

HARBORING DATA: Information Security, Law, and the Corporation

Edited by Andrea M. Matwyshyn

Stanford University Press, Stanford CA, 2009, ISBN 978-0-8047-6008-9

Price \$31.96, pp. 368

Reviewed by John W. Patton

Journal of High Technology Law

Suffolk University Law School

Harboring Data is a nonfiction book written by a collection of authors specializing in a variety of fields such as computer science, law, e-commerce, intellectual property, and data security. A few of the many areas of law discussed in the book are data breach notification laws, trade secret law, corporate laws such as duty of care and duty of loyalty, and confidentiality law. The book is edited by Andrea M. Matwyshyn,¹ who, along with the guest authors, presents some compelling problems with corporate information security. These problems are mostly caused by hackers, and have exposed weaknesses in corporate data security and how corporations handle or don't handle such problems. *Harboring Data* explains some of the laws regarding computer information dissemination and how those laws affect corporate data management and response.

Matwyshyn begins the book with a story of a hacker who in 2005 stole roughly 45.7 million credit and debit card numbers from TJX, Inc., a major retailer worth \$17.4 billion.² The theft caused TJX billions of dollars in losses from settlements, attorney fees, and court-awarded damages. TJX's computer network that the hacker accessed to

¹ Andrea Matwyshyn is an assistant Professor of Legal Studies and Business Ethics at the Wharton School at University of Pennsylvania.

² ANDREA MATWYSHYN, *HARBORING DATA: INFORMATION SECURITY, LAW, AND THE CORPORATION*, 3 (Stanford University Press) (2009).

obtain the numbers had a less sophisticated security system than most people have on their home wireless networks. Matwyshyn describes the TJX example to illustrate that many corporations which neglect spending the time and money on security often have to pay a price.

The first chapter, written by Jonathon Pincus,³ Sarah Blankinship,⁴ and Tomasz Ostwald,⁵ explains three common security issues: user error, measurement, and vulnerability disclosure. User errors are just what the name implies, but more importantly, user errors have more to do with a system's failure to reduce potential mistakes caused by users. Measurement is the idea that security systems have to be properly rated based on how effective they are in protecting what they are made to protect. For example, safes are rated according to how long they can withstand an attack from a thief that possesses specific safe-hacking tools, such as a torch. Computer security systems lack such ratings, and attempting to create such a system is far from reality. Lastly, vulnerability disclosure deals with the fact that software systems often contain flaws that cause the program to operate differently than intended. Attackers discover and take advantages of these flaws.

The Computer Fraud and Abuse Act of 1984 (CFAA) is discussed in chapter two by authors Kris Erickson⁶ and Philip N. Howard.⁷ They explain that the CFAA has a harsh penalty, five to ten years of imprisonment for first-time offenders. However, they

³ Jonathon Pincus is an author and blogger and the former General Manager for Strategy Development for Microsoft's Online Services Group.

⁴ Sarah Blankinship is a Senior Security Strategist at Microsoft.

⁵ Tomasz Ostwald is a Senior Program Manager at Microsoft.

⁶ Kris Erickson is an instructor in the Department of Geography at the University of Washington, and authored a dissertation on the online hacker community.

⁷ Philip Howard is an Associate Professor in the Communications Department at the University of Washington.

argue that it has not been an effective deterrent for thieves because of the recent surge in computer-related offenses.

There are some common corporate security mistakes explained by author Kim Zetter⁸ in chapter three, and they are often handled unlawfully by corporations. Some of the mistakes are a lack of concern, lack of money to invest in security, and lack of skilled personnel. Responses to security breaches are often mishandled, such as Verizon Wireless in 2006.⁹ Verizon was a victim of “pretexting,” a method whereby attackers, in this case data brokers, posed as Verizon customers who called Verizon to obtain copies of private cell phone records and then sold them online. Verizon did not issue a press release or send notifications to affected customers; instead it issued a press release touting its success in obtaining a court injunction against some of the data brokers. Additionally, Verizon’s failure to notify California customers of the security breach possibly violated California’s notification law. However, the author points out that the law does not cover cases of pretexting. This exposes a potential problem with California’s law. At the same, the fact that California is the only state that has enacted such a law is problematic.

