Book Review

Cryptography: From Luddite to Leader

A Book Review of "Encryption Made Simple For Lawyers"

by Jill A. Karmy

David G. Ries, Sharon D. Nelson, John W. Simke. ***Encryption Made Simple for Lawyers*****.** ABA Law Practice Division (2015), Paperback, 232 pages, $47.95 ABA LPM members; $69.95 non-members; Product Code 5110793.

In modern day terms, a luddite is someone who generally claims things were "just fine" back in the day, and refuses to adopt new technology. This may work for your everyday life, but being a luddite in your legal practice is probably malpractice. That is why I jumped at the chance to review the book, "Encryption Made Simple for Lawyers." After all, the duty of confidentiality is one of an attorney's most fundamental duties.

This book is authored by three individuals: an attorney specializing in electronic evidence law, another attorney specializing in technology litigation, and a digital forensics expert. It is aimed at the small firm and solo practitioner, as most large firms have in-house or remote technology consultants. The book starts with a discussion of cryptography. As the authors explain, cryptography is the science of secret communication. Encryption is a form of cryptography, whereby data is converted into a form called ciphertext that cannot be easily understood by unauthorized people. While I found this book to be very practical, skip the first three chapters (unless you are a technology guru, in which case you probably don't need this book). The first chapter is a historical discussion of encryption, from hieroglyphics to modern day practices. The second and third chapters discuss why encryption is so important, including a case study on data breaches. Here is the key point the authors make in these initial chapters: Encryption is truly the only way you can reasonably protect sensitive client information. You are welcome. I just saved you 45 pages of reading.

If you have the time, Chapter 4 is helpful to understanding the technology behind encryption. As the authors truthfully point out, you do not need to read this chapter to use encryption in your practice. Skip it.

Chapters 5 through 11 are the meat of the book. These chapters span 100 pages. After reading these 100 pages, the authors hope that you will be able to competently secure laptops, desktops, servers, smartphones, tablets, e-mail, and documents, with little more than a point and a click – ok, a couple of clicks and some brain power. For the most part, I found this to be true. I appreciated that the authors devoted a chapter to each type of device or document separately, as this enables you to skip directly to those chapters that are most relevant to your needs and to your practice.

You will find the read fast and easy. I encrypted my new office laptops and mobile devices as I read each chapter. The chapters on document and email encryption take a little more focus and concentration. The best part of the book, in my opinion, is that it includes screen-shots, pictures and examples so that you can visualize the process. The authors also include instructions for securing Apple operating systems and iPhones, as well as Microsoft operating systems and Android devices.

For those of you who know you need to do more to protect client data, but you also know that you will not read even 100 pages of this book, skip to pages 173-176. The authors have, so graciously, included an 8-step Quick Start Action Plan for encryption.

This book is a relaxed read on a complex topic and I recommend it for any small firm or solo practitioner. The book ends with a discussion on the future of encryption, including an intricate analysis of quantum computing. The authors leave you with a somber thought: current methods of encryption will not be enough to protect client data in our future world, but it is enough….for now.

Jill Karmy *is the managing member of Karmy Law Office, PLLC in Ridgefield, WA. She is an EAGLE member of WSAJ and focuses her practice on the representation of injured workers.*