
The Informational Commons at Risk

Alasdair Roberts

Associate Professor,
School of Policy Studies and
Fellow, Open Society Institute
<http://www.aroberts.org>

Abstract. *Conventional wisdom says that we are on the cusp of a Global Information Society, in which new technologies will provide citizens with unprecedented access to information. This is an appealing but flawed vision of the future. Governments are still reluctant to disclose information about core functions. At the same time, neoliberal reforms have caused a diffusion of power across sectors and borders, confounding efforts to promote governmental openness. Economic liberalization has also made it more difficult to enforce corporate disclosure requirements. Meanwhile, technological change has spurred efforts by businesses and citizens to strengthen their control over corporate and personal information. Efforts to defend the borders of the “informational commons” — the domain of publicly-accessible information — will be also be complicated by problems of policy design and political mobilization. Imposing transparency requirements was easier when authority was closely held by national and sub-national governments. The task is more difficult when power is widely diffused.*

This paper will be published in Daniel Drache, ed., Recovering the Public Domain (London: Routledge). It is part of the Auditing Public Domains project of the Robarts Centre for Canadian Studies at York University: <http://www.robarts.yorku.ca>. Support for this research was provided by the Open Society Institute, New York.

Our first impression of the public domain is territorial. We imagine it as a space — an agora, square or commons — that is accessible to everyone as a right of citizenship, and in which important public business, such as the governance of the community, can be undertaken.¹ But the

public domain is obviously more than this. It also includes commonly-held intangibles without which the commons or agora would be unusable. These include a sense of shared identity and trust, as well as norms and rituals that regulate collective deliberations (Fukuyama 1995; Putnam

2000). There is another, critically important intangible: the pool of information about community affairs that must be publicly accessible for citizens to engage intelligently in the act of self-government. The territorial commons is paralleled by an ephemeral but equally important "informational commons," comprised of all the information that is accessible as a matter of right to all citizens.

Conventional wisdom says that the informational commons is broader than ever before. Technological improvements have given citizens an unprecedented capacity to retrieve government information, such as local crime statistics, the discharge records of local polluters, and test results for neighbourhood schools. They can download transcripts of that day's legislative hearings, the text of proposed laws, budget proposals from government departments, and policy analyses from non-government groups. Better communication technologies are said to give citizens and non-governmental organizations an unparalleled capacity to monitor the activities of governments and corporations anywhere in the world, often provoking government action or consumer boycotts to protect human rights (Giddens 2000: 144 and 154). And longstanding restrictions on distribution to information appear to have broken down. On the Internet, citizens violate copyright laws with impunity. Government's capacity to enforce secrecy laws seem to be undermined when sensitive documents are quickly replicated on websites the world over (Norton-Taylor and Pallister 1999; Loeb and Struck 2000).

This technological revolution has happened so quickly that we imagine it to be limitless. "Information wants to be free," the saying goes²; the pace of liberation depends only on our willingness to invest

in better hardware and fiber-optic cable. Our ultimate destination, leaders of the G8 nations announced in July 2000, will be a Global Information Society, in which improved access to information will "strengthen democracy, increase transparency and accountability in governance, promote human rights, enhance cultural diversity, and foster international peace and stability" (G8 2000). "Anyone with a modem," says Alan Murray, will be able to "gather nearly as much intelligence as the CIA" (Long 2000).

This is an appealing but flawed vision of the future. It overestimates the power of new technologies and ignores other trends that may actually restrict public access to information. The informational commons is contested terrain. Governments and corporations — and citizens themselves — have all taken steps to preserve secrecy, often spurred to do so by the power of new modes of surveillance, or by the desire to gain economic advantage by asserting their property rights over the central commodity of the new information economy.

The purpose of this chapter is to canvass current threats to the informational commons. It makes three broad points. First, there is no evidence that new information technologies have altered the willingness of governments to improve transparency for their most sensitive functions, such as policy formulation or law enforcement activities. Second, technological advances have been offset by neoliberal reforms that have reduced transparency, either by shifting power to private and supranational institutions, or by enabling corporate flight to jurisdictions with weaker disclosure requirements. Finally, the second-order effects of technological change have been neglected. Corporations and individuals are

already reacting to the impact of new technologies by strengthening legal and technical controls over information, thereby restricting the realm of publicly accessible information.

As our euphoria about the power of new information technologies fades, we will begin to see that the boundaries of the information commons are contested, and in some places have already receded. This should alarm advocates of strong democracy. The informational commons, as much as a territorial commons, is essential to self-government. But the fight to reclaim the informational commons will also be complicated by problems of policy design and political mobilization. Imposing openness codes was easier when authority was closely held by national and sub-national governments. The task is more difficult when power has diffused away from governments and across borders.

SECRECY AT THE HEART OF GOVERNMENT

Technological advances have led to dramatic improvements in public access to some kinds of government information. Documents that were once found only in legislative or depository libraries can now be quickly retrieved through the internet — at least by citizens who can afford the technology and understand the structure of government. But the improvement in openness is also qualified in another and more important way. The internet has transformed information that was already publicly accessible as a matter of principle, and made it accessible as a matter of fact. However, it has not caused governments to abandon old habits of protecting many key documents under the mantle of official secrecy.

Since 1997, advocates of governmental openness in the United Kingdom have

realized how much strength remains in the old doctrine of official secrecy. Britain is one of the few Commonwealth democracies that does not have a freedom of information (FOI) law, which establishes a legal right of access to some government documents. In Opposition, Britain's Labour Party repeatedly promised to adopt a strong FOI law as part of a broader program of constitutional modernization. A new law, party leader Tony Blair said in March 1996, would "end the obsessive and unnecessary secrecy which surrounds government activity" (Blair 1996).

After its election in May 1997, the Blair government began a retreat from its earlier commitments. A white paper released in December 1997 was hailed for its "surprisingly radical approach" (Frankel 1997); nevertheless, there were significant limits on the proposed new right of access to information. The new FOI law would not affect security and intelligence services, some defence functions, law enforcement functions of police and regulatory agencies, or legal advice to government. The burden of proof imposed on officials who wanted to withhold information would be less onerous if information related to "decision-making and policy advice processes in government" (United Kingdom 1997).

These restrictions were criticized in a May 1998 parliamentary review (Select Committee on Public Administration 1998), without effect. On the contrary, there was intense lobbying by key government departments for the FOI proposals to be further restricted or entirely abandoned. In July 1998, the minister who had developed the proposals was removed from Cabinet, and responsibility was given to the Home Secretary, who was known to favour a more limited law. A draft bill released in May 1999 would have denied

any access to information relating to policy development or information whose disclosure would “prejudice the effective conduct of public affairs.” The burden of proof on officials for most other exemptions to the right of access was also reduced (Home Office 1999). Despite continued criticism from parliamentarians, many of these restrictions were retained in a second draft bill introduced in the House of Commons in November 1999.³ The bill languished in Parliament, with growing speculation that it might not be adopted before the general election in 2001 (Jones 2000).⁴

The deficiencies of the British bill are matched in most of the Commonwealth FOI laws. Several, including the new Irish law, allow ministers to issue directives that prohibit any independent review of their decisions to withhold sensitive information.⁵ Among the restrictions in Canada’s FOI law are a broad ban on access to records relating to policymaking and management, as well as a limit on judicial review of decisions relating to sensitive state interests.⁶ The Chretien government has delayed on ministerial promises to undertake a review of the law,⁷ and opposed backbench efforts to broaden the ATIA (Bronskill 2000). It has also sought new restrictions on access to information. For example, the proposed Money Laundering Act will completely eliminate a right of access to much information held by a new law enforcement agency, the Financial Transactions and Reports Analysis Centre.⁸

In the United States, the end of the Cold War briefly seemed to provide an opportunity to reverse secrecy rules intended to protect national security. Shortly after his inauguration, President Clinton issued a memorandum to government departments directing them to “renew their

commitment” to the Freedom of Information Act (Clinton 1993), while Attorney General Janet Reno reversed a Reagan-era policy on interpretation of FOIA and urged departments to resolve thousands of backlogged requests (Reno 1993), Clinton also appointed a taskforce to review government policy on classified information. Heads of the Central Intelligence Agency and the Department of Energy (which operates the government’s nuclear weapons complex) promised to “come clean” with the public about their activities during the Cold War (Gruenwald 1993).

