as often as we win them. I certainly feel strong pressure to get along with my central-government colleagues, and my staffers are all public servants who might like to work elsewhere in government later in their careers.

To date I do not deserve to be considered an active agent for the legitimization of government practices, although I have had my failures. At the end of two years of discussions, the Pharmanet prescription profile system went into effect with most of my suggestions for data protection incorporated, but I could not stop the mandatory nature of the system in the face of the cabinet's desire to establish it as a cost-saving measure. I had no impact on another massive system for invading the privacy of one-sixth of the adult population, criminal-record checks for all those who work with children—the government and the legislature were not persuaded by any of my private or public advice. I had to accept a system of data matching intended to ensure that British Columbia's recipients of income assistance are not also receiving such help from other provinces. (The record of cheating is undeniable. The privacy of all those on income assistance is invaded because of the fraudulent behavior of a small minority. We succeeded in getting a requirement that all recipients of income assistance be notified of the data matching, and in getting ongoing monitoring of the fraud-prevention process. When we questioned the legal authority of the Ministry of Human Resources to perform data matching, the ministry secured legislative authority for the activity, thus minimizing my impact and authority.)

### **The Effective Conduct of Data Protection**

In compliance with my own admonitions, I have adopted and applied a functional, expansive, and empirical, rather than a formal and legalistic, approach to my statutory tasks. In essence, I try to keep the broad goals of protecting privacy in mind rather than worrying unnecessarily about legal niceties. I do have to follow the Freedom of Information and Protection of Privacy Act; however, as I said in my Order 74-1995, I am not much interested in making Jesuitical distinctions that would bring credit to a medieval theologian but would not make much sense to the taxpayers of British Columbia.

As a matter of fact, I find myself preoccupied in more than 140 decisions to date with the broad goals of the aforementioned act. My greatest goal has been promoting openness and accountability of government to



the public. My Achilles' heel with respect to judicial review is proving to be an expansive application of solicitor-client privilege, despite my efforts to restrict its application in accordance with the broad goals of the act. With respect to the privacy side of my dual mandate, and this may be an inherent limitation of the single-commissioner model, I can be accused of having occasionally sacrificed the privacy interests of individuals in the pursuit of greater openness.

Fortunately, section 22 of the act contains a set of privacy standards that my colleagues and I apply to specific decisions about the disclosure of personal information by public bodies. This has involved very nice distinctions in about half of my decisions. I, like others, will be quite interested to see where the bright lines are finally drawn in this regard about such problems as disclosing the identities of complainants or informants. I believe that my own emphasis on making decisions on a case-by-case basis, rather than worrying too much about consistency, fits into a pragmatic and functional approach to my statutory tasks. I am clearly concerned about making appropriate policy decisions on the basis of the act rather than being what Americans call a strict constructionist.

The empirical approach of my office also deserves attention. We are interested in knowing, in as much detail as is necessary, how a proposed new system or a modification of an existing one will actually work. This is not a trite point, because I believe it is an extremely important perspective for a data protector to adopt. One cannot regulate a system without fully understanding it.

Another important component of our approach is avoiding public and private confrontations by being pragmatic in our approach to negotiations. Spiros Simitis (the data-protection commissioner of the German state of Hesse) wisely described this as "a gradualist or incremental approach to data protection, involving cooperation, a process of learning, and a search for consensus."<sup>19</sup> We are not even remotely interested in fighting for the sake of fighting. I also fully agree with Simitis, based on practical experience, that our work is political in the best sense of that abused word, which means, in this context, having good working relationships with those being regulated in order to convince them that they are being treated fairly, seeking appropriate allies as needed, and communicating effectively with the public through the media.<sup>20</sup>

