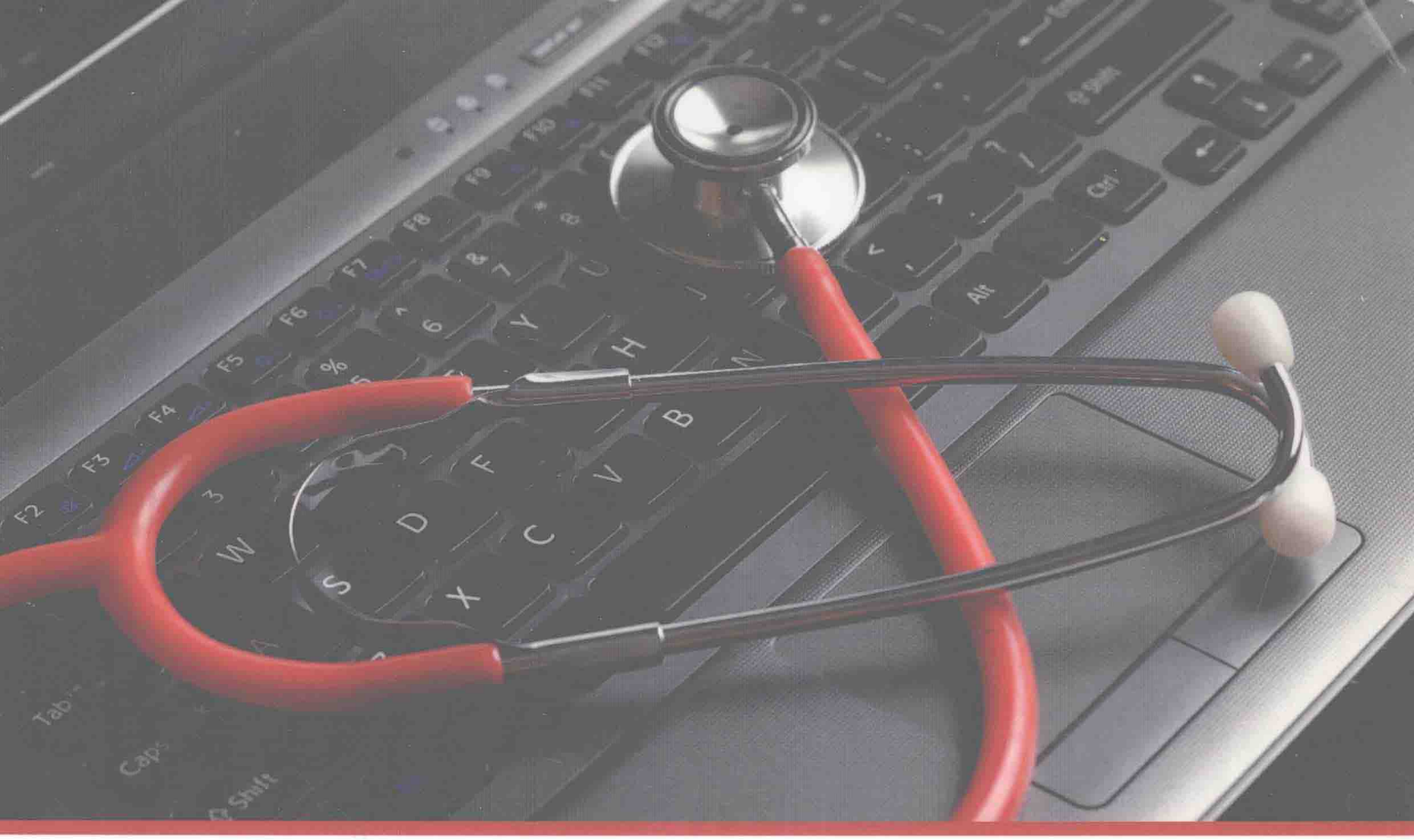

HEALTH CARE PRIVACY and SECURITY

2013 EDITION

ANDREW SERWIN
KENNETH MORTENSEN

THOMSON REUTERS
WESTLAW

Health Care Privacy and Security

2013 Edition

Andrew B. Serwin

and

Kenneth P. Mortenson

WEST®
A Thomson Reuters business

For Customer Assistance Call 1-800-328-4880

Material # 41310766

ISBN 978-0-314-61701–9

About the Authors

Kenneth P. Mortensen is Vice President, Assistant General Counsel & Chief Privacy Officer at CVS Caremark Corporation, where he has enterprise responsibility for information governance strategy to empower the superior application of information as a critical enterprise asset used to optimize risk and facilitate innovation incorporating an approach that protects individual privacy and drives operational compliance. Ken manages the Information Governance organization of the Legal Department, which includes a legal team, privacy operations, and, indirectly, the enterprise information security and risk governance group.

Ken is a member of the board of directors for the International Association of Privacy Professionals or IAPP. Founded in 2000, the IAPP is the world's largest association of privacy professionals with more than 11,000 members in 70 countries. The IAPP helps define, support, and improve the privacy profession through networking, education, and certification.

Before to coming to CVS Caremark, Ken was Boston Scientific Corporation's first ever Chief Privacy Officer and had world-wide responsibility to implement a global corporate privacy and security program, including EU data protection policy, at the medical device manufacturer.

Prior to re-entering the private sector, Ken served in the Administration of President George W. Bush as the Chief Privacy and Civil Liberties Officer for the U.S. Department of Justice, where he was the primary counsel and policy advisor to the Attorney General and Deputy Attorney General on privacy and civil liberties matters, including revisions to the Attorney General Guidelines for Domestic FBI Operations, updates to Executive Order 12333, and the FISA (Foreign Intelligence Surveillance Act) Amendments Act. He created the newest independent office within the Department, the Office of Privacy & Civil Liberties, with responsibilities under the Privacy Act of 1974 and the e-Government Act. Ken negotiated numerous international agreements with privacy and civil liberties safeguards that supported national security and law enforcement activities, including the High Level Contact Group between the U.S. and EU to create an understanding on privacy for government information sharing. Before coming to Justice, Ken joined the U.S. Dep't of Homeland Security early in its existence, first as a Senior Advisor and ending as the Deputy Chief Privacy Officer, counseling on privacy and security issues related to agency programs.