These efforts had a limited impact. Because FOIA administration is highly decentralized, Reno’s efforts to liberalize interpretation of the law and clean up backlogs had little influence. As new national security concerns arose at the end of the decade, defense and intelligence agencies lobbied for statutory amendments that would weaken FOIA by excluding many records from the law.⁹

Defense and intelligence agencies also succeeded in undermining proposals for reform of classification policies drafted by Clinton’s task force (Smith 1994; Weiner 1994). Nevertheless, an executive order signed by Clinton in 1995 did require federal agencies to declassify millions of pages of records from the Cold War era.¹⁰ However, implementation did not proceed smoothly. The Central Intelligence Agency claimed that budget cuts made it impossible to declassify old records quickly (Lardner Jr. 1998). Declassification efforts at the Department of Defense were also hampered by cutbacks (Aftergood and Blanton 1999). Conservatives alleged that the Department of Energy’s attempt to promote openness had encouraged espionage, prompting the department to adopt more meticulous procedures for

declassification of records (Department of Energy 2000). A recent executive order has extended the 1995 deadlines for declassification of old records.¹¹

The Clinton taskforce's proposed rules for classifying new records were also compromised by attacks from defense and security agencies. While the classification rules contained in the 1995 executive order are more liberal than the Reagan policy which they displaced, critics argue that the rules are more restrictive than the Carter administration's policy, which explicitly required agencies to balance the public's right to know against national security concerns (Quist 1989: Ch. 3). The Department of Energy also considered new rules that would limit the range of classified information, but these have been shelved because of worries about spying (Weeks 2000).

Senator Daniel Moynihan's experience in battling for openness provides evidence of the continuing power of the national security community. In 1994, Moynihan lobbied successfully for a special commission that would look for "a new way of thinking about secrecy" (Moynihan Commission 1997) in the post-Cold War era. The Commission eventually recommended a new Government Secrecy Reform Act that would codify and limit classification practices. The Clinton administration opposed the bill, arguing that it would restrict presidential discretion (Berger 1998), and it died in 1999.¹² Moynihan then introduced a more limited bill to encourage declassification of old records.¹³ It has also been weakened in response to administration concerns, and has not yet been adopted (Aftergood 2000). The Cold War has ended, Moynihan recently observed, but the "vast secrecy system ... shows no signs of receding" (Moynihan 1998: 214)

THE FRAYING EDGES OF GOVERNMENT

The historic tendency of governments to preserve secrecy for the most sensitive governmental interests has been aggravated by a second trend: efforts to restructure or "reinvent" national and sub-national governments. These restructuring efforts are part of a broader neoliberal reform program that is intended to limit the role of government in social and economic life. Restructuring is often presented as an unavoidable response to fiscal stresses. However, it also motivated by a desire to restore the "governability" of western democracies (Crozier, Huntington et al. 1975; Rose 1980), by restricting the capacity of citizens to exert influence over policy in key sectors. The erosion of information rights as a consequence of domestic governmental restructuring is neither temporary nor inadvertent: on the contrary, it is a critical part of the effort to make policy processes more manageable.¹⁴

One of the most prominent components of domestic neoliberal reform has been the privatization of state-owned enterprises. Privatization did not always erode information rights, since government practice in allowing access to records held by state-owned enterprises was mixed. (Canada, for example, usually excluded its crown corporations from its FOI law.) But in some circumstances, where state-owned enterprises delivered critical services or monopolized the market, information rights were recognized and consequently eroded through privatization. In Ontario, environmental advocates protested when the provincial utility, Ontario Hydro, was reorganized and largely privatized; while Hydro had been subject to provincial FOI law, its successors are not (Toronto Globe and Mail 1999). Similar complaints were voiced

when the Australia's federal government proposed the privatization of Telstra, the national telecommunications monopoly (Australian Law Reform Commission 1996: Para. 16.7), and its state governments privatized electricity, gas, and water utilities. After intense lobbying, the British government backed away from its 1997 proposal to include privatized utilities in its new FOI law. The current bill contains a weaker provision giving the Cabinet the discretion to include private organizations that perform a public function (Parker and Parker 1998; Milne 1999).

The increased popularity of contracting-out has also jeopardized information rights. Cash-strapped governments have outsourced "non-core" or ancillary activities for many years. More recently, they have broadened the scope of contracting, by enlisting the private sector to finance, build and operate major components of infrastructure. Britain's Private Finance Initiative (PFI) represents the most systematic effort at this sort of outsourcing. By December 1999, the government had signed more than 250 PFI contracts, initiating £16 billion of private investment in roads, hospitals, schools, prisons, government offices, and computer systems (Arthur Andersen and Enterprise LSE 2000). Canadian governments have also experimented with private financing, particularly in the transportation sector. An industry group says that these "public-private partnerships" will soon produce a "minor revolution" in the structure of Canadian government (Canadian Council for Public-Private Partnerships 1999).

No Canadian FOI law — and few laws in other jurisdictions¹⁵ — preserves a right of access to information when activities are transferred to private sector contractors. Governments could draft contracts to maintain information rights, but they have

no strong incentive to do so, and usually do not. Furthermore, citizens may be unable to obtain information that is held by government agencies that relates to the negotiation or management of those contracts. Although a citizen's right of access to this information persists, contractors have a countervailing right to insist on the withholding of commercial information provided in confidence to government. Contractors may also have a right to make a judicial appeal of government decisions to release contract information. Critics in many countries have complained that the power of contractors to delay or block the release of information weakens the ability of citizens to hold governments and contractors accountable for contract performance.¹⁶

Government's reliance on contractors is one aspect of the new "structural pluralism" (Giddens 2000: 55) that now typifies thinking about the organization of public services. Another is the proliferation of quasi-independent organizations that are established by government but which refuse to be described as governmental. Many of these organizations have corporatist governance structures, with boards that include representation from major client groups. Many are also excluded from FOI laws. In Canada, these include the new air traffic services corporation, Nav Canada; several new airport authorities; the St. Lawrence Seaway Management Corporation; the reorganized Canadian Wheat Board; Canadian Blood Services; the Canadian Foundation for Innovation; the Canadian Millennium Scholarship Foundation; and the Canada Pension Plan Investment Board. The British government has experimented with similar structures for its air navigation services. Several Canadian provinces have delegated regulatory functions to comparable quasi-independent agencies which

are also excluded from FOI law (Roberts 2000: 313).

Restructuring also affected access to government information in more prosaic ways. Fiscal retrenchment implied a reduction in “non-essential” spending within government; for many policy-makers, this included a reduction in resources dedicated to administration of FOI laws. The natural result was a lengthening in the time required to process FOI requests. Budget cuts also weakened offices responsible for enforcement of FOI laws, encouraging departments to engage in other forms of non-compliance, such as the unjustified withholding of information. In addition, governments increased the fees charged for processing FOI requests, sometimes with dramatic effect. In Ontario, fee increases that were justified as part of a broader effort to make government “more affordable and efficient” caused a thirty-five percent drop in FOI requests (Roberts 1999).

Governments also began raising fees for access to information that had previously been distributed at low or no cost. In the early 1980s, policymakers began to realize that the vast “data stockpile” held within government agencies could be exploited as a source of new revenues (Schiller 1989). In the United States, many federal agencies entered into partnerships with private firms to package and sell government information (Grossklaus 1991; Gellman 1995) (Kelley 1998). Recent attempts to introduce legislation that would regulate these partnerships and preserve public access to information were defeated after lobbying from the database industry (Prophet 1999). In Canada, federal agencies have sharply increased the price of information products or entered into licensing agreements that allow the private sector to sell gov-

ernment information (Morton and Zink 1991; Nilsen 1996: 7-8; Hubbertz 1999). “The concept of government information as a *corporate resource*,” says Kirsti Nilsen, “appears to be overriding the concept of public *rights* to that information” (Nilsen 1994: 205).

SUPRANATIONAL GOVERNANCE

The neoliberal agenda includes other reforms that have also impaired governmental openness. Efforts to liberalize international trade and capital flows have required the invention or elaboration of supranational institutions to serve as fora for policymaking and dispute resolution, and instruments for crisis management. These institutions often impose substantial constraints on policymaking by national and subnational governments; indeed, many critics suggest that these supranational institutions constitute an emerging system of global governance. At the same time, these institutions lack many of the structural features that have legitimized lower orders of government, including a comparable level of transparency. Indeed, the secretiveness of supranational institutions is frequently cited, even by proponents of economic integration, as one of the factors contributing to the “crises of legitimacy” afflicting supranational institutions.