The book further discusses security breaches pertaining to trade secrets. Author Elizabeth Rowe¹⁰ explains in chapter five that if trade secrets pass to third parties, the trade secret owner may not have any recourse against the third party to prevent the dissemination of the secret. There is no federal law governing trade secrets, but most

⁸ Kim Zetter is an award-winning investigative journalist and a former staff member of *Wired News*.

⁹ MATWYSHYN, *supra* note 2, at 59.

¹⁰ Elizabeth Rowe is an Associate Professor of Law at the University of Florida, and former partner at Hale and Dorr, LLP.

states have adopted the Uniform Trade Secrets Act (UTSA).¹¹ The key to transforming information into protected secrets under the UTSA is to keep the information secret. Attackers who breach security to obtain such information often render it “not a secret” and now the trade secret owner is longer afforded protection under the UTSA. Trade secret information is often stolen by employees of a corporation, and courts will often view this as a breach of the duty of loyalty. Rowe explains that the duty of loyalty, however, is insufficient to safeguard against trade secrets.

Protecting health care data is another area insufficiently protected by US law. Authors Sharona Hoffman¹² and Andy Podgurski¹³ criticize the Health Insurance Portability and Accountability Act (HIPAA). The authors maintain that the scope of HIPAA is too narrow; it only covers health plans, health care clearing-houses, and health care providers who transmit electronic protected health information. This leaves out parties who transmit health information such as employers, marketers, and operators of websites that sell medical equipment. These groups use electronic health information, but are not governed by HIPAA enabling them to use health data in ways that lead to discrimination, identity theft, or for example, stifled adoption efforts.

In chapter nine, author Jennifer Chandler¹⁴ discusses contract law as it relates to licensing in cyberspace. She maintains that licensing terms can undermine cyberspace security. For example, software licenses often contain terms that impede testing or examination of the software, or prohibit the public disclosure of the results of such examinations. One such provision is known as “anti-benchmarking,” which affects

¹¹ MATWYSHYN, *supra* note 2, at 93.

¹² Sharona Hoffman is a Professor of Law and Bioethics.

¹³ Andy Podgurski is an Associate Professor of Computer Science at Case Western Reserve University.

¹⁴ Jennifer Chandler is an Assistant Professor of Law at the University of Ottawa School of Law.

performance testing of software, often prohibiting the publication of the results without the consent of the software vendor. Chandler discusses some of the general contract law doctrines such as unconscionability and public policy as possible doctrines to address these potential problems. However, she claims that these doctrines are largely ineffective and that courts are often unwilling to broaden their scope to include cyberspace cases.¹⁵

The book delves into other areas where data security is crucial. For example, the Children's Online Protection Act (COPA) of 1998 addresses the collection of data regarding children and aims to protect children from accessing sexually explicit material online. However, COPA has been ineffective because parental involvement in monitoring children's internet usage is not adequately facilitated. Also, COPA is ineffective because it is under-inclusive in two regards; it only protects children under the age of thirteen,¹⁶ and it lacks extraterritorial effect to the significant amount of sexual explicit material originating outside of the US.¹⁷

Harboring Data is an appropriate and potentially valuable book for anyone interested in corporate law and the problems presented by security systems breaches. The authors present important, relevant issues and the shortcomings of current law and legislation. The value of the book comes from the opinions and knowledge of the expert authors, many of whom explain interesting cases that went unreported in the news. The format of the book was concise and easy to follow with a clear conclusion at the end of each chapter. The authors explain the relevant federal laws and assess their weaknesses as they pertain to various industries. I would recommend this book to corporate

¹⁵ MATWYSHYN, *supra* note 2, at 196.

¹⁶ See 15 U.S.C. § 6501 (1998).

¹⁷ See *ACLU v. Gonzales*, 478 F. Supp. 2d 775, 810 (2007).

attorneys, and to anyone interested in the current state of affairs in online security and unlawful data dissemination.