A Guide to Privacy and Data Security Law in the Information Age

Second Edition
PLI’S COMPLETE LIBRARY OF TREATISE TITLES

ART LAW

BANKING & COMMERCIAL LAW
Asset-Based Lending: A Practical Guide to Secured Financing
Documenting Secured Transactions: Effective Drafting and Litigation
Equipment Leasing–Leveraged Leasing
Hillman on Commercial Loan Documentation
Maritime Law Answer Book

BANKRUPTCY LAW
Bankruptcy Deskbook
Personal Bankruptcy Answer Book

BUSINESS, CORPORATE & SECURITIES LAW
Accountants’ Liability
Anti-Money Laundering: A Practical Guide to Law and Compliance
Antitrust Law Answer Book
Broker-Dealer Regulation
Conducting Due Diligence in a Securities Offering
Consumer Financial Services Answer Book
Corporate Compliance Answer Book
Corporate Legal Departments: Practicing Law in a Corporation
Corporate Political Activities Deskbook
Corporate Whistleblowing in the Sarbanes-Oxley/Dodd-Frank Era
Covered Bonds Handbook
Cybersecurity: A Practical Guide to the Law of Cyber Risk
Derivatives Deskbook: Close-Out Netting, Risk Mitigation, Litigation
Deskbook on Internal Investigations, Corporate Compliance, and White Collar Issues
Directors’ and Officers’ Liability: Current Law, Recent Developments, Emerging Issues
Doing Business Under the Foreign Corrupt Practices Act
EPA Compliance and Enforcement Answer Book
Exempt and Hybrid Securities Offerings
Fashion Law and Business: Brands & Retailers
Financial Institutions Answer Book: Law, Governance, Compliance
Financial Product Fundamentals: Law, Business, Compliance
Financial Services Regulation Deskbook
Financially Distressed Companies Answer Book
Global Business Fraud and the Law: Preventing and Remediating Fraud and Corruption
Hedge Fund Regulation
Initial Public Offerings: A Practical Guide to Going Public
Insider Trading Law and Compliance Answer Book
Insurance and Investment Management M&A Deskbook
International Corporate Practice: A Practitioner's Guide to Global Success
Investment Adviser Regulation: A Step-by-Step Guide to Compliance and the Law
Life at the Center: Reflections on Fifty Years of Securities Regulation
Mergers, Acquisitions and Tender Offers: Law and Strategies
Mutual Funds and Exchange Traded Funds Regulation
Outsourcing: A Practical Guide to Law and Business
Privacy Law Answer Book
Private Equity Funds: Formation and Operation
Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age
Public Company Deskbook: Complying with Federal Governance & Disclosure Requirements
SEC Compliance and Enforcement Answer Book
Securities Investigations: Internal, Civil and Criminal
 Securities Law and Practice Handbook
The Securities Law of Public Finance
Securities Litigation: A Practitioner's Guide
Social Media and the Law
Soderquist on Corporate Law and Practice
Sovereign Wealth Funds: A Legal, Tax and Economic Perspective
A Starter Guide to Doing Business in the United States
Technology Transactions: A Practical Guide to Drafting and Negotiating Commercial Agreements
Variable Annuities and Variable Life Insurance Regulation

COMMUNICATIONS LAW
Advertising and Commercial Speech: A First Amendment Guide
Sack on Defamation: Libel, Slander, and Related Problems
Telecommunications Law Answer Book

EMPLOYMENT LAW
Employment Law Yearbook
ERISA Benefits Litigation Answer Book
Labor Management Law Answer Book

ESTATE PLANNING AND ELDER LAW
Blattmachr on Income Taxation of Estates and Trusts
Estate Planning & Chapter 14: Understanding the Special Valuation Rules
International Tax & Estate Planning: A Practical Guide for Multinational Investors
Manning on Estate Planning
New York Elder Law
Stocker on Drawing Wills and Trusts

HEALTH LAW
FDA Deskbook: A Compliance and Enforcement Guide
Health Care Litigation and Risk Management Answer Book
Health Care Mergers and Acquisitions Answer Book
Medical Devices Law and Regulation Answer Book
Pharmaceutical Compliance and Enforcement Answer Book

IMMIGRATION LAW
Fragomen on Immigration Fundamentals: A Guide to Law and Practice

INSURANCE LAW
Business Liability Insurance Answer Book
Insurance Regulation Answer Book
Reinsurance Law