Complaints about “secretive and autocratic” negotiations (Nader 1993) fuelled protests against the 1993 North American Free Trade Agreement and contributed to the eventual defeat of a Clinton administration proposal to renew “fast track” negotiating authority in November 1997. The next year, similar complaints led to the abandonment of negotiations over a new treaty on the treatment of foreign direct investment. Formal discussions on the proposed Multilateral Agreement on

Investment (MAI) began within the Organization for Economic Cooperation and Development (OECD) in May 1995, but attracted little publicity until non-governmental organizations obtained a confidential negotiating text in January 1997. Protests against the treaty and the “veil of secrecy” (AAP Newsfeed 1998) that had cloaked negotiations erupted worldwide. The OECD attempted to rebut the complaints, meeting directly with non-governmental organizations and delaying MAI talks to allow “further consultation between the negotiating parties and interested parts of their societies” (Financial Post 1998). But these belated attempts at transparency proved ineffective, and negotiations were formally abandoned in October 1998.

Protestors at the World Trade Organization’s Seattle conference in November 1999 launched similar complaints about secrecy. The WTO, which is responsible for enforcement of trade rules adopted after the Uruguay Round negotiations, adopted a code on access to information shortly after its establishment in 1995, but it had many limitations. Chief among these was the exclusion of documents produced within the WTO’s dispute settlement procedures, including submissions by nations involved in a dispute and preliminary decisions by WTO panels. In addition, non-governmental organizations were barred from observing or reading transcripts of hearings on trade disputes (Debevoise 1998). The rules, Ralph Nader complained in 1996, meant that important trade policy decisions were made “a group of unelected bureaucrats sitting behind closed doors in Geneva” (Nader and Wallach 1996, p. 94).

By Fall 1999, governments of many advanced economies had recognized that these complaints were undermining the

credibility of the trade regime among their citizens. The United States called improved openness “a priority issue,” conceding that “transparency in the operation of the WTO itself has become a critical factor in ensuring the long-term credibility of the multilateral system” (United States Trade Representative 1998, p. 37; U.S. Mission 1999). But the Seattle meeting did not produce agreement on reforms to improve transparency. Many nations — including several developing economies — oppose the American proposals, arguing that they would subject the WTO to undesirable “external non-legal pressures” and destabilize its dispute settlement procedures (WTO General Council 1998; Raghavan 2000).

The International Monetary Fund (IMF) also suffers legitimacy problems that are rooted in perceptions of excessive secrecy. There is an irony in such criticisms, because the IMF is itself a mechanism for promoting access to information: It facilitates international economic policy coordination through its surveillance of domestic policy decisions by member countries (Pauly 1997).¹⁷ But the IMF also plays a growing role in providing conditional aid to nations with balance of payments difficulties and in managing global financial crises. Observers on both ends of the political spectrum attacked the Fund for its response to the East Asian financial crisis that began in Summer 1997, and related crises in Russia and Brazil. Joseph Stiglitz, chief economist of the World Bank during the crisis, later said that “excessive secrecy” had allowed the Fund to pursue indefensible policies (Stiglitz 2000: 60). In 1998, Conservatives in the U.S. Congress, frustrated by their inability to obtain internal reports that were said to be critical of the IMF’s handling of the crisis, refused to provide \$18 billion in emergency aid for the Fund

(Saxton 1998). The impasse was resolved in October 1998, when the IMF agreed to release some key documents on lending activities and policy changes.¹⁸

However, there are clear limits to the IMF's willingness to improve transparency. Some members of Congress unsuccessfully advocated broader disclosure requirements, with stronger mechanisms for ensuring compliance.¹⁹ Since 1998, legislators have also attempted without success to tie U.S. support to disclosure of IMF operating budgets and improved financial statements.²⁰ The IMF regards the disclosure of staff reports relating to the Fund's surveillance function as a experiment, undertaken only with the consent of countries whose policies are being reviewed (International Monetary Fund 1999). The IMF's managing directors have warned that it is accountable only to the governments of its member countries, and that increased openness will require a consensus among those governments (Camdessus 1998; Köhler 2000: 260).²¹

Another effort at economic integration — the European Union — has also been hobbled by complaints about the secretiveness of its main institutions. Such complaints contributed to the rejection of the Maastricht Treaty by Danish voters in June 1992, and more recently to the attempt by the European Parliament to censure the European Commission in January 1999, and the eventual resignation of the Commission in March 1999 (Guardian 1999). Attempts to improve transparency have had limited impact. An administrative FOI code adopted in December 1993²² is widely thought to be ineffective; disagreements among the Union's member nations about appropriate levels of transparency have led to delays and inconsistent decisions. A commitment to stronger FOI rules was

included in the 1997 Treaty of Amsterdam. However, a draft of the proposed new rules prepared by the Commission and released in January 2000 has been heavily criticized. The EU Ombudsman says the proposed rules contain "a list of exemptions without precedent in the modern world" (Söderman 2000).

CORPORATE CONTROL OF INFORMATION

The achievement of an open society does not depend only on improved access to government information. It also depends on appropriate rules to regulate access to information that is controlled by the private sector. Some observers have suggested that corporate control of information is weakening, primarily because of the impact of new technologies. They note that intellectual property law, which gives corporations the capacity to restrict dissemination of information, has been undermined. At the same time, governments have begun using the internet to disseminate information collected from the private sector through regulatory processes.

There are two major difficulties with this argument. The first is its inattention to the second-order effects of technological change — that is, the ways in which corporations react to technological change by finding new ways of controlling the flow of information. The second is its inattention to the impact of neoliberal reforms on the capacity of governments to impose disclosure requirements on the private sector.

In Summer 2000, the high-profile Napster lawsuit seemed to provide further evidence of the "crisis in intellectual property" (Barlow 1994) that had been caused by advances in information technology. The Recording Industry Associa-

tion of America claimed that Napster software encouraged copyright violation by allowing individuals to retrieve music from other personal computers. Although courts supported the RIAA's attempt to block Napster, many other "peer-to-peer computing" programs designed to evade legal challenges quickly emerged to replace it (Berman 2000).

The severity of this "crisis" can be overstated.²³ In fact, industries that rely heavily on intellectual property have attained significant improvements in legal protection over the last decade. One of the most notable gains has been through the expansion of international trade agreements to include provisions for strengthening intellectual property rights, particularly in developing world, where patent and copyright laws have been less stringent or weakly enforced. The 1994 Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) compels nations to adopt intellectual property standards comparable to those in the United States and some other developed nations. Furthermore, it allows governments to use the World Trade Organization's dispute settlement procedures to impose trade sanctions on nations that fail to comply (Long 2000).²⁴

Even in the United States, legal protection has been improved in response to the perceived threat from new technologies. The 1998 Digital Millennium Copyright Act (DCMA) makes it an offence for citizens to break software or hardware "locks" that restrict access to information distributed in digital form, even if the consumer's use of that information would normally be considered a fair use under copyright law (Benkler 1999: 419-420). The Motion Picture Association of America recently relied on the DCMA to block dissemination of software that would

break the encryption system on digital versatile disks (DVDs). The court conceded that its judgement prevented some fair uses of material on DVDs (U.S. District Court for the Southern District of New York 2000: 49). Another judgement allowed the on-line auctioneer EBay to invoke the common law of trespass to restrict efforts to collect information on its website (U.S. District Court for the Northern District of California 2000). The U.S. Congress is also considering legislation that would prohibit extraction of non-copyrighted information from databases if it harms the commercial value of a database.²⁵

These legal protections will soon be complemented by technical improvements that give producers of intellectual property more control over the use of their products. These new digital-rights-management (DRM) systems include software and hardware designed to enhance the value of digital data by impairing the capacity of consumers to reproduce or manipulate information (Economist 1999; Solomon 2000). Commentators have suggested that DRM systems will eventually displace copyright law as the principal method of regulating the use of information (Lessig 2000: 126-127). The influence of DRM systems will be felt more heavily as print is supplanted by new technologies as the dominant form of information distribution.

Advocates of the information society suggest a second reason why corporate control of information might be weakening: because of the improved capacity of governments to disseminate information collected through regulatory processes over the internet. For example, residents of the United States can now easily retrieve information about the use of toxic chemicals by industries in their neigh-

bourhood; the information is collected and distributed through an online database — the Toxics Release Inventory — maintained by the Environmental Protection Agency.²⁶ In fact, many students of regulation have begun to argue that disclosure of this sort of information can be a simple but effective tool for regulating corporate conduct (Johnson and Beaulieu 1996). The publication of information about business practices enables communities to mobilize for political action and has a sharp impact on investors' assessment of the value of firms (Fleming 1983).