I can only smile, diffidently, at my description of the ideal data-protection commissioner as a person who is “self-confident, perceptive, experienced, well-connected, reasonable but firm, has a strong presence, and is politically astute.”<sup>21</sup> In terms of building a constituency, I have been blessed with the lobbying and public-education activities of the Freedom of Information and Privacy Association (FIPA) and the British Columbia Civil Liberties Association (BCCLA). The concentration of perhaps two-thirds of the population of British Columbia in greater Vancouver and Victoria makes it easier to reach the public and to interest the media in the work of our office. In terms of promoting my stated views on how things ought to be done in order to make data protection effective, I have been singularly blessed by being educated at the feet of some of the great practitioners of the art, including Spiros Simitis, Hans Peter Bull, Jan Freese, and John Grace. Thus, it would have indeed been surprising if I did not know what I should at least try to do in the conduct of this “vital activity.”<sup>22</sup>

I especially like being reminded by my own writings that it is necessary to understand and be mindful of the competing interests of the government, the legislature, the public service, and various segments of the public.<sup>23</sup> There is no use pretending that privacy protection is the main purpose or activity of any part of government. Competing interests must be taken account of in finalizing decisions on specific data-protection matters and in finally deciding what advice to offer a public body about a particular program or practice. My oversight of certain aspects of the work of municipal police forces is a good case in point. I have been concerned with such issues as the security of records and the adequacy of audit trails for police users of the Canadian Police Information Centre (CPIC).

In my 1989 book I vacillated between the avoidance of bureaucracy in a data-protection organization and the risk of having “an overworked and overcommitted staff that provides only the illusion of data protection.”<sup>24</sup> My office has not had the time to become either overworked or overcommitted, although I plead guilty to the common sin of neglecting inspections or audits (which I prefer to call site visits). This activity takes second place to my particular need to write orders to settle specific cases.

I fully agree with my prescriptive statement that the primary role of a data-protection agency is the actual articulation and advancement of the privacy interests that must be defended in a particular setting.<sup>25</sup> In my case, the public body and/or the legislature eventually establishes what they perceive to be the acceptable balance among competing interests (not always to my complete satisfaction). For specific cases, however, I reach conclusions about appropriate information practices as the decision maker, subject to judicial review in the courts.

### **Independence and the Exercise of Power**

The exercise of independence by a regulatory authority, subject to appropriate external controls, is vital to successful data protection. In British Columbia, I am somewhat protected as an officer of the legislature, with a fixed six-year term that is not renewable, a salary tied to that of the chief judge of the Provincial Court, and a generous pension plan for the actual period of employment. Because I knew from my studies about the importance of the independence factor, and because of my own personality, I have emphasized my independence in words, actions, and orders. I am protected by having a tenured professorship to return to at the end of my appointment, the importance of which I knew from the previous experience of Hans Peter Bull and Spiros Simitis in Germany.<sup>26</sup>

The fact that my budget (\$2.6 million Canadian) comes from the same Treasury Board that funds the entire public service has not escaped my attention. Fortunately, I have an approved staff of 25. That is the number that I planned for from the beginning, and I am committed to accomplishing what we can with that staff by learning to work more and more effectively. But I am also subject to the same budget cutbacks that have occurred throughout the government of British Columbia. If our workload continues to grow significantly, I may also find myself with cap in hand before the Treasury Board, seeking to justify increases in budget and personnel in a very tight fiscal situation.

My staff consists of public servants appointed in compliance with the Public Service Act, which at least makes them insiders to government in terms of potential job mobility. Because of the wishes of the legislature, none of them are union members.

My concern for independence is counterbalanced by the desire to build an effective network in government circles to facilitate the mediatory role of our office in settling most of the requests for reviews of access decisions that come to us. While I know that networking is necessary, there is also a risk of our being coopted by a desire to get along and go along. Again, I am very grateful that two public-interest advocacy groups, the Freedom of Information and Privacy Association and the BC Civil Liberties Association, keep our feet to the fire with constructive criticism.

Fears among public bodies of my “independence” may also have been mitigated by the fact that they have to date been successful in about two-thirds of the cases I have had to decide. While my decisions against the government tend to receive a lot of publicity, especially from successful media applicants, public bodies have won major victories on attempts by the public to access long-distance telephone logs and back-up e-mail tapes. I also like to emphasize that my 140 decisions to date have been reasonable and pragmatic, hoping thereby to assuage the ongoing anxieties of more than 2,000 public bodies by demonstrating that the intervention of my office in their routine work is well considered, with appropriate deference to professional judgment and awareness of the practical realities of running a government or providing public services.