Formerly, Ken was founding/managing law partner at Harvey & Mortensen with clients that ranged from start-ups to state attorneys general, including serving as outside counsel to Pennsylvania Attorney General Mike Fisher for Internet and cyber issues as well as designing and operating the Commonwealth's initial Do Not Call website. Before private practice, Ken was a Teaching Fellow at Villanova University School of Law, where he taught computer and information law and managed operations for a think tank, the Center

for Information Law and Policy. Ken began his career at Burroughs Corporation as an Electrical Engineer performing large system design and test development for mainframe computers. In addition to his J.D. from Villanova University School of Law, he has an M.B.A. from Villanova University and a B.S.E.E. from Drexel University.

Andrew B. Serwin is an internationally recognized thought leader regarding information's evolving role in the economy and society, including how businesses can achieve key business objectives through the use of information, strategies companies must implement to protect and secure information, and what are appropriate uses of information. He combines a deep understanding of privacy and security regulatory issues, with advanced certification in business process improvement, as well as privacy. He is also the founding chair of the Privacy, Security & Information Management Practice and is a partner in the San Diego/Del Mar and Washington, D.C. offices of Foley & Lardner LLP. Mr. Serwin has handled a number of high-profile privacy and consumer protection matters, including multiple privacy enforcement matters before the Federal Trade Commission, and is internationally recognized as one of the leading consumer protection and privacy lawyers.

Mr. Serwin advises a number of *Fortune* 500 companies regarding global privacy compliance, including: state, federal and international restrictions on the use and transfer of information; behavioral advertising; social gaming; security breach compliance; mobile marketing; incident response resulting from data misuse and hacking; COPPA compliance; EHR/PHR concerns; marketing restrictions; HIPAA and state medical privacy laws; social media and blogging policies; Do-Not-Call restrictions; compliance with CAN-SPAM and state e-mail laws; employee monitoring; pretexting; location-based services; the drafting and implementation of privacy and security policies; risk assessments; compliance with ECPA and FISA; content monitoring; compliance with the CFAA and state computer crime laws; as well as information governance guidance in the context of M&A and technology transactions.