For these reasons, improved access to information can also spawn a powerful backlash from affected industries. The distribution of TRI data over the internet caused "spasms" in the chemical industry, which engaged in court action and political lobbying to thwart proposals to broaden the TRI database (Fairley 1997; Fairley and Mullin 1998).²⁷ The conflict over TRI is only one of several battles waged by U.S. industry to restrict the flow of environmental information. Businesses have also resisted implementation of an EPA pilot project to create online risk profiles of major industrial facilities (Fairley 1997)²⁸; lobbied law enforcement and intelligence agencies to block the EPA's proposal to publish their crisis management plans, arguing that the plans would be misused by terrorists (Matthews 2000); and sought new restrictions on access to internal audits of compliance with environmental laws.²⁹

The capacity of businesses to resist disclosure requirements has been enhanced as a result of economic liberalization. If the government of one jurisdiction is reluctant to shield industries from requirements to release information, it is easier than ever before for industries to

relocate to jurisdictions whose governments will be less demanding.

The phenomenon of interjurisdictional flight is not new. Within the United States, Delaware is a home for many businesses partly because of its weak rules on disclosure of information on corporate governance. Recently, the Russian mafia was alleged to have exploited Delaware's corporation law to cloak an elaborate moneylaundering scheme (Village Voice 1999). A more dramatic illustration of the potential danger of interjurisdictional flight is provided by the burgeoning speculative prison industry. Speculative prisons are built by private operators to house prisoners from other states whose own prisons are overcrowded. Because there is no contractual relationship between prison operators and governments of the states in which they operate, there is no guarantee that governments or citizens will have access to information relevant to public safety, such as the number or classification of inmates, staffing policies, or emergency response plans. Attempts by state legislatures to impose disclosure requirements are often met with threats to relocate facilities — threats that are compelling to the economically disadvantaged jurisdictions in which such prisons are typically located (Collins 1999).³⁰

Economic liberalization has already encouraged business flight across national borders, to countries whose incorporation and banking laws contain weaker disclosure requirements. In 1998, the OECD argued that transnational flight of "geographically mobile activities, such as financial or other service activities" posed an urgent challenge for governments of the developed nations, because of increased risk of tax evasion or money laundering (OECD 1998: 9, 24). It recently

issued a blacklist intended to encourage reform by nations that were judged to engage in “harmful tax practices,” including inadequate levels of corporate disclosure (OECD 2000). In addition, the G7 nations operate a task force on money laundering that pressures “non-cooperative countries” for reform (Financial Action Task Force 2000). The OECD and G7 nations have also attempted to pressure nations whose lax disclosure requirements are said to aggravate global financial instability.³¹

Disclosure requirements for other sectors might also be eroded as a consequence of liberalization. Environmental groups have protested that trade liberalization will encourage industry flight to nations with weaker rules on environmental protection, initiating a global “race to the bottom” on environmental standards.³² Labour unions have complained that liberalization has undermined their ability to monitor working conditions in factories that produce apparel and other consumer goods for the advanced economies; they have called for new programs to compel disclosure of factory locations and audits of working conditions (Bernstein 1999).³³ Persuading western governments to take coordinated action that will improve transparency in these areas may be difficult: there is no immediate and concrete threat to their interests, comparable to the threat posed by tax evasion or economic instability, that outweighs their reluctance to intrude on the sovereignty of other nations.

HYPER-PRIVACY?

Individual citizens can also encroach on the boundaries of the informational commons. Much of the information that communities use in the process of self-governance is *personal* information — that is, information about another identi-

able individual³⁴ — or is constituted of knowledge derived through the manipulation of aggregated personal information by researchers or administrators. However, the right of access to personal information is now being strictly limited, as citizens assert a countervailing right to privacy.

The movement to strengthen legal protection for personal information is, in part, another second-order effect of technological change. It has been given momentum by fears about the ability of businesses to use new technologies, including web-based commerce, to collect and manipulate consumer information³⁵, and by fears about the improved surveillance capacity of law enforcement and intelligence agencies.

The movement is not purely a reaction to technological change. It is also part of a larger, decades-long effort to obtain legal recognition for an array of basic rights, and a concomitant tendency to use “rights discourse” to frame policy discussions (Glendon 1991). A right to privacy is included within in the United Declaration of Human Rights, the International Covenant on Civil and Political Rights and several other international and regional treaties. Many national constitutions also recognize the right to privacy (Fleming 1983). The privacy movement is also bolstered by the steep long-term decline in popular trust of major governmental and private institutions (Etzioni 1999: 75-102).

Fears about the loss of privacy are often justified. However, the doctrine of personal privacy can also be employed in unexpected ways, often with significant social costs.

One of these unintended effects may be a restriction in the public’s capacity to

oversee the conduct of government agencies. Traditional arguments about the need to protect sensitive governmental interests can now be bolstered by new arguments about the need to protect the privacy of officials within public agencies. For example, the mayor of a Quebec City suburb recently declined to release details of her expense claims, arguing that this would violate her personal privacy; Quebec's information commissioners supported the mayor's decision (Cobb 1999). Earlier, the Canadian Department of Finance cited privacy concerns as the reason for its refusal to release sign-in logs for its employees; the information was only released after a slim majority of the Supreme Court of Canada rejected the department's arguments (Supreme Court of Canada 1997). The Nova Scotia Court of Appeal recently upheld a government decision to deny a request by a patient of a provincial drug treatment facility for records of the investigation into her allegations of sexual assault, arguing that it would invade the privacy of the employee who was the subject of the allegations (Cahill 1999).

The tension between accountability and privacy is felt in other countries as well. In Europe, human rights organizations have complained that new privacy laws may compromise their ability to report on allegations of human rights violations by police and security forces (HURIDOCS 1993). In March 2000, the Spanish Association Against Torture was investigated for privacy abuses after it published names of prison officials who were alleged to have committed acts of torture (Nodo 50 2000). In the United States, senior federal judges recently resisted public disclosure of their conflict-of-interest statements, claiming that internet publication of the statements would violate their privacy (Pringle 2000).

Privacy claims may infringe on public accountability in other ways. Under proposed amendments to French criminal law, the media would be prohibited from showing pictures of a person wearing handcuffs before conviction, as well as crime scene photos that would "harm the dignity of the victim" (Guerrin 2000). The French proposals exemplify a growing ambivalence about the openness with which judicial proceedings have typically been conducted. Some U.S. courts are considering new restrictions on access to court case files, noting that personal information that had once been "practically obscure" might now be easily retrieved over the internet (AOUSC 1999). In Canada, the federal government promised to reconsider its policy of publishing employment insurance appeal decisions on the internet after legislators complained about the violation of personal privacy.³⁶

The unwillingness of citizens to surrender personal information has also been evidenced in popular protests against national censuses. The most dramatic protests occurred in West Germany in 1987, when census-taking was marred by mass protests and rioting (Fleming 1983). Before the 2000 U.S. census, libertarians appealed to citizens to "strike a blow for privacy" by refusing to answer census questions (Sylvester 2000). Senior Republicans suggested that citizens would be justified in ignoring census questions, and the U.S. Senate called on the Census Bureau to ensure that citizens would not be "prosecuted, fined or in anyway harassed for failure to respond."³⁷ Recent Canadian censuses have provoked protests as well (Privacy Commissioner 2000: 49-56). The federal government is planning a public relations effort to "proactively deal" with privacy concerns before the 2001 census, including a

reminder about penalties for non-compliance (Statistics Canada 2000).³⁸

In early 2000, worries about privacy triggered an extraordinary public protest against the Longitudinal Labour Force File (LLFF), a database built by policy analysts within the federal Department of Human Resources Development for research on departmental programs. The database combined information from several other sources, including federal tax returns, unemployment insurance files, and federal pension files. The database conformed with requirements of the federal Privacy Act, which regulates the use of personal information by government, and there was no evidence of misuse by officials. Nevertheless, Canada's Privacy Commissioner protested that the LLFF was "a citizen profile" that could easily be abused by government (Privacy Commissioner 2000: 64-70). Prodded by the media, more than forty thousand citizens submitted requests for personal information contained in the LLFF. Within weeks, the database had been dismantled. The government later promised a review of the Privacy Act (McLellan 2000).

