

## **CH.7**

### *Balancing Freedom of Information and the Protection of Privacy*

Information and communication technologies (ICTs) have revolutionized the way in which we communicate. The ubiquitous use of email, cellphones, digital cameras, instant messaging, and social networking allows people to share information instantly and to connect, reconnect, and stay connected with people all over the globe in ways that were inconceivable a mere decade ago. At the same time, the ever-increasing ability of computer technology to collect, store, retrieve, and transmit information is dramatically changing how commerce and governance is conducted. Organizations collect massive amounts of data (in word and pictorial form) concerning our activities as both citizens and consumers. This gives rise to privacy concerns; in particular, how can individuals control what is known about themselves? But ICTs also provide opportunity for fostering social and political engagement, enhancing service, facilitating trade, and increasing security. While it is reasonable to worry about

the possibility of “Big Brother” knowing everything about you, the “knowing” can work in both directions: ICTs also allow the individual citizen-consumer to scrutinize government and other large organizations in ways that were not possible a few years ago. There might be good reasons for an organization to seek to suppress information, but as this becomes more difficult, government, corporate, and non-profit accountability will undoubtedly increase.

Social scientists in the coming decades will be confronted with two vexing questions. How will ICTs change the nature of the relationship between citizens and government? How will ICTs change the relationship between the citizen-consumer and others in society with either complementary or competing interests? The analysis of competing interests is central to the discipline of political science, which concerns itself with the distribution of power. But these issues will touch the lives of many professionals from a wide range of disciplines. Sociologists, legal scholars, and philosophers have waded into the murky waters of the privacy debate to assess the challenges new technologies pose for the ability of citizen-consumers to control their personal information. Scholars with an interest in human rights and public administration have looked at the relationship between transparency and democratic governance. They have considered how dissidents use new devices for surveillance and communication to counter hegemonic thought or to promote larger organizational accountability. Still others have examined the legislative framework that underpins privacy and transparency. The difficulty is that the technologies and the issues are changing so quickly that studies become dated shortly after they are completed.

The intersection of freedom of information (FOI) and the protection of privacy should be of great interest beyond the scholarly community as well; these issues impact everyone. The issues, however, are so complex and the technology for digitizing government, commerce, and communications is changing at such a rapid pace that it is virtually impossible for social science analysis to keep up. For the average person, the task of understanding the issues is verging on impossible. But unless we are content to be swept along by the forces of change, accepting whatever is given to us by those who have a particular interest (usually commercial) in the new technologies, we must at least attempt to keep our heads above water. We might even decide to swim across the current and head for shore.

Governments collect massive amounts of data concerning their citizens. As taxpayers who pay for the collection of this information, and indeed for the operations of government generally, citizens are entitled to know what their governments are doing and what information they hold. Consumers want to know the same things. Though they might not have the same rights to access information regarding the internal workings of a company as citizens with respect to governments, they certainly should have the ability to determine whether or not the company is operating within the regulatory framework that is set out in legislation. The ability to access information ensures accountability, which hinges on two old chestnuts of public administration: fixed rules and due process. Put more plainly, both consumers and citizens should be able to track the activities of large organizations in order to eradicate, or at least inhibit, corruption by ensuring that those organizations are operating within the law.

Unfortunately for the citizen-consumer, there can be great administrative resistance to any attempt to create a regime of free-flowing information. This is not always a result of corruption or other wrongdoing. It can be the result of a lack of resources provided to those in charge of managing information, making it very difficult for them to effectively perform their mandated role. It also can be the result of ignorance of the actual purpose of freedom of information laws. Clearly, those whose roles include responsibility for responding to access requests would benefit from training and sufficient resources to fulfill their obligations.

What is troublesome for critics of a vision of the world where information flows freely is their suspicion that the riches will not be distributed evenly and that existing inequities will be reinforced. Those who are in the position to collect and manipulate information will benefit from the flow far more than others with limited or no access. Thus, existing inequities could be exacerbated between countries in the northern and southern hemispheres, corporations and consumers, socio-economic classes, anglophones and speakers of other languages, and the mainstream and the marginalized. These concerns ultimately relate to larger issues of control of the Internet and of intellectual property. Who controls information and knowledge?

Of equal importance to the creation of a FOI regime is the protection of privacy. Privacy in many respects is an even more complex concept than transparency and as such is difficult to define. At its most basic, however, it speaks to the autonomy of the individual, specifically the right to be left alone to pursue one's self-interest without interference. It includes the need for confidentiality; without this,

professionals in the legal and health fields could not develop the relationship of trust with their clients that they need if they are to provide effective service. Similarly, there is a place for secrecy in some organizational activities: a measure of secrecy can be necessary for commercial success and for security. Though it is tempting to juxtapose simplistically the right of an individual for privacy with the right of the group to advance the interest of the majority of people within a society, ultimately a measure of privacy for the individual is in the best interest of the group. Total transparency is “too much of a good thing,” and so is total privacy.