Mr. Serwin has provided advice to companies in a diverse set of industries, including advising: a leading Internet auction company; a nation-wide health insurer; ISPs; leading online retailers; major hospital chains; genetics companies; a leading social network; an international security company; data aggregators; a leading chain of international health and fitness clubs; a nation-wide auto retailer; one of the nation's largest home builders; a number of major utilities; medical device manufacturers; several major telecommunications companies; behavioral advertising companies; software-as-a-service providers; a leading retail pharmacy chain and PBM; several major hotel and resort companies; and several nationally-recognized universities. Mr. Serwin also has unique experience in representing emerging technology companies, having served as the founder and president of an internet start-up.

Mr. Serwin also has extensive litigation and enforcement experience, having served as lead counsel in a number of FTC matters, matters before the Office of Civil Rights, as well as state consumer protection matters and consumer privacy litigation matters based upon the alleged misuse of personal information.

Mr. Serwin was named to *Security Magazine's* "25 Most Influential Industry Thought Leaders" for 2009—he is the only lawyer in private practice to ever receive this award, and was ranked second in the 2010 *Computerworld* survey of top global privacy advisors. He is recognized by *Chambers USA* as one of the top privacy & data security attorneys nationwide (2009-2012), where he has described by clients as *"a tireless worker, holding onto the ever-shifting puzzle pieces of the law in this area in a way that other privacy lawyers cannot.",* and noted as "an excellent privacy lawyer, a real expert in the field," by Chambers Global 2012. The *Legal 500* recognized Mr. Serwin as a Leading Lawyer in data protection and privacy (2010-2011), where clients stated that he "understands business concerns and provides practical, to-the-point, advice." He has been Peer Review Rated as AV® Preeminent™, the highest performance rating in Martindale-Hubbell's peer review rating system, and was selected for inclusion in the *San Diego Super Lawyers®* lists (2007-2012), and was selected by his peers for inclusion in *The Best Lawyers in America®* in the field of information technology law (2010-2012).

Mr. Serwin serves as Executive Director of the Lares Institute, a think-tank focused on privacy and information management issues, as well as general counsel of the RIM Council of the Ponemon Institute, LLC, as well as the privacy and the legal subcommittees of the PSAB of the California Health and Human Services Agency by the California Office of HIPAA Implementation. He previously served as Co-Chair of the California State Bar's Cyberspace Law Committee and as a member of the Committee of Administration of Justice, as well as a member of the Publications Board for the Business Law Section of the American Bar Association.

Mr. Serwin has written a number of books, including the leading treatise on privacy, "Information Security and Privacy: A Guide to International Law and Compliance", a book that was named one of Thomson-Reuters' Best-Selling Books for 2010, and "Information Security and Privacy: A Guide to Federal and State Law and Compliance," which collectively are a three-volume, 4,000 page series that examines all aspects of privacy and security laws, published by Thomson-Reuters, which have been called "*the best privacy sourcebook*," "*an indispensible resource for privacy professionals at all levels*," and "*a book that everybody in the information privacy field should have on their desk*," and has been cited by *Ostergren v. Cuccinelli*, 615 F.3d 263 (4th Cir. 2010). He is also the author of several leading law review articles: "Privacy 3.0—The Principle of Proportionality," 42 *U. Mich. J.L. Reform* 869 (2009), "Poised on the Precipice: A Critical Examination of Privacy Litigation," 25 *Santa Clara Computer & High Tech. L.J.* 883 (2009), cited by *Hammond v. The Bank of New York Mellon Corp.* 2010 WL 2643307, (S.D.N.Y., June 25, 2010), and *Joseph Oat Holdings, Inc. v. RCM Digesters, Inc.*, 2010 WL 5065037, (3rd Cir. December 13, 2010), and "The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices", 48 San Diego L. Rev. 809 (2011). He has written over 100 articles and presented over 100 times on litigation and privacy.

