Reviews / Comptes rendus

Controlling Knowledge: Freedom of Information and Privacy Protection in a Networked World

by Lorna Stefanick
(Athabasca, AB: AU Press, 2011, 250 pages)

In an age where technology is rapidly changing how we communicate in both our personal and professional lives and privacy issues frequently make headline news, Lorna Stefanick's *Controlling Knowledge: Freedom of Information and Privacy Protection in a Networked World* is extremely timely. Writing for a general audience and including many real-life examples, Stefanick unpacks the complexities of freedom of information and privacy protection (FOIP) and explains how these concepts relate to governance—sparking my interest as a continuing education administrator because instructors have been increasingly inquiring how to incorporate activities using publicly accessible external sites such as blogs, wikis, or Facebook into their teaching.

Many instructors, though enthusiastic about the potential benefits of these tools, may be unaware of privacy issues associated with their use in education or uncertain how they will affect their teaching strategies in practical terms. As Stefanick asserts, many of us are familiar with the basics of FOIP but are complacent about protecting it until either our privacy or ability to access information is threatened or removed. Indeed, the proliferation of new technologies makes it difficult for the average person to become familiar with the privacy policies and potential issues pertaining to each new technology. Educators will therefore benefit from Stefanick's discussion about how technology has changed the ways in which information is captured, stored, and disseminated. As well, this book may benefit university administrators who play a role in defining FOIP principles, values, and policies at their institutions.

The first half of the book lays the conceptual groundwork for privacy and access to information as they relate to legislation, as well as introduces relevant cultural influences and historical events from Canada and around the globe. Stefanick begins with a discussion of the challenges in defining privacy, the reasons that privacy protection is valued by society, and the importance of shifting norms of privacy. Stefanick then delves into examples of how personal autonomy may be threatened by the rapid and efficient data flow recent technologies have enabled. This discussion leads to the juxtaposed topic of freedom of information (FOI) or, more specifically, the idea of transparency—a necessary condition for accountability—and it becomes apparent that "the point at which transparency becomes an infringement on the ability of individuals or a group of individuals to pursue their self-interest without undo interference from others is not clear" (94). Privacy protection and FOI often result in competing interests, and Stefanick advocates quite convincingly for balance between the two. However, where the line to achieve this balance should be drawn and who makes that decision depends on many factors that are further explored throughout the book.

In the second part of her book, while focusing on how networked technologies have provided many benefits in the areas of electronic health records, surveillance, and social networking, Stefanick discusses the cost of these technologies to our privacy. Case studies of these three very different sectors demonstrate how the issues of FOIP are pervasive in multiple areas of our lives and affect an overwhelmingly significant portion of the population. From a privacy perspective, health information is thought by many to be the most sensitive area for which protection is essential. Electronic heath records have enabled many improvements in the areas of patient diagnosis, treatment, and safety; reduced health care system costs; and contributed to general research, health promotion, and disease containment. However, when mismanaged or used for other purposes, this same information could potentially be used to devastating effects for patients: for example, there have been reported cases of genetic discrimination or insurance companies denying coverage.

In the chapter on surveillance, Stefanick describes how the recent marriage of video and Internet technologies has empowered ordinary citizens to record and distribute videos to a large audience over the Internet, all without a gatekeeper. While the tools making these actions possible can increase transparency and thereby have a positive impact on accountability, concerns exist about legitimate instances of nondisclosure (for example, information related to national security), as well as the level to which technology allows all of us to be watched and what this means for our privacy. In a post 9/11 world, surveillance is tightly linked with security and may therefore be a desirable societal norm. However, clear answers to the questions of where surveillance should occur (especially in public spaces) and by whom (private companies such as Google do not necessarily follow privacy best practices, as exemplified by privacy issues that arose when Google took pictures for their Street View tool), as well as how such images are collected, used, and retained, do not yet exist.

Social networking sites such as Facebook engage and empower individuals, both socially and politically, because they provide connectivity. However, if users disclose too much personal information and are unaware of how to properly set privacy settings, participation on Facebook can also diminish personal autonomy. Facebook itself has been shown to neglect taking adequate steps in protecting its users' privacy, allowing third parties to access information on Facebook users. In such cases, where individuals are not consciously choosing what personal information to reveal and to whom, undesirable outcomes can occur, such as identity theft or the inability to remove or change a digital identity that may prove incriminating in the future.

While information communication technologies have contributed to the increasing complexity surrounding how information is managed, Stefanick concludes that it is not information communication technologies themselves that are the biggest threat to privacy, but rather our willingness to give up our privacy in exchange for other perceived benefits. Ultimately, regardless of the purposes for using technology, Stefanick challenges readers to examine their underlying assumptions about privacy, access to information, accountability, and democracy. Because it forces its readers to consider the proper balance between the rights of the individual and those of the larger community, this book is a must-read for anyone interested in privacy.

Linda Koechli, Ryerson University