My own office lacks an oversight mechanism for reporting to the legislature in a truly meaningful way. Receipt of my annual report is a relatively perfunctory matter; it is simply tabled with the reports of everyone else, and no legislative committee discusses it with me. The Privacy Commissioner of Canada and my counterpart in Ontario appear to have somewhat more meaningful reporting relationships with their respective legislatures. My annual reports have been relatively nice to government and not especially controversial. I have also not issued a special report to the BC legislature on a particular problem; that would likely attract more attention.

The flip side of this issue of reporting is that my situation also prevents direct interference by legislators in my work. I did have the experience of being told publicly by one member of the legislature that I worked for her. I prefer, now, to state that I am appointed with a six-year no-cut contract, subject to impeachment for maladministration and other heinous matters. There is a provision for a special committee of the legislature to

begin a review of the functioning of the act within 4 years of its going into effect (meaning October 4, 1997), and I expect at that time to revisit this matter.

My main contacts with members of the legislature, especially with members of the select committee that appointed me in 1993, are on an individual basis. As a result of my negative experience with criminal-record checks in the spring of 1995, I am committed to directly informing the 75 members of the legislature about my views on privacy matters coming before them.

The legislature has amended the Freedom of Information and Protection of Privacy Act on several occasions, but not in ways that affect my work. The major amendments have been “notwithstanding” clauses to other acts to protect the operations of certain specialized agencies of government on freedom-of-information matters. My advice to the cabinet on most of these proposals was accepted. How to provide for adequate warnings of future contemplated changes is problematic; again, networking appears to be the solution.

With respect to the exercise of power by my office, I have heard vague rumblings that I have too much power and related complaints that I am making policy for the government. Though we have not had “an uphill fight” to make our voices heard,<sup>27</sup> I am more aware than at the time of my appointment of the limits of what my office can accomplish, even with the expansive mandate entrusted to it under section 42 (the “information czar” clause) of the act. We have the resources to be at most a thorn in the side of thousands of public bodies. We are also having to continue to work hard “to win the cooperation of the regulated,”<sup>28</sup> a task admirably performed by a director, a dozen portfolio officers, and two intake officers in my office.

Our main problem is learning about the major initiatives of public bodies at all levels that have surveillance implications when it is still possible to do something about them, although I think that my colleagues and I now have better antennae and a better network than we did in our early days. The government assigns task forces and study teams to examine various initiatives and then sometimes refuses, or is reluctant, to tell me about them because the cabinet has yet to give its approval. But once the cabinet has acted, my hands are relatively tied. There are also so

many ongoing issues of access to information and data protection that crisis management is almost the dominant mode of operating. And the more orders I produce, the more one public body or another may have reason to be unhappy with me. They remember their losses much more acutely than their victories.

At the end of the day, as I have noted above, my independence and power are considerably limited, in the policy field, by the authority of the legislature to make any statutory decision that it wishes to introduce or to increase surveillance of the population in some manner.<sup>29</sup>

I concluded my 1989 treatment of these issues by emphasizing the importance of personnel selection and public relations. I have been most fortunate to recruit a professional staff of considerable experience and varied professional and administrative backgrounds and careers. It has been difficult for anyone with less than 10 years' experience to win a posting at the senior level in my office. These individuals not only know how government works, they also fully appreciate our independent role. Several key personnel came from the office of the ombudsman and thus understand intimately the role of guardian agencies in the political and bureaucratic process.