The potential conflict between demands for privacy and the public interest in sound management of government programs is also evident in debates over the use of personal health information. In Canada, healthcare consumes about ten percent of national income. Governments and researchers argue that their capacity to assess the effectiveness of health programs, and new treatments and technologies, may be undermined if tight constraints are put on the use of personal health information. Rules that require explicit consent to these secondary uses of information might prove administratively cumbersome. Individuals might also deny consent for secondary uses of their

health information, undermining the reliability of databases and results that are drawn from them (Lowrance 1997).

The controversy over Canada's new Personal Information Protection and Electronic Documents Act³⁹ was largely grounded in disagreements about the limits that should be put on use of personal health information. The bill proposed by the federal government required many healthcare organizations to obey strict rules on the use of personal information. Provincial governments, which operate Canada's healthcare systems, argued that the rules should not apply to organizations who collect and use information for "the purposes of health research or management of the health system" (Lindberg 1999).⁴⁰ Parliament eventually gave health organizations a one-year reprieve, with the expectation that provincial governments would use the time to develop their own policies for the handling of personal health information. Several provinces have now drafted health information laws, provoking the same debate about the balance between private and public interests.⁴¹

The controversy transcends national borders. Critics say that a recent Australian privacy bill is also "too generous in relation to management and research uses without consent" (Australian Privacy Charter Council 2000). The U.S. government has proposed new privacy standards for health care providers that would allow disclosure of personal health information without explicit consent for "health care operations" and for some "national priority purposes" such as research or public health. The proposed rules have been heavily criticized by privacy advocates who argue that a citizen's "right to choose" should trump "governmental or national purposes" (Sobel 2000).

Amitai Etzioni worries that a desire to achieve “hyper privacy” may also compromise the ability of government agencies to investigate crimes and protect national security (Etzioni 1999: 75-102). In the United States, privacy advocates have successfully resisted efforts by federal agencies to create “backdoors” in new technologies that would allow surveillance (Sykes 1999: 167-182) and limit availability of strong encryption technologies, such as the software program Pretty Good Privacy (Garfinkel 1995: 109-112). An attempt by the Federal Bureau of Investigation to adopt new technology for monitoring e-mail communications has also been delayed because of privacy concerns (Schwartz 2000).⁴² The British government was harshly criticized for adopting a new law that would authorize similar initiatives to improve surveillance by law enforcement agencies.⁴³

For libertarians, the challenge to governmental capabilities that is posed by hyper-privacy is not problematic. On the contrary, libertarians recognize that the expansion of government responsibilities in the post-war period depended in large part on improved capacity to collect and manipulate information from citizens. Restricting that capacity becomes one method of restricting government’s role (Southeastern Legal Foundation 2000).⁴⁴ But most citizens in the advanced democracies do not take so consistent a position: distrust of government is matched by a desire for continued governmental activism, and an impatience with badly managed public spending.⁴⁵ For these citizens, the insistence on very strong privacy protections is less defensible.

PROTECTING THE INFORMATIONAL COMMONS

In the last twenty years we have witnessed a dramatic improvement in infor-

mation and communication technologies. On its own, this technological revolution might seem likely to lead us to an era of unprecedented broadening of the informational commons, and the emergence of a true “global information society.” But this would be a misguided view, for two reasons.

First, we have not yet realized the second-order effects of technological change. The fact that new technologies allow easier access to information will lead to a reappraisal of what sort of information ought to be contained within the informational commons. The struggle to adopt stronger protection for personal information, partly driven by a fear of what new technologies can do, is one such second-order effect. So, too, is the attempt by businesses to eke profits out of new technologies by strengthening their legal and technical control over information. These second-order effects will qualify the improvements in access initially provided by technological improvements.

In addition, there are other powerful social changes that must be accounted for. Fiscal stresses, and the rising popularity of neoliberal politics, have led to profound changes in the structure of our governments. A world economy, distinguished by freer trade and improved capital mobility and regulated by a new superstructure of financial and trade institutions, has emerged. Citizens have become more adept in demanding protection for basic human rights, including the right to privacy. These other social changes may also shrink the boundaries of the informational commons, offsetting the gains realized by technological change.

As a consequence, the struggle to broaden the information commons is far

from over. Indeed, there is good reason to think it may become even more difficult, again for two reasons. First, the task of designing policies to promote openness is likely to become more complex. In the big-government, pre-globalization era, the task of designing policies that improved access to information was straightforward. Many critical functions were performed by a relatively homogeneous group of organizations directly owned and controlled by government. The result was that one regulatory tool — the comprehensive FOI law — could be highly effective in promoting openness.

This no longer holds true. Social power has slowly leaked away from governments. It has diffused among an array of private, quasi-private, and governmental bodies, some of which are wholly contained within single jurisdictions, and some of which span jurisdictions. Heterogeneity is the order of the day. Old FOI laws no longer seem to cover the most important loci of social power. Indeed, it is difficult to imagine how a single law could be drafted to fit the diverse range of entities that have replaced big government.

Accompanying this problem of policy design are new difficulties in building coalitions that are powerful enough to push for adoption of policies that promote openness. It was once easy to build an alliance of citizens, businesses and non-governmental organizations, all of whom shared a common interest in foisting strong openness rules on big government. But it is harder to build powerful alliances when power has diffused, and members of the old coalition — citizens, businesses, or non-governmental organizations — are transformed into the objects of regulatory action. Coalition-building is also complicated

when power is transferred to supranational institutions, and effective campaigns for openness require cross-border coordination.

In short, the informational commons is still contested terrain, and there is no assurance that its advocates will muster forces adequate to preserve its borders. Nevertheless, the struggle for an informational commons remains crucially important. The right to self-government — which is itself a basic human right⁴⁶ — means little if citizens lack the information needed to make intelligent decisions. If the informational commons is not protected, we may eventually confront a paradox: we have acquired an unprecedented technical capacity to engage each other in collective deliberations, but lack the raw material needed to deliberate well.

Notes

¹ For example, Kunstler defines the public realm as “pieces of terrain left between private holdings” (Kuntsler 1996). In this volume, Daniel Drache observes that the public domain is often thought to be “synonymous with the public park, the skating rink, the local library, music halls, art galleries, bus and subway routes, and the local post office” (Drache forthcoming).

² The phrase was first used by Stewart Brand, a cofounder of the Well, one of the first online discussion fora.

³ Freedom of Information Bill, Bill 5 of Session 1999-2000.

⁴ British governments have also been vigorous in their use of the Official Secrets Act to discourage the publication of information by former officials. Stephen Dorril observes that “Labour politicians . . . have been easily seduced by the magic of

secrecy and privileged access to special sources" (Dorril 2000: 758-800)

⁵ The Australian and New Zealand laws also include provisions for ministerial certificates.

⁶ Access to Information Act, R.S.C. c. A-1, ss. 21, 50 and 69.

⁷ Justice Minister Allan Rock promised a review in 1994 (Calamai 1994). His successor Anne McLellan made a similar commitment in March 2000 (Durkan 2000). In August 2000, McLellan announced that an internal committee had been set up to review the law (McLellan 2000), but this was regarded skeptically by many observers.

⁸ Proceeds of Crime (Money Laundering) Act, Bill C-22, 36th Parl., s. 55.

⁹ The current defense authorization bill would exclude operational files of the Defense Intelligence Agency, as well as unclassified information provided by foreign governments: S. 2549, 106th Cong., ss. 1044-45. The proposed Cyber Security Information Act of 2000, HR 4246, 106th Cong., would exclude information collected from the private sector relating to potential "cyber attacks" on critical infrastructure.

¹⁰ E.O. 12958, April 17, 1995.

¹¹ E.O. 13142, November 19, 1999.

¹² The Government Secrecy Reform Act was introduced as S. 712, 105th Cong. It was re-introduced as S. 22, 106th Cong.

¹³ Public Interest Declassification Act, S. 1801, 106th Cong. Introduced in October 1999.

¹⁴ In addition to FOI laws, governments adopted several other instruments to promote public accountability in the post-war period, including administrative

procedures laws, ombudsmen and special commissioners, public consultative mechanisms, and interest group funding. Many of these instruments have also been limited as a consequence of governmental restructuring.

¹⁵ The Irish FOI law is one of the exceptions. Some U.S. state laws also maintain a right of access.

¹⁶ Canadian experience is briefly described in (Roberts 2000). For a sense of the Australian debate, see: (Administrative Review Council 1997). For the American debate, see: (Fitzgerald 1995; Bunker and Davis 1998). For a view of the British debate, see: (Campaign for Freedom of Information 1994).