Efforts to balance privacy and transparency can be seen in the proliferation of both FOI and privacy regimes around the world. Legislative initiatives are a result of new technologies for collecting, storing, and disseminating information, of the rise of e-commerce activities that use electronic information, of the ability to create comprehensive information profiles by matching data, and of the sheer amount of information that is being collected. But the biggest challenge to privacy ultimately comes from the private sector; there is a great deal of money to be made from access to our personal information. While the differences among legislative regimes reflect both the time and place in which they were developed, generally speaking, regimes are converging as nations attempt to align their practices to facilitate trade.

Data management, of course, is not just restricted to written records: there are many types of data derived from other sources. This book has considered not only the printed word but also the sharing of medical images such as X-rays, photographic images produced from cellphones, cameras, and video cameras, and locational information obtained from GPS

devices. The issues around the collection, retention, and use of information are complex and as varied as the technologies that allow their collection. As such, issues cannot be neatly divided into two silos of competing interests corresponding to access and privacy.

Thus far this book might seem to suggest that it is the ICTs themselves that are the single largest threat to privacy. An important factor in decreasing privacy is our willingness to give up our privacy in exchange for something else. Using Facebook to socialize, using loyalty cards to earn free products, and posting pictures or videos for the attention they draw are all examples of decisions that individuals make that compromise their privacy. Assuming that they have a basic understanding of the implications of their decisions, those making them have decided that the personal gain that they accrue from these activities is worth the privacy they lose.

But does this mean that the abdication of privacy necessarily guarantees an expectation of transparency or some other societal benefit? Clearly not, but of equal concern is the tendency of some to become “privacy pit bulls” who intuitively recognize the problems for individual autonomy associated with new ICT technologies but do not pay much attention to the use of data for the promotion of the public good. In this instance, the “public good” is most easily understood from a public administration perspective, where “transparency” implies access to information. Transparency can result in improved service delivery, increased security, and increased accountability. As is demonstrated in the discussion of health information, access to information can make very tangible improvements to patient treatment both in terms of service delivery and knowledge gained through

medical research. Better methods for the detection and treatment of illness will save money because of shortened hospital stays, fewer days missed from work, and less unpaid familial outpatient care. All of these benefits, however, come at the expense of sharing what many consider their most private information.

Similarly, the chapters on surveillance and social networking argue that transparency and access to information are critical for ensuring democratic accountability, and in particular due process and participation. Transparency ensures the rule of law — that the rules of the game are clearly understood and followed. While the rules could arguably favour a particular group, at the very least the rules are visible, and as such, they can be debated. The chapter on social networking demonstrates how access to information can facilitate new forms of relationships, either peer-to-peer social networking or networking for the purpose of affecting political change. This new communication is fundamentally different from previous top-down forms of hierarchical communication and facilitates the engagement that is critical to both social cohesion and political participation. The accountability that transparency seeks to produce is seen as defining the public benefit of surveillance. Surveillance is used to increase public safety and to monitor the activities of individuals in the workplace (particularly with respect to police and military personnel). Surveillance is also used to increase efficiency and convenience in a variety of activities. As before, a critical question when examining these “public goods” is: What level of societal benefit must be evident to justify the infringement on privacy? Privacy, as its advocates are quick to point out, is central to a person’s sense of personal space and security. It

allows us a measure of control over what people know about us. In the end, the political community must determine the balance between privacy and transparency. Ultimately what is being asked is: What is the proper balance between the rights of individuals and those of the larger community that they live within?

This book argues that in the new millennium the dual areas of freedom of information and protection of privacy are of critical importance to the nature of the relationships between the citizen-consumer and large organizations (including but not limited to the state). The adage “knowledge is power” is particularly applicable in the information age: having (or not having) access to information and the knowledge associated with it will alter relationships of power. So too will the ability to keep information confidential, be it personal or organizational. ICTs are providing new opportunities for the undermining of autonomy through various forms of surveillance. At the same time, they offer a measure of personal empowerment, making it possible, for example, for an individual to connect easily with like-minded people for the purpose of keeping large organizations accountable. When using ICTs, though, most individuals focus on the benefits of “connection” without thinking about what is lost with respect to their individual autonomy. This point is of particular significance to so-called digital natives, who may find that the digital record of their youthful exuberance (or imprudence) can harm their employment or relationship prospects in the future.

One of the primary goals of this book has therefore been to underscore the importance of freedom of information and protection of privacy to social relationships. In doing so, it

seeks to stimulate a thoughtful and self-reflective analysis of how the management of new technologies will define the roles and personal spaces of new graduates who are poised to take their places as citizen-consumers contributing both to the democratic process and to the market economy. In particular, this reflection will encourage all of us to analyze issues that have been debated for centuries: What does the ideal political community look like, and what implications does this ideal have for individual autonomy?