INTELLECTUAL PROPERTY LAW
Copyright Law: A Practitioner's Guide
Faber on Mechanics of Patent Claim Drafting
How to Write a Patent Application
Intellectual Property Law Answer Book
Kane on Trademark Law: A Practitioner's Guide
Likelihood of Confusion in Trademark Law
Patent Claim Construction and Markman Hearings
Patent Licensing and Selling: Strategy, Negotiation, Forms
Patent Litigation
Pharmaceutical and Biotech Patent Law
Post-Grant Proceedings Before the Patent Trial and Appeal Board
Substantial Similarity in Copyright Law
Trade Secrets: A Practitioner's Guide
LITIGATION
American Arbitration: Principles and Practice
Class Actions and Mass Torts Answer Book
Electronic Discovery Deskbook
Essential Trial Evidence: Brought to Life by Famous Trials, Films, and Fiction
Expert Witness Answer Book
Evidence in Negligence Cases
Federal Bail and Detention Handbook
How to Handle an Appeal
Medical Malpractice: Discovery and Trial
Product Liability Litigation: Current Law, Strategies and Best Practices
Sinclair on Federal Civil Practice
Trial Handbook

REAL ESTATE LAW
Commercial Ground Leases
Friedman on Contracts and Conveyances of Real Property
Friedman on Leases
Holtzschue on Real Estate Contracts and Closings: A Step-by-Step Guide to Buying and Selling Real Estate
Net Leases and Sale-Leasebacks

TAX LAW
The Circular 230 Deskbook: Related Penalties, Reportable Transactions, Working Forms
The Corporate Tax Practice Series: Strategies for Acquisitions, Dispositions, Spin-Offs, Joint Ventures, Financings, Reorganizations & Restructurings
Foreign Account Tax Compliance Act Answer Book
Internal Revenue Service Practice and Procedure Deskbook
International Tax & Estate Planning: A Practical Guide for Multinational Investors
International Tax Controversies: A Practical Guide
International Trade Law Answer Book: U.S. Customs Laws and Regulations
Langer on Practical International Tax Planning
The Partnership Tax Practice Series: Planning for Domestic and Foreign Partnerships, LLCs, Joint Ventures & Other Strategic Alliances
Private Clients Legal & Tax Planning Answer Book
Transfer Pricing Answer Book

GENERAL PRACTICE PAPERBACKS
Anatomy of a Mediation: A Dealmaker’s Distinctive Approach to Resolving Dollar Disputes and Other Commercial Conflicts
Attorney-Client Privilege Answer Book
Drafting for Corporate Finance: Concepts, Deals, and Documents
Pro Bono Service by In-House Counsel: Strategies and Perspectives
Smart Negotiating: How to Make Good Deals in the Real World
Thinking Like a Writer: A Lawyer’s Guide to Effective Writing & Editing
Working with Contracts: What Law School Doesn’t Teach You

Order now at www.pli.edu
Or call (800) 260-4754 Mon.–Fri., 9 a.m.–6 p.m.

Practising Law Institute
1177 Avenue of the Americas
New York, NY 10036

When ordering, please use Priority Code NWS9-X.
This work is designed to provide practical and useful information on the subject matter covered. However, it is sold with the understanding that neither the publisher nor the author is engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

QUESTIONS ABOUT THIS BOOK?

If you have questions about replacement pages, billing, or shipments, or would like information on our other products, please contact our customer service department at info@pli.edu or at (800) 260-4PLI.

For any other questions or suggestions about this book, contact PLI's editorial department at: plipress@pli.edu.

For general information about Practising Law Institute, please visit www.pli.edu.

Legal Editor: Paul Matsumoto

Copyright © 2006–2017 by Practising Law Institute.


All rights reserved. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written consent of Practising Law Institute.

ISBN: 978-1-4024-2749-7

LCCN: 2006934913
I am excited to present this new edition of *Proskauer on Privacy*. Again, I would like to thank Proskauer Rose LLP for its continued support of this treatise, and the talented group of authors for their annual updates and valuable contributions.

Much has changed since the publication of the first edition of this book. Privacy law continues to rapidly evolve in an increasingly digital environment. The power of technology—the Internet, wireless broadband, streaming video distribution, cloud computing, mobile devices and applications, big-data analytics, targeted advertising—has opened up new possibilities in e-commerce, marketing, communication, and social interactions. At the same time, however, individuals who are “connected” to the digital world via a laptop or mobile device have, in many cases, implicitly or explicitly granted others access to certain web browsing habits and personally identifiable information, data that has become an important asset for business and government agencies alike.