¹⁷ The same might be said of the World Trade Organization, whose Trade Policy Review Mechanism serves a comparable surveillance function (Hoekman and Mavroidis 1999).

¹⁸ The conditions were stipulated in the Omnibus Appropriations Act, PL105-277, passed by Congress on October 21, 1998. Executive Directors representing the major donor countries agreed to implement similar reforms in a memorandum to the IMF Managing Director on October 30, 1998.

¹⁹ See IMF Transparency and Efficiency Act, HR 3331, 105th Cong., and: (Saxton 1998).

²⁰ Debt Relief and IMF Reform Act of 1999, HR 2939, 105th Cong. (September 1999); IMF Reform Act of 2000 (H.R. 3750, 105th Cong. (February 2000). See also HR 3425, 105th Cong., section 504, which was adopted by reference in the FY Omnibus Appropriations Act, PL 106-113.

²¹ These comments give a hint of the broader question underlying the debate over transparency of the WTO and the IMF: can these organizations be "democratized," through the recognition of certain rights

given directly to citizens, and exercised through non-governmental organizations; or must they remain as "bureaucratic bargaining systems," in which procedural rights are given only to participating governments? (Dahl 1999).

²² Council Decision 93/731/EC.

²³ Practical difficulties may also undermine Napster (Adar and Huberman 2000; Greenman 2000).

²⁴ For a discussion of the impact of TRIPS in Latin America, see: (Correa 2000).

²⁵ Collections of Information Antipiracy Act, H.R. 354, 106th Cong. See also: (Benkler 1999: 440-446).

²⁶ The Toxics Release Inventory (TRI) was established by the Emergency Planning and Community Right-to-Know Act of 1986, 42 USC 11023. For an illustration of how environmental activists have used the database, see <http://www.scorecard.org>.

²⁷ The most recent legislative proposal is Rep. Waxman's Children's Environmental Protection and Right to Know Act, H.R. 1657, 106th Cong.

²⁸ The plan is known as the Sector Facility Indexing Project. A modified database went online in May 1998.

²⁹ See the Environmental Protection Partnership Act, S. 1661, 106th Cong. Many states have adopted comparable "audit privilege" laws (Koven 1998; Arlen and Kraakman 2000).

³⁰ State legislators complained that they were "stonewalled" by the Corrections Corporation of America after a mass escape from its Youngstown, Ohio facility in 1998 (Morse 1998).

³¹ The OECD has established a Task Force on Corporate Governance (OECD 1999: 3), while the G7's Financial Stability Forum has established a Working Group on Offshore Centres (Financial Stability Forum 2000: 1).

³² However, there is no clear evidence that such flight has occurred. See: (Jaffe and Peterson 1995; Neumayer 2000).

³³ Labour unions have been supported by a coalition of student groups and other non-governmental organizations (Klein 2000: 343 and 409; Lee and Bernstein 2000). This coalition may provide a model of how effective movements for transparency can be established in a world in which power has diffused across national borders.

³⁴ For a review of the definitions used in Canadian privacy laws, see: (McNairn and Woodbury 1998: 7(2)(a)).

³⁵ See: (Garfinkel 2000). The depth of public concern was illustrated in Fall 1999, when the American firm DoubleClick announced that it intended to combine its own databases, containing data on internet surfing habits, with recently purchased databases containing the purchasing histories of 88 million U.S. households. DoubleClick eventually retreated from the plan (Tynan 2000: 106).

³⁶ See Hansard, May 31, 2000.

³⁷ H.Con.Res. 290, 106th Cong., section 344.

³⁸ A related question is whether historians and other researchers should have access to returns from earlier censuses. Statistics Canada has resisted researchers' requests for access to returns from the 1906 and 1911 censuses, arguing that disclosure would breach promises of confidentiality made by the government at that time. The

Privacy Commissioner has endorsed this position (Privacy Commissioner 2000: 49-56). A preferred approach, privacy advocates claim, is the eventual destruction of census records.

³⁹ Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5. The Act received royal assent in April 2000.

⁴⁰ The Canadian Healthcare Association, representing hospitals and other healthcare agencies, took a similar position.

⁴¹ Alberta's Health Information Act allows the use of personal information without consent for internal management and policy development, and authorizes disclosure without consent to the provincial government for "health system purposes." Critics complain that law "destroys the right to information privacy" by giving citizens' records "people they do not know and for purposes for which they have never given consent" (Alberta Liberal Caucus 1999). Ontario's draft Personal Health Information Protection Act has also been derided as "an access bill, not a privacy bill" (Public Interest Advocacy Centre 2000).

⁴² The technology, named Carnivore, is being reviewed by Congress. Another FBI program named Digital Storm — which would employ "data mining" techniques to improve monitoring of telephone and cellular calls — has also proved controversial.

⁴³ The Regulation of Investigatory Powers Act (UK) 2000 c. 23, became law in July 2000. Another object of criticism has been the Council of Europe's proposed International Convention on Crime in Cyberspace, which would commit governments to developing methods of accessing computer systems for criminal investigations: (Blumner 2000).

⁴⁴ For a more general statement of the libertarian position, see: (Murray 1997).

⁴⁵ A recent U.S. survey found that nearly half of its respondents regarded their national government as a threat to their personal freedom; at the same time, a majority advocated an expansion of federal responsibilities in many areas (NPR 2000).

⁴⁶ See Articles 19 and 21 of the United Nations Declaration of Human Rights.

Works Cited

AAP Newsfeed (1998). Fischer defends negotiations after Mason criticism. *AAP Information Services Pty. Ltd.* Canberra. March 3, 1998.

Adar, Eytan and Bernardo Huberman (2000). *Free riding on Gnutella*. Palo Alto, CA: Xerox Palo Alto Research Center. August 2000.

Administrative Review Council (1997). *The Contracting Out of Government Services: Access to Information*. Australian Government Printing Service. February 1997. Issues Paper.

Aftergood, Steven (2000). E-mail: Moynihan bill on declassification. Listserv: foi-l@listserve.syr.edu. June 7, 2000.

Aftergood, Steven and Tom Blanton (1999). The securocrats' revenge. *The Nation* (August 9-16, 1999): 20.

Alberta Liberal Caucus (1999). *News release: Albertans' right to privacy degraded by Klein*. Edmonton: Alberta Liberal Caucus. December 10, 1999.

AOUSC (1999). *Privacy and access to electronic case files in the federal courts*. Washington, DC: Administrative Offices of the United States Courts, Office of Judges Programs. December 15, 1999.

- Arlen, Jennifer and Reiner Kraakman (2000). When companies come clean: Mitigation is better than environmental audit privileges. *Business Law Today* 9.3 (January-February 2000): Web edition.
- Arthur Andersen and Enterprise LSE (2000). *Value for Money Drivers in the Private Finance Initiative*. London: Private Finance Initiative Treasury Taskforce. January 26, 2000.
- Australian Law Reform Commission (1996). *Open Government: A Review of the Federal Freedom of Information Act 1982*. Canberra: Australian Law Reform Commission. Report no. 77.
- Australian Privacy Charter Council (2000). *Submission on Privacy Amendment (Private Sector) Bill 2000 to the House of Representatives Committee on Legal and Constitutional Affairs*. Canberra: Australian Privacy Charter Council. May 2000.
- Barlow, John Perry (1994). The economy of ideas. *Wired* 2.3 (March 1994): Web edition.
- Benkler, Yochai (1999). Free as the air to common use: First Amendment constraints on enclosure of the public domain. *New York University Law Review* 74.2 (May 1999): 354 et seq.
- Berger, Samuel (1998). Letter to Rep. Lee Hamilton on S. 712, the Government Secrecy Reform Act. Washington, DC: National Security Council. September 17, 1998.
- Berman, Dennis (2000). With technology like this, who needs Napster? *Business Week* 3694 (August 14, 2000): 121.
- Bernstein, Aaron (1999). Sweatshop reform. *Business Week* 3627 (May 3, 1999): 186.
- Blair, Tony (1996). Speech at the Campaign for Freedom of Information annual awards ceremony. London: Campaign for Freedom of Information. March 25, 1996.
- Blumner, Robyn (2000). Cyberfear leading to international invasion of privacy. *Milwaukee Journal Sentinel*. Milwaukee, Wisconsin. June 6, 2000. 17A.
- Bronskill, Jim (2000). Senior Liberals shoot down broader Access Act. *Ottawa Citizen*. Ottawa. June 7, 2000. A3.
- Bunker, Matthew and Charles Davis (1998). Privatized government functions and freedom of information. *Journalism and Mass Communication Quarterly* 75.3: 464-477.
- Cahill, Barry (1999). Are freedom of information and protection of privacy mutually exclusive? A comment on Dickie. *Government Information in Canada* 19 (October 1999): Web edition.
- Calamai, Peter (1994). Not necessarily between a Rock and a hard place. *Media* 1.2 (July 1994): 28.
- Camdessus, Michel (1998). Remarks to the World Affairs Council. Philadelphia, PA: International Monetary Fund. November 6, 1998.
- Campaign for Freedom of Information (1994). *Proceedings of a seminar on commercial confidentiality*. London: Campaign for Freedom of Information. October 18, 1994.
- Canadian Council for Public-Private Partnerships (1999). About the Canadian Council for Public-Private Partnerships. Web: <http://www.inforamp.net/~partners>. Accessed: March 31, 1999.
- Clinton, William J. (1993). Statement of the President regarding implementation of FOIA. In A. R. Adler, Ed. *Litigation Under the Federal Open Government Laws*. Washington, DC: American Civil Liberties Union. A34.