### **The Adequacy of Advisory Powers**

This is the area where my views have changed the most since 1989 as a result of my direct experience with a regulatory data-protection statute in British Columbia. I only hinted then at the fact that advisory powers might not be adequate to the tasks at hand.<sup>30</sup> I now believe that a privacy commissioner should have regulatory power at his or her disposal. Yet the reality is that most of the problems brought to my office are settled through mediation, not through orders and binding rulings. Our approach is very conciliatory. We act "in a flexible and pragmatic fashion, responding as much as possible to experience and learning" from our mistakes.<sup>31</sup>

Our work has been facilitated by considerable media coverage. It is difficult to measure what the public thinks about us, but those in the Lower Mainland and in Victoria have been given many opportunities to learn about our watchdog role in privacy matters. Since the media tend to

support decisions favoring their requests for access to information tends, there is probably a “halo effect” transferable from my work as Information Commissioner to my work as Privacy Commissioner. Independent surveys of public opinion continue to document very high levels of concern in British Columbia for the protection of individual privacy: “Outbreaks of aroused public concern create a positive climate for the implementation of data protection.”<sup>32</sup> A series of relatively minor privacy disasters, especially in the health and medical field, have been very important for consciousness raising among the general public. Sensitive personal records being faxed to the wrong places have been prime examples of this trend. This led the Ministry of Health to authorize a very useful report by Dr. Shaun Peck, the Deputy Chief Medical Officer for the province, entitled *Review of the Storage and Disposal of Health Care Records in British Columbia* (1995).

One “weakness” in the Freedom of Information and Protection of Privacy Act that I anticipated in 1989 is the absence of statutory sanctions. If a public body or its agency fails to comply with the fair-information-practices provisions of the act, there are no criminal sanctions in the act itself, however serious the breach. I am satisfied for the moment, however, to rely on progressive disciplinary proceedings for the exercise of social control. But a four-day suspension of a municipal police officer for unauthorized use of the Canadian Police Information Centre to access the provincial motor-vehicle database was widely perceived as too small a slap on the wrist, and indeed a complainant has appealed it. While other “offenders” might be prosecuted under various sections of the Criminal Code of Canada, this may not be enough to satisfy the public lust for blood when a serious breach of the act occurs. I maintain a holding brief on this matter as I await guidance from direct experience. I sense that the public would like to know that there is a provision in the act to “punish” someone when egregious breaches of confidentiality occur.<sup>33</sup>

### **The Primacy of Data-Protection Concerns**

I argued in 1989 that privacy protectors should stick to their knitting and avoid direct responsibility for the other information-policy issues of their respective societies. The implication was that they should avoid issues not

related to controlling surveillance of the population and emphasize the protection of individual human rights.<sup>34</sup> The pressures to meddle in broad issues of information policy are indeed great, especially as the “information highway” debate rolls along and especially for an individual who is both an information commissioner and a privacy commissioner. As I have said above, I am aware of the limits of what my office can accomplish with the resources that we can legitimately expect society to entrust to us. What I have done is establish working relationships with others charged with such matters as promoting computer security, including people in the office of the province’s new Chief Information Officer. I very much welcome the fact that the Chief Information Officer has assumed overall responsibility for the province’s information policy. I like to be kept informed of important developments affecting information policy, but there are limits to what I can do to shape them. On the other hand, I prepared submissions on privacy issues to the Industry Canada task force on the information highway and to similar deliberations on the same topic by the Canadian Radio-television and Telecommunications Commission.

Since I have accepted working in a system where access to information and privacy protection are combined in the same act, what more could I try to do in the area of information policy? The real burdens of trying to do the former relatively well speak volumes for a policy of non-expansionism for officials with responsibilities like mine.

### **Complaints, Audits, and Access Rights**

The section on this subject in my book presented some conclusions about the conduct of the actual core activities of data-protection agencies. My skepticism about the centrality of complaints as a guide to implementation has been borne out in British Columbia. Complaints are indeed a “safety valve” for an aggrieved public (usually the person who thinks he or she has been negatively affected) and do help to set priorities for audits or inspections by my office.<sup>35</sup> The latter point is especially relevant for complaints from interest groups such as the BC Civil Liberties Association. Its complaint about drug testing by the BC Racing Commission gave me an opportunity to visit a harness track and to prepare a report on drug testing in this tiny part of the public sector.



It is easy for persons who have been subject to government action, such as removal from office, to complain to my office that their privacy has been invaded, since information about them was allegedly used in an unauthorized fashion. In such a case, my portfolio officers investigate and prepare a report, which is released to the individual. There are complainants who seek government benefits but do not wish the authorities to hold or use personal information about them. My sense is that my colleagues do a fair bit of explanation of the facts of life to such individuals. I had certainly not anticipated the number of difficult clients that would find their way to a “helping” organization such as my own; university students are quite a compliant lot in comparison.

