Foreword

In December 2015 the Book Board of the ABA Section of Science and Technology Law discussed the concept of a book about cybersecurity in the home. We recognized that many books had been written from the perspective of an information security professional to lawyers and other professionals, but that none of them seemed to address cybersecurity in the home. We solicited suggestions and proposals from members of the ABA's Information Security Committee, and several individuals responded. We received one proposal that stood above the rest. That proposal was a book outline from John Bandler that covered all the bases.

Chapters 1 through 3 of *Cybersecurity for the Home and Office* aim to educate readers about the value of data in their lives and how cybercriminals will try and exploit that value with ransomware and other attacks. Chapter 4 provides an introduction to key principles about data protection, especially the need to protect the confidentiality, integrity, and availability of personal data. Chapters 5 and 6 provide an overview of how computers store and transmit data.

In Chapters 7 through 10, Mr. Bandler provides tips on securing data, whether it is at rest on your home computer or in motion as it is being transmitted over the Internet. Key concepts in these chapters are the "security dial" (personal risk tolerance) and the tools needed to conduct a personal risk assessment of your computing practices. With the growth of cloud storage for personal data, securing access with two-step authentication (strong passwords and one-time codes) is also highlighted. Protecting your family, especially your children and seniors, from attack or other types of abuse is the subject of Chapter 11.

Chapters 12 and 13 tell readers how to secure their data when outside the home, while traveling or at the office. Chapter 13 provides added security considerations for the small office, and Chapter 14 covers ethical obligations specific to lawyers. Finally, Chapter 15 provides a methodology for solving problems you might have with your computer, and the appendices provide helpful forms and templates to organize and protect your data.

There are two types of people—those who have been hacked and those who don't know they've been hacked. Most of us have already been hacked, and we just don't know it. *Cybersecurity for the Home and Office* is a call to action. Readers of this book will grow to appreciate that personal data protection needs to become a priority in our lives, and effective information security for our personal information requires that we make good choices to secure our devices. Our behavior needs to change. We need to develop better habits concerning our data, and *Cybersecurity for the Home and Office* is a playbook to help readers incorporate "cyber hygiene" into our daily routine.

Ben Wilson, JD CISA CISSP
ABA Section of Science and Technology Law