- Cobb, Chris (1999). Access panel's ruling opposed. *Montreal Gazette*. Montreal, Quebec. January 16, 1999. A6.
- Collins, William C. (1999). *Privately operated speculative prisons and public safety*. Washington: Department of Justice, Office of Justice Programs.
- Correa, Carlos (2000). Reforming the intellectual property rights system in Latin America. *World Economy* 23.6 (June 2000): 851-873.
- Crozier, Michel, Samuel P. Huntington, et al. (1975). *The crisis of democracy*. New York: New York University Press.
- Dahl, Robert (1999). Can international organizations be democratic? In I. Shapiro and Hacker-Cordón, Eds., *Democracy's Edges*. Cambridge: Cambridge University Press. 19-40.
- Debevoise, Whitney (1998). Key procedural issues: Transparency. *International Lawyer* 32 (Fall 1998): 817.
- Department of Energy (2000). *Special Historical Records Review Plan (Supplement), Public Laws 105-261 and 106-65*. Washington, DC: Department of Energy. March 1, 2000.
- Dorril, Stephen (2000). *MI6*. New York: The Free Press.
- Drache, Daniel (forthcoming). The return of the public domain after the triumph of markets. In D. Drache and R. Higgot, Eds., *Globalization and the post-Washington Consensus*. London: Routledge.
- Durkan, Sean (2000). Chretien pledges one-tier health care. *London Free Press*. London, Ontario. March 19, 2000. A5.
- Economist (1999). Digital rights and wrongs. *The Economist*. London. July 17, 1999. Web edition.
- Etzioni, Amitai (1999). *The Limits of Privacy*. New York: Perseus Books.
- Fairley, Peter (1997). EPA plans on-line report cards. *Chemical Week* 159.10 (March 12, 1997): 13.
- Fairley, Peter (1997). Right-to-know knocks: Will the industry open up? *Chemical Week* 159.32 (August 20, 1997): 19-21.
- Fairley, Peter and Rick Mullin (1998). Scorecard hits home. *Chemical Week* 160.21 (June 3, 1998): 24-26.
- Financial Action Task Force (2000). *Annual Report 1999-2000*. Paris: Financial Action Task Force. June 22, 2000.
- Financial Post (1998). Flak prompts delay in MAI negotiations. *Financial Post*. April 29, 1998. 16.
- Financial Stability Forum (2000). *Report of the Working Group on Offshore Centres*. Washington: Financial Stability Forum. April 5, 2000.
- Fitzgerald, Mark (1995). Should government information be privatized? *Editor and Publisher* 128. (November 11, 1995): 30-31.
- Fleming, Joseph (1983). Wire story: West German census. *United Press International*. Bonn, West Germany. December 16, 1983.
- Frankel, Maurice (1997). *Unlocking the truth: The government's FOI white paper*. London: Campaign for Freedom of Information. December 16, 1997.
- Fukuyama, Francis (1995). *Trust*. New York: The Free Press.
- G8 (2000). *Okinawa Charter on Global Information Society*. Okinawa, Japan. July 22, 2000.

- Garfinkel, Simson (1995). *Pretty Good Privacy*. Cambridge: O'Reilly.
- Garfinkel, Simson (2000). *Database nation*. Beijing ; Cambridge: O'Reilly.
- Gellman, Robert (1995). Twin evils: Government copyright and copyright-like controls over government information. *Syracuse Law Review* 45.3 (1995): 999-1072.
- Giddens, Anthony (2000). *The Third Way and Its Critics*. Cambridge, UK: Polity Press.
- Glendon, Mary Ann (1991). *Rights Talk*. New York: The Free Press.
- Greenman, Catherine (2000). Taking sides in the Napster war. *New York Times*. New York. August 31, 2000. Web edition.
- Grossklaus, D. (1991). Byting the hand that feeds them. *Washington Monthly* 23.11 (November 1991): 37-42.
- Gruenwald, Juliana (1993). Wire story: Delay in declassifying radiation documents. *United Press International*. Washington. December 30, 1993.
- Guardian (1999). Santer has to take notice. *The Guardian*. London. January 16, 1999. 20.
- Guerrin, Michel (2000). French media angered by new privacy law on pictures. *The Guardian Weekly*. London. June 8, 2000. 29.
- Hoekman, Bernard and Petros Mavroidis (1999). *WTO dispute settlement, transparency and surveillance*. Washington, DC: World Bank. WTO 2000 Capacity Building Project background paper.
- Home Office (1999). *Freedom of Information: Consultation on Draft Legislation*. London: Home Office. May 1999. Cm 4355.
- Hubbertz, Andrew (1999). Response to "Closing the Window". *Government Information in Canada*. 17 (March 1999): Web edition.
- HURIDOCS (1993). *HURIDOCS Standard Formats: A Tool for Documenting Human Rights Violations*. Versoix, Switzerland: Human Rights Information and Documentation Systems International. 1993.
- International Monetary Fund (1999). *IMF takes additional steps to enhance transparency*. Washington, DC: International Monetary Fund. April 16, 1999. PIN 99/36.
- Jaffe, Adam and Steven Peterson (1995). Environmental regulation and the competitiveness of U.S. manufacturing. *Journal of Economic Literature* 33.1 (March 1995): 132-164.
- Johnson, Pierre Marc and Andre Beaulieu (1996). *The Environment and NAFTA*. Washington, DC: Island Press.
- Jones, George (2000). Countryside bill could be stifled by Lords logjam. *Daily Telegraph*. London. August 1, 2000. 8.
- Kelley, Wayne (1998). Keeping public information public. *Library Journal* 123 (May 15, 1998): 34.
- Klein, Naomi (2000). *No Logo*. Toronto: Knopf Canada.
- Köhler, Hans (2000). IMF must adapt and reform. *IMF Survey* 29.16 (August 14, 2000): 258-260.
- Koven, Lisa (1998). The environmental self-audit evidentiary privilege. *UCLA Law Review* 45.4 (April 1998): 1167-1200.
- Kuntsler, J.H. (1996). *Home from Nowhere*. New York: Simon and Schuster.