His works have been cited by numerous law reviews and treatises, including: American Law Reports (ALR); American Jurisprudence 3rd; California Law Review; Callmann on Unfair Competition; Harvard Journal of Law & Technology; Iowa Law Review;

Southern California Interdisciplinary Law Journal; Stanford Law Review; and Wright & Miller, Federal Practice and Procedure—Criminal.

Mr. Serwin is a graduate of the University of San Diego School of Law (J.D., *cum laude*, 1995), where he was a member of the Order of the Coif. He earned his B.A. in political science, *cum laude*, from the University of California, San Diego in 1992. Mr. Serwin is admitted to practice law in California and the District of Columbia.

Tammy H. Boggs is an associate with Foley & Lardner LLP, where she represents clients in a variety of industries in consumer class action litigation, privacy and security litigation, and general business disputes. Ms. Boggs has substantial experience in all stages of litigation and civil procedure, including complex e-discovery issues, depositions, motion practice, trial preparation and alternative dispute resolution. She represents clients in both state and federal court proceedings. Ms. Boggs has also defended clients in patent litigation pending in district courts and the International Trade Commission. She is a member of the Privacy Litigation; Business Litigation & Dispute Resolution; Intellectual Property Litigation; and Privacy, Security & Information Management Practices. She serves on the firm's Diversity Committee.

Ms. Boggs has represented clients in a number of high-profile privacy and consumer protection matters brought by regulatory agencies, and has experience in coordinating incident responses to security breaches. She advises clients on compliance with privacy laws and best practices for information governance.

Ms. Boggs is also a member of the firm's Pro Bono Asylum/Immigration Practice, and has won asylum for numerous pro bono clients before the San Diego Immigration Court.

Prior to joining Foley, Ms. Boggs was an associate at Heller Ehrman LLP. While attending law school, she was a judicial extern to the Honorable Vaughn Walker, United States District Court Chief Judge in 2005. Before beginning her legal career, Ms. Boggs was a lead accounting analyst for Silicon Valley Bank, and provided financial auditing and tax services at Deloitte & Touche LLP. As a Certified Public Accountant (inactive), she performed audits of large corporations, including companies in the high tech, manufacturing, financial services, and insurance industries.

Ms. Boggs earned her law degree from the University of California, Hastings College of the Law (J.D., *cum laude* , 2007) where she was a member of the Prince Evidence and Jessup International Law Moot Court Competition Teams, and received accolades in Appellate Advocacy, Moot Court, and Legal Writing & Research. She is a graduate of the University of California, Los Angeles with a degree in business economics and an accounting minor (B.A., *magna cum laude,* 1999).

Ms. Boggs is admitted to practice law in California, before all District Courts of California, and before the Ninth Circuit Court of Appeals. She is fluent in spoken Mandarin Chinese.

Representative Present and Past Clients: WellPoint/Anthem Blue Cross, CVS Caremark, Bank of America, Disney, Old Republic Home Protection Company, Online Guru, Sony Electronics, AmeriCredit Financial Services, Clarendon National Insurance Company, and Kyocera Wireless.

Representative Publications and Presentations:

- "Analysing proposed changes to COPPA: the operator's role," *Data Protection Law & Policy*, September 2012
- Contributing Author, "Expert Analysis" column, *Class Action Law360,* 2011
- "Class v. Merits Discovery in Consumer Class Actions," prepared for Bridgeport California Consumer Class Action Conference, January 2011
- "Two Recent Class Action Decisions Further Develop Pleading Requirements Under California's Unfair Competition Law," Bloomberg's *Antitrust & Trade Law Report,* August 2010
- "Discovery in Class Actions: Privacy Implications and Best Practices," prepared for Bridgeport Class Action Litigation Conference, August 2010

Matthew Haddad is Associate General Counsel at WellPoint, Inc. He advises WellPoint and its affiliates on matters including Privacy and Security; HIPAA Standard Transactions and Code Sets; Pharmaceutical, Government and Academic Research; and Contract Negotiation. Mr. Haddad is a member of the Virginia State Bar, the International Association of Privacy Professionals and the Association of Corporate Counsel.