I must also admit that the Freedom of Information and Protection of Privacy Act was drafted in such a way that public bodies, including law-enforcement agencies and those who can claim to be engaged in a law-enforcement matter, enjoy considerable latitude in using personal information for purposes perceived as legitimate. This is a matter that we will have to review in detail in preparing submissions for the legislative review of the act. The public service, including municipal police forces, were not guileless in the shaping of the legislation.

My sense is that complaints to my office in British Columbia have not yet produced the systemic results that I would hope for from such a mechanism for redressing grievances. We have had much more systemic success from our eight investigative reports as a result of incidents that have occurred or, in fact, complaints. Incidentally, our frequent practice in the latter regard is to rely on separate investigative reports prepared by public bodies themselves, such as the Ministry of Health or a hospital, when privacy disasters occur. This has the particular benefit of preserving our human resources for essential activities and permitting us to audit the auditors.

I have always been an admirer of the conduct of audits or inspections by the German federal and state data-protection offices and the Privacy Commissioner of Canada for the pursuit of statutory objectives: “Audits are crucial to an activist, aggressive stance; . . . it is necessary to create an atmosphere of prior restraint for prospective privacy offenders.”<sup>36</sup> I am especially interested in on-site inspections, which I have come to describe by the more neutral term “site visits.” My most significant contribution

in 1992 to the shaping of the BC Freedom of Information and Protection of Privacy Act was to urge, successfully, the inclusion of authority for the commissioner to “conduct investigations and audits to ensure compliance with any provision of this Act” (Section 42(1)(a)).

My site visits are a form of consciousness raising among public bodies. I have been to many prisons, an adolescent detention center, Correctional Services, hospitals, and municipal police forces, city halls, local Human Resources offices, psychiatric and counseling offices, universities and colleges, and public health departments. My colleague who paves the way for site visits has to engage in quiet diplomacy, since the initial reaction to a proposed inspection is not always welcoming. I meet with the head of the public body or office, the persons with direct responsibility for compliance with the act, and senior management. Whenever possible, I give a talk about the act to a gathering of the staff, and I answer questions. This has been a particular characteristic of my visit to hospitals, an area that I am very concerned about in terms of promoting fair information practices. I always do a walkabout to visit representative parts of the operation. I sample printed and electronic records, review what is accessible from staff computers, and ask questions of individual staff as I encounter them, whether in personnel offices or in the workstations of head nurses. I have the authority to look at any records held by a public body. Many small problems tend to come to the surface during my visits, and these are often easily remedied. I believe that I have especially reinforced the roles of those with delegated responsibilities for implementation of the act—the agents on the spot, so to speak. My visits also have a ripple effect, by word of mouth, among similar public bodies.

The reality is, however, that I have relatively little time to spend on site visits, if I am going to keep up with my case load of decision making. The portfolio officers from my office are often in the field mediating specific cases, and I have encouraged them to contribute to the conduct and impact of site visits. They too offer advice on the spot and suggest improvements. I intend to avoid the illusion of data protection by repeating site visits to public bodies that appear to warrant them.

Despite the efforts of my learned colleagues among privacy advocates to persuade me otherwise, my direct experience has reinforced the skepticism I expressed in my book about the importance of access and correc-

tion rights.<sup>37</sup> I am delighted that the Ministry of Children and Family Services has given out more than a million pages of records to thousands of applicants who want to learn the histories of their lives as children in care or as adoptees. That is a direct, consequential benefit of the act with enormous significance for individual lives. I believe, intuitively, that knowledge that a person may access information about him or her recorded by a public body engenders appropriate prudence and cautiousness among those who create and compile such records in the first place. For the large ministries that collect a lot of personal information, the Portfolio Officers on my staff mediate a considerable number of individual requests for access to personal information. Thus, I have rarely had to deal directly with a denial of access to personal information. We are also very involved in ensuring access to general information held by public bodies.