- Lardner Jr., George (1998). CIA won't declassify files, blames budget. *Washington Post*. Washington, DC. July 17, 1998. A15.
- Lee, Louise and Aaron Bernstein (2000). Who says student protests don't matter? *Business Week* 3685 (June 12, 2000): 94-96.
- Lessig, Lawrence (2000). *Code and other laws of cyberspace*. New York: Basic Books.
- Lindberg, Mary (1999). *Statement on behalf of the Ontario Ministry of Health on Bill C-6*. Ottawa, Ontario: Senate Standing Committee on Social Affairs, Science and Technology. December 2, 1999.
- Loeb, Vernon and Doug Struck (2000). Web site posts secret CIA briefing papers. *Washington Post*. Washington, DC. July 23, 2000. A2.
- Long, Clariisa, Ed. (2000). *Intellectual property rights in emerging markets*. Washington, DC, American Enterprise Institute.
- Lowrance, William W. (1997). *Privacy and health research*. Washington, DC: Department of Health and Human Services, Office of the Assistant Secretary for Planning and Evaluation. May 1997.
- Matthews, William (2000). Access denied. *Federal Computer Week* (May 29, 2000): Web edition.
- McLellan, Anne (2000). *Notes for an address to the Canadian Bar Association*. Halifax, Nova Scotia: Department of Justice. August 21, 2000.
- McNairn, Colin and C.D. Woodbury (1998). *Government Information: Access and Privacy*. Toronto: Carswell.
- Milne, Roger (1999). A question of freedom. *Utility Week* (June 11, 1999): 17.
- Morse, Janice (1998). Guards faulted in escapes. *The Cincinnati Enquirer*. Cincinnati, Ohio. August 5, 1998. B1.
- Morton, Bruce and Steven Zink (1991). Contemporary Canadian Federal Information Policy. *Canadian Public Administration* 34.2 (Summer 1991): 312-328.
- Moynihan Commission (1997). *Report of the Commission on Protecting and Reducing Government Secrecy*. Washington, DC. March 3, 1997. S.Doc. 105-2, 103d Congress.
- Moynihan, Daniel (1998). *Secrecy: The American Experience*. New Haven, Connecticut: Yale University Press.
- Murray, Charles (1997). *What it means to be a libertarian*. New York: Broadway Books.
- Nader, Ralph (1993). NAFTA vs. democracy. *Multinational Monitor* 15.10 (October 1993): Web.
- Nader, Ralph and Lori Wallach (1996). GATT, NAFTA, and the subversion of the democratic process. In J. Mander and E. Goldsmith, Eds., *The Case Against the Global Economy*. San Francisco: Sierra Club Books. 92-107.
- Neumayer, Eric (2000). Trade and the environment: A critical assessment. *Journal of Environment and Development* 9.2 (June 2000): 138-159.
- Nilsen, Kirsti (1994). Government information policy in Canada. *Government Information Quarterly* 11.2: 191-209.
- Nilsen, Kirsti (1996). The effects of electronic publication on social science researchers in Canada. In C. Meadow, M. Weaver and F. Hébert, Eds., *Electronic publishing; It impact on publishing, education, and reading*.

- Toronto: Faculty of Information Studies, University of Toronto. 1-25.
- Nodo 50 (2000). *No data privacy for top torturers*. Nodo 50. April 15, 2000.
- Norton-Taylor, Richard and David Pallister (1999). MI6 tries to limit internet damage. *The Guardian*. London. May 15, 1999. 6.
- NPR (2000). *Americans distrust government, but want it to do more*. Washington, DC: National Public Radio. July 28, 2000.
- OECD (1998). *Harmful Tax Competition: An Emerging Global Issue*. Paris: Organization for Economic Cooperation and Development. April 1998.
- OECD (1999). *OECD Principles of Corporate Governance*. Paris: Organization for Economic Cooperation and Development, Ad Hoc Task Force on Corporate Governance. April 19, 1999. SG/CG(99)5.
- OECD (2000). *Towards Global Tax Cooperation: Progress in Identifying and Eliminating Harmful Tax Practices*. Paris, France: Organization for Economic Cooperation and Development, Committee on Fiscal Affairs. June 26, 2000.
- Parker, Andrew and George Parker (1998). Utilities win fight to curb freedom act impact. *Financial Times of London*. London. July 22, 1998. 8.
- Pauly, Louis (1997). *Who elected the bankers?* Ithaca, New York: Cornell University Press.
- Pringle, Kenneth (2000). Judges release financial records. *APBnews.com*. New York. June 21, 2000. Website.
- Privacy Commissioner (2000). *Annual Report, 1999-2000*. Ottawa: Office of the Privacy Commissioner.
- Prophet, Katherine (1999). Threats to Public Access to Federal Government Publications in Canada and the United States. *Government Information in Canada* 18 (August 1999)
- Public Interest Advocacy Centre (2000). *Fact sheet on the Personal Information Protection Act*. Ottawa: Public Interest Advocacy Centre. April 11, 2000.
- Putnam, Robert (2000). *Bowling Alone*. New York: Simon and Schuster.
- Quist, Arvin (1989). *Security Classification of Information*. Oak Ridge, Tennessee: Oak Ridge National Laboratory. September 1989.
- Raghavan, Chakravarthi (2000). *Continuing conceptual divides at the WTO*. Penang, Malaysia. March 2, 2000.
- Reno, Janet (1993). Statement of the Attorney General regarding implementation of FOIA. In A. Adler, Ed. *Litigation Under the Federal Open Government Laws*. Washington, DC: American Civil Liberties Union. A35-36.
- Roberts, Alasdair (1999). Retrenchment and Freedom of Information: Recent Experience Under Federal, Ontario, and British Columbia Law. *Canadian Public Administration* 42.4 (Winter 1999): 422-451.
- Roberts, Alasdair (2000). Less Government, More Secrecy: Reinvention and the Weakening of Freedom of Information Law. *Public Administration Review* 60.4 (July-August 2000): 298-310.
- Rose, Richard (1980). *Challenge to governance*. Beverly Hills: Sage Publications.
- Saxton, Jim (1998). *News release: Hearing to discuss IMF transparency*. Washington, DC: Joint Economic Committee, U.S. Congress. February 19, 1998.

- Saxton, Jim (1998). *News release: New IMF reform rooted in Transparency and Efficiency Act*. Washington, DC: Joint Economic Committee, U.S. Congress. October 20, 1998.
- Schiller, Herbert (1989). *Culture, Inc.* New York: Oxford University Press.
- Schwartz, John (2000). FBI internet wiretaps raise issues of privacy. *Washington Post*. Washington, DC. July 12, 2000. E1-E4.
- Select Committee on Public Administration (1998). *The Freedom of Information White Paper*. London: House of Commons. May 19, 1998. Third Report, Session 1997-98.
- Smith, R. Jeffrey (1994). CIA, others opposing White House move to bare decades-old secrets. *Washington Post*. Washington, DC. March 30, 1994. A14.
- Sobel, Richard (2000). *Comments on proposed HHS rules on medical records*. Washington, DC: National Coalition for Patient Rights. February 17, 2000.
- Söderman, Jacob (2000). The EU's transparent bid for opacity. *Wall Street Journal Europe*. February 24, 2000.
- Solomon, Karen (2000). Toward fewer free lunches. *The Industry Standard* (June 26, 2000): 212-226.
- Southeastern Legal Foundation (2000). *Census in Crisis*. Atlanta, Georgia: Southeastern Legal Foundation. April 3, 2000.
- Statistics Canada (2000). *Census Communications Program, 2001 Census*. Ottawa: Statistics Canada. n.d.
- Stiglitz, Joseph (2000). What I learned at the world economic crisis. *The New Republic* 222.16 (April 17-24, 2000): 56-60.
- Supreme Court of Canada (1997). *Dagg v. Minister of Finance*. [1997] S.C.J. No. 63.
- Sykes, Charles (1999). *The End of Privacy*. New York: St. Martin's Press.
- Sylvester, Sherry (2000). Libertarians oppose census questions. *San Antonio Express-News*. San Antonio, Texas. February 12, 2000. 1B.
- Toronto Globe and Mail (1999). Editorial: Free up Ontario Hydro. *Toronto Globe and Mail*. Toronto. February 26, 1999. A10.
- Tynan, Daniel (2000). Privacy 2000: In web we trust? *PCWorld* (June 2000): 103-116.
- U.S. District Court for the Northern District of California (2000). *EBay, Inc. v. Bidder's Edge, Inc.: Order granting preliminary injunction*. San Jose, CA. May 24, 2000. Whyte, J.
- U.S. District Court for the Southern District of New York (2000). *Universal City Studios, Inc., et al, v. Shawn C. Reimerdes, et al*. New York. August 17, 2000. Kaplan, J.
- U.S. Mission (1999). *Communication to the Working Group on the Interaction between Trade and Competition Policy*. Geneva: United States Permanent Mission to the WTO. July 13, 1999.
- United Kingdom (1997). *Your Right to Know: The Government's Proposals for a Freedom of Information Act*. London: Stationery Office. December. Cm 3818.
- United States Trade Representative (1998). *1998 Annual Report of the President of the United States on the Trade Agreements Program*. Washington, DC: Office of the United States Trade Representative.
- Village Voice (1999). Russian cons and New York banks. *Village Voice*. New York. December 7, 1999. 57-61.

Weeks, Jennifer (2000). Keeping secrets.
Washington Post. Washington, DC. June 25,
2000. B3.

Weiner, Tim (1994). U.S. plans overhaul on
secrecy. *New York Times*. New York. March 18,
1994. A1.

WTO General Council (1998). *Minutes of
Meeting of the General Council*. Geneva:
World Trade Organization. April 24, 1998.
WT/GC/M/28.