Molly McCoy, JD, MPH, CIPP/US is Senior Counsel at WellPoint, Inc. She advises WellPoint and its affiliated health plans and other subsidiaries on matters including Privacy and Security, HIPAA and HITECH, state privacy law, Business Associate Agreement negotiations, and proposed international, federal and state privacy law. Ms. McCoy is a member of the New York and Colorado State Bars and the International Association of Privacy Professionals.

Peter McLaughlin is senior counsel with Foley & Lardner, LLP in the firm's Boston office, where he is a member of the Privacy and Healthcare practices. He regularly advises clients on their understanding of and compliance with healthcare privacy and security, in addition to representing clients against federal and state regulatory matters. Before joining the firm, Mr. McLaughlin had been Assistant General Counsel - Privacy & Security and privacy leader for Cardinal Health, Inc., a Fortune 20 healthcare company. He is a graduate of Columbia University and the Georgetown University Law Center.

Megan E. O'Sullivan is an associate with Foley & Lardner LLP and a member of the Business Litigation & Dispute Resolution Practice and Privacy, Security & Information Management Practices.

Ms. O'Sullivan has represented clients in a number of privacy and consumer protection matters, including: the drafting and implementation of privacy and information security policies; security breach compliance; incident response; drafting and negotiating privacy agreements; and advising clients on general compliance obligations under both state and federal privacy and data security legislation.

Ms. O'Sullivan was a summer associate for Foley (2009) and also obtained experience with the San Francisco Superior Court in the Alternative Dispute Resolution Program where she assisted in the planning and implementation of the Asbestos Alternative Dispute Resolution Program. Prior to entering law school, Ms. O'Sullivan served as a staff assistant for the Office of Congresswoman Susan Davis.

Ms. O'Sullivan earned her law degree, *cum laude*, from the University of California, Hastings College of the Law (J.D., 2010) where she earned a CALI Award (top student of the class) in negotiations and ADR Externship Class. She was also a board member of the U.C. Hastings Negotiation Team. Ms. O'Sullivan graduated Phi Beta Kappa with a degree in political science and a minor in Spanish from the University of California, Berkeley (B.A., 2006). While at Berkeley, she completed an honors thesis and received numerous honors recognitions. Ms. O'Sullivan spent one year of undergraduate study at the Autonomous University of Barcelona, in Spain.

Ms. O'Sullivan is admitted to practice in California and before the Northern, Southern, Central, and Eastern Districts of California.

Eileen R. Ridley is a partner with Foley & Lardner, LLP where she serves on the firm's National Management Committee and is Vice Chair of the Litigation Department. She is a member of the firm's Privacy, Security & Information Management practice group and is the co-chair of the Privacy Litigation Task Force. Ms. Ridley has tried over 20 matters and has handled in excess of 40 class actions including matters involving the healthcare industry and privacy and information security issues. Ms. Ridley is a contributing author on Antitrust and Unfair Competition Law Section, The State Bar of California, CALIFORNIA STATE ANTITRUST AND UNFAIR COMPETITION LAW, Chapter 29, *The Consumers Legal Remedy Act*, (Cheryl Lee Johnson, ed., Matthew Bender & Co. 2009) and Protecting Personally Identifiable Information: A Guide for College and University Administrators, Chapter 2, *Recent Trends in Data Security and Regulatory Enforcement*, (Peter McLaughlin, ed., Council on Law in Higher Education, 2011). Ms. Ridley was also recognized by the *Legal 500* for her work in insurance: advice to insurers.

Table of Contents

CHAPTER 1. INTRODUCTION

CHAPTER 2. HEALTH INFORMATION AND PRIVACY AND SECURITY

I. INTRODUCTION

II. HIPAA

A. In general

B. Scope of HIPAA Regulations and Enforcement

C. Hearings

D. Security

E. Privacy

F. Uses and disclosures