### **Monitoring Surveillance Technology**

I advocated a special role for data-protection agencies in monitoring developments in information technology at a time when personal computers were not yet ubiquitous. In my 1989 book I wrote: “For either a well-meaning or a malevolent regime, there are no technical limits to electronic surveillance and social control at the present time.”<sup>38</sup> The situation can only be viewed as having worsened since I wrote those words, and one fears that it will continue to deteriorate despite the best efforts of data protectors. Technological imperatives are increasingly harnessed to government’s goals of reducing costs, avoiding fraud, and improving efficiency.

One can today only acknowledge “the continued and voracious expansion of the public and private sectors’ appetite for more and more refined and integrated personal data at the expense of personal space and individual autonomy.”<sup>39</sup> I am more aware of this in the private sector than in the public sector. My sense is that the public sector has not been able to afford the software and data-matching resources for personal information that have been marshalled by direct marketers (especially in the United States).

We are making an effort in British Columbia to reach the “specialists in informatics” who can “mobilize technological expertise for protective purposes.”<sup>40</sup> But I do not have such specialists on my staff, nor could I

justify such expenditures.<sup>41</sup> I am fortunate to have on my staff a few people with systems backgrounds and considerable interest in applications and developments in technology. I rely on their antennae and networks to keep me informed on relevant issues. The government operates various fiber-optic networks across the province, which means that we need not worry too much about the security of data being transmitted across the network. But the government's recent decision to disband the BC Systems Corporation, which ran those operations, might have had detrimental effects if its security specialists, a team of approximately a dozen, were not kept intact within the Office of the Chief Information Officer.

In 1989 I raised the issue of data protectors' functioning as legitimizers of new forms of technology.<sup>42</sup> This issue continues to concern me. When the Ministry of Health asked for my advice about the Pharmanet prescription profile system, which it was fully determined to implement in any event, I insisted that everyone required to participate in the program (i.e., anyone wanting any prescription filled) should have the option of a password. When I finally needed to join Pharmanet myself, I learned that I was the first one to ever ask for a password at a certain busy pharmacy; the staff had to consult a manual to learn how to give me one. I fear that most participants have no idea that it is even possible to get a password with which to control access to their own prescription records.

We are having modest success in British Columbia in promoting the preparation of privacy impact assessments by public bodies introducing new forms of technology and new or significantly altered personal-information systems.<sup>43</sup> The Ministry of Health is a leader in this. When a proposal of this sort reaches my office with an accompanying impact statement, it is a considerable blessing from every perspective, including the protection of human rights, because the proponents have already thought about fair information practices at the design stage of whatever they are contemplating. We do not have the resources to prepare similar documentation except under duress in the course of crisis management.

### **Strengthening Data-Protection Legislation**

My office is preoccupied with its assigned tasks every day. For this reason, opportunities to look around and remember the big picture are built

into our work program. The professional members of the staff periodically go on one-day retreats. We regularly hold all-staff luncheons, at which a number of talented privacy specialists have spoken. And in 1996 we co-sponsored an international conference in Victoria on the theme of *Visions of Privacy for the 21st Century*.

Since the BC Freedom of Information and Protection of Privacy Act is typically general, we are encouraging public bodies to incorporate specialized fair information practices into revised legislation or regulations dealing with specialized activities.<sup>44</sup> I believe strongly that general principles should be incorporated in sectoral legislation, over time, as it is revised, so long as the privacy commissioner continues to have oversight of its detailed functioning.

A related matter is our ongoing effort to require privacy codes to be in place for those who collect or receive personal information on behalf of public bodies. Thus I am encouraging the Insurance Corporation of British Columbia to require a privacy code for its Autoplan agents, who insure all motor vehicles in the province. I am also concerned with ensuring that the thousands of service providers and contractors for the Ministry of Health and the Ministry of Children and Family Services implement fair information practices as required by the Freedom of Information and Protection of Privacy Act. The 1996 Model Privacy Code of the Canadian Standards Association is an ideal vehicle for additional self-regulation.

