Book Extract: *Information Security and Privacy – A Practical Guide for Global Executives, Lawyers and Technologists*

By Thomas Shaw

This month, our committee's new book, *Information Security and Privacy – A Practical Guide for Global Executives, Lawyers and Technologists,* will become available (**here**). The ABA bookstore's webpage shows the table of contents, all of the contributors and part of the first chapter. But I wanted to do more to give a flavor for what is inside, so the following are a series of brief extracts from the book. In creating a book with such a (very) large number of contributors, most if not all of whose work was intertwined with the work of others, it is not possible to individually credit each author's writing in each section. As such, I am using this article as a way to credit and give face to some of those contributors whose writings truly excelled.

Now that the book is published, here are some ways to get it promoted. The book will be reviewed in the upcoming issue of *SciTech Lawyer.* We are also having a number of testimonials written on the book. There is a whole marketing plan around the book's publication, including an upcoming press release. There are also a variety of non-traditional marketing efforts underway to widely disseminate the book, including blurbs by presenters at the RSA conference and availability in the RSA bookstore, outreach to non-lawyer organizations and contacts with foreign bar associations. Please feel free to recommend this book to colleagues and clients and add it to your professional networks and presentations. Congratulations to all of you who wrote so well and thank you all for your team work.

I also wanted to thank here not only those who followed through on their authoring commitments but several others who agreed to step into the breach when the original authors could not meet those commitments. Leading this group is Charlene Brownlee, who stepped in to help not just once but twice. Also stepping in and accepting the call to pick up the baton were Edward R. McNicholas, Rebecca Grassl Bradley, Daniel Garrie, Benjamin Tomhave, Dan Oseran and Steven Teppler. Your assistance in this complex endeavor is very much appreciated and made the book so much the better.

The Extracts – Introductory Paragraphs

Encryption – Robert Jueneman
(in Chapter 5)

The need for encryption has increased parallel to the increased movement of data outside controlled environments. The use of the Internet in all its forms, the vast increase in the use of outsourcing, and many new types of mobile technology mean that an organization's data may need to be protected at all times in all locations. Several key questions must be addressed in creating a cryptographic system that deploys encryption:

- How sensitive is my information, and which encryption algorithms and key lengths are recommended to protect it?
- What is the difference between data at rest, data in transit, and data in use, and what should be done to protect this data?
- What are the key business, information security, and privacy risks, and what can be done to mitigate them?

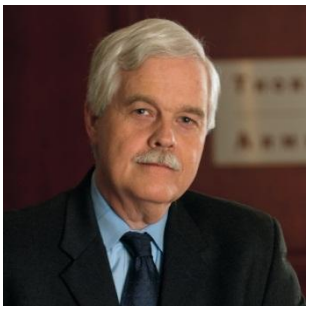
Canadian Information Security and Privacy Law – Michael Power
(in Chapter 2)

Canada is a federal state with a number of data protection laws governing the processing of personal information. Comprehensive legislation, for private-sector organizations, exists in the form of the federal Personal Information Protection and Electronic Documents Act (PIPEDA), as well as provincial statutes in British Columbia, Alberta, and Quebec. Determining which laws apply requires an analysis of a number of factors, but PIPEDA contains a mechanism to avoid duplicate coverage by exempting organizations already subject to "substantially similar" provincial legislation."

Health Insurance Portability and Accountability Act / Health Information Technology for Economic and Clinical Health Act – Charlene Brownlee
(in Chapter 2)

To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) included Administrative Simplification provisions that required the Department of Health and Human Services (HHS) to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. The Office for Civil Rights (OCR) administers and enforces the Privacy Rule and Security Rule. The Enforcement Rule provides standards for the enforcement of all the Administrative Simplification Rules.

Safeguarding Client Data: Lawyer's Ethical and Legal Obligations – David Ries
(in Chapter 2)



Confidential data in computers and information systems, including those used by lawyers and law firms, faces greater security threats today than ever before. Lawyers have ethical, common law, and statutory obligations to protect information relating to clients. In addition, protection of confidential information is sound business and professional practice. It is critical for

attorneys to understand and address these obligations and to exercise constant vigilance to protect client data.

Identity Management and Authorization - Tom Smedinghoff
(in Chapter 5)

In this age of the Internet, social networks, and mobile computing and the related issues of phishing, hacking, social engineering, and identity theft discussed in Chapter 4, the answer to the question, "who are you?" becomes critical. On the Internet, without the benefit of face-to-face personal contact, authenticating the identity of the remote party is of the utmost importance. It plays a key role in fighting identity fraud, is essential to establishing the trust necessary to facilitate electronic transactions of all types, and in many cases has become a legal obligation.

FTC Regulatory Actions – Marcia Hofmann
(in Chapter 3)

The Federal Trade Commission (FTC or the Commission) is the federal agency tasked with ensuring the efficient operation of the marketplace by protecting consumers from unfair and deceptive trade practices and promoting competition among businesses. While the FTC enforces various antitrust and consumer protection laws, this section discusses the Commission's enforcement of the Federal Trade Commission Act (FTCA) and other statutes designed to protect the privacy of consumer information. Data security is one of the top priorities under the FTC's privacy agenda. The FTC is also responsible for coordinating the federal response to identity theft and assistance for victims of identity theft.

Contract-based Claims – David Navetta
(in Chapter 3)

Information technology and the processing, storage, and transmission of information are ubiquitous. At the same time (and likely as a result of this ubiquity), the regulatory and legal liability environments pose increased risks and potential for enormous liability. Additionally, whether with cloud computing providers or via more traditional avenues for outsourcing information technology functions (e.g., ASP, hosting, and storage), companies are increasingly outsourcing their information technology functions to third-party service providers to stay competitive and efficient. It is likely that adoption of these practices will continue to increase.

The Need to Verify Certificate Authorities – Steven Roosa
(in Chapter 5)

Secure business communications rely on the PKI model described in the previous section. This process involves the authentication of the parties involved in the communication by third party Certificate Authorities (CAs). While some CAs may be well-known and easily trusted, others may be unknown or may involve CAs that organizations may not want to be part of their network of trust for secure communications. As such, it is necessary for lawyers and technologists to work together to actively determine all of the CAs that the organization will trust, instead of passively accepting that all CAs are worthy of trust. This starts with understanding the models of trust used by end-user Internet browsers when accessing websites.

Relationship Between Information Security and Privacy – Tanya Forsheit
(in Chapter 1)

Several relationships exist between information security and privacy. One relationship of information security and privacy is that one enables the other. Privacy requires information security to achieve its objectives. At the same time, privacy is larger than just the information security controls designed and implemented on its behalf. There are many other aspects to privacy that are not part of what information security aims to achieve. To understand this difference, we must first define privacy before looking at its relationships with information security.

The Role of Lawyers – E. Regan Adams
(in Chapter 8)

Lawyers play a crucial role in assisting an organization to implement information security and privacy policies and practices. The modern lawyer plays an ever more interesting and vital role—one undergoing transformation as digitalization sweeps the globe and the dynamic nature of data rapidly changes how organizations function. Today, the lawyer's job is no longer constrained to knowing just the law; it is about knowing processes and technology and shaping them to comply with laws and regulations in all subject areas and locations. Two of the lawyer's most critical roles are to manage risk and to help build defensibility into the core of an organization's information security and privacy practices.