What remains problematic in British Columbia, despite the European Union's 1995 Directive on Data Protection, is an effort to extend data protection to the private sector. I still optimistically believe that the situation will change in the next several years, but I have to admit that my written and oral efforts to stimulate discussion of the matter have fallen on deaf ears to date.<sup>45</sup> The fact that Quebec became the first jurisdiction in North America to so legislate is, of course, encouraging. I wrote in 1989 that "statutory data protection is also essential for the private sector," and that "the long-term goal must be to ensure individual rights in all spheres of human existence." It was not practical to lobby the BC government on this score while the Freedom of Information and Protection of Privacy Act was being implemented in three tiers over three years; however, the reelection of the New Democratic government in 1996 presents new opportunities.

The Freedom of Information and Protection of Privacy Act is quite progressive, even by Canadian standards. It now extends to 33 self-governing bodies of professions or occupations, including the College of Physicians and Surgeons and the Law Society of British Columbia. I hope to encourage self-governing professional bodies to promote self-regulation among their members via privacy codes. I am also encouraging a review of the adequacy for the next century of the provisions respecting privacy in the BC Credit Reporting Act.

### **Toward the Future**

In 1989 I boldly asked what data-protection authorities would look like by the year 2000, which seemed far enough in the future that I would not have to face the consequences of what I wrote. I did not anticipate that I too would be in part responsible for that future vision, since my term ends in 1999. I raised the prospect that we would be perceived as “a rather quaint, failed effort to cope with an overpowering technological tide,” and I said it was self-evident that “data protection agencies will have to be vigilant, articulate, and resourceful in fashioning acceptable solutions in the public interest.”<sup>46</sup> Although I believe that my office has been vigilant and resourceful to date, I am less inclined now to draw an optimistic conclusion than I was in 1989, because of the ongoing explosion of the digital economy and online Internet services.

### **Acknowledgements**

I am grateful to the following colleagues: P. E. (Pam) Smith, Lorraine Dixon, and Kyle Friesen.

### **Notes**

1. David H. Flaherty, *Protecting Privacy in Surveillance Societies* (University of North Carolina Press, 1989).
2. *Ibid.*, p. 377.
3. *Ibid.*, p. 373.
4. *Ibid.*, p. 375.

5. *Ibid.*, p. 377.
6. See William A. Parent, Privacy: A brief survey of the conceptual landscape, *Santa Clara Law and Technology Journal* 11 (1995), no. 1: 21–26.
7. *Protecting Privacy in Surveillance Societies*, p. 8.
8. *Ibid.*, p. 380.
9. *Ibid.*, p. 379.
10. *Ibid.*
11. *Ibid.*, p. 380.
12. *Ibid.*, p. 406.
13. *Ibid.*, p. 383.
14. *Ibid.*, p. 383.
15. *Ibid.*, p. 383.
16. *Ibid.*, p. 384.
17. *Ibid.*, p. 384.
18. *Ibid.*
19. *Ibid.*, p. 385.
20. *Ibid.*, p. 386.
21. *Ibid.*, p. 387.
22. *Ibid.*, p. 387.
23. *Ibid.*, pp. 388–389.
24. *Ibid.*, p. 389.
25. *Ibid.*, p. 391.
26. *Ibid.*, pp. 41–44, 113, 260, 414.
27. *Ibid.*, p. 393.
28. *Ibid.*, p. 393.
29. *Ibid.*, p. 394.
30. *Ibid.*, pp. 394–395.
31. *Ibid.*, p. 395.
32. *Ibid.*, p. 396.
33. *Ibid.*, p. 397.
34. *Ibid.*, pp. 397–398.
35. *Ibid.*, p. 400.
36. *Ibid.*
37. *Ibid.*, pp. 401–402
38. *Ibid.*, p. 402.
39. *Ibid.*, p. 403.

40. Ibid.

41. See *ibid.*, p. 404.

42. *Ibid.*, pp. 403–404.

43. *Ibid.*, p. 405.

44. *Ibid.*, pp. 404–405.

45. *Ibid.*, p. 406.

46. *Ibid.*, pp. 406–407.