Ever the over-burdened traffic officer, the law is always playing catch-up with technology when it comes to privacy and data security concerns. Privacy laws in the United States remain a patchwork, consisting of common law principles rooted in federal and state constitutional provisions, federal and state statutes aimed at specific areas of concern such as the privacy of health and financial information, and communications privacy laws concerned with limiting access to communications by law enforcement and third parties. These enactments have been supplemented by administrative regulations and enforcement efforts of various administrative agencies such as the Federal Trade Commission and state consumer protection authorities. In addition, many foreign jurisdictions—most notably, the EU—have their own privacy-related laws, requiring multinational corporations and other entities doing business abroad to comply with another set of laws that are sometimes stricter than those in the United States. Filling in the gap, industry self-regulatory efforts, digital privacy advocates, and the market itself have tried to forge solutions that attempt to buffer the burgeoning online economy with reasonable privacy protections.

All of this is what makes privacy and data security such a dynamic area of law, and I hope our avid interest in the field of privacy is reflected in these pages.

**KRISTEN J. MATHEWS**

October 2016
Preface to the First Edition

As the new editor of Proskauer on Privacy, I would like to thank Proskauer Rose LLP for its continued support of this treatise, and my esteemed cast of authors for their annual contributions.

I would also like to thank my former partner Chris Wolf, the former editor of this treatise, for all that he contributed to its previous published versions. In respect for what he and many others have contributed to this volume since its inception, I leave Chris’s original acknowledgments intact below.

KRISTEN J. MATHEWS
June 2010

† † †

In Mark Twain’s The Adventures of Tom Sawyer, when Aunt Polly told Tom Sawyer to whitewash her fence as punishment for playing hooky from school, Tom persuaded his friends to help. In putting together Proskauer on Privacy, I have felt a little bit like Tom Sawyer. Much of the labor in writing this book was borne by others. This treatise would not have been possible if not for my expert friends who decided, like Tom Sawyer’s friends, that it would be fun to do the work. I should hasten to add that organizing, editing, and writing portions of this volume have hardly been punishment for me. This project has helped me immerse myself—even more than my daily practice allows—in the law of a rapidly developing and increasingly important area. It has been an honor and a privilege to contribute to this volume and to edit the submissions by true scholars in the field.

Primary thanks, of course, go to the contributors themselves. They have dealt with difficult deadlines and a demanding editor. And they have all risen to the challenge of writing concise, practical yet thorough explications of their parts of privacy law.

Special thanks also go to my colleagues Rachel Glickman and Tim Tobin, associates in the Washington, D.C. office of Proskauer, to whom many of the administrative and editorial tasks fell. Along with our former colleague David Rappaport, they worked tirelessly to help me get this book done, and I will be forever in their debt. My appreciation also goes to my long-time Administrative Assistant Peggy Castle and Proskauer Legal Assistant Miguel Andolong, as well as to interns
Michael Burton and Matt Mailloux. The editors and staff at PLI made creation of this treatise a real pleasure.

And, finally, my deep appreciation to the Chair of Proskauer Rose LLP and my friend, Allen Fagin, who supported the idea of this project from the very beginning and who made sure that I always had the needed resources to get the job done right.
Kristen J. Mathews is a partner in Proskauer’s New York office, is head of Proskauer’s Privacy and Data Security Practice Group, and is a member of the Technology, Media and Telecommunications Practice Group. For over a decade, Ms. Mathews has specialized in technology, e-commerce, and media-related transactions and advice, with concentrations in the areas of data privacy, data security, direct marketing, and online advertising. She regularly advises clients on a wide range of matters, including privacy and data security compliance, responding to data security breach incidents, preparing privacy and data security policies, data profiling, behavioral marketing, open-source software issues, financial privacy, payment card data security, and telematics. She is ranked as a top practitioner in her field by Chambers USA, Chambers Global, and Legal 500. She is certified as an information privacy professional by the International Association of Privacy Professionals and is the editor of Proskauer’s A Moment of Privacy e-newsletter and its Privacy Law Blog. Ms. Mathews also chairs Proskauer’s annual Proskauer on Privacy Conference.
About the Contributors

David Ames (Chapter 15) is a Director in PricewaterhouseCoopers LLP’s Security Consulting practice based out of Atlanta and specializes in cyber security investigations and security compliance. Within those areas of focus David has significant experience with PCI readiness work and assessments, malware analysis, data forensics, and incident response. David leverages this experience to help his clients define their cyber security strategy, prepare for incident response, perform enterprise threat modeling exercises, and establish sustainable and risk-based PCI compliance programs. David graduated from the University of Georgia with a degree in Management Information Systems; he is a PCI Qualified Security Assessor (QSA) and currently holds the Certified Information Systems Security Professional (CISSP) and GIAC Reverse Engineering Malware (GREM) certifications.

Peta-Anne Barrow (Chapter 14) is co-head of Proskauer’s International Privacy and Data Security Group, resident in the London office. Her practice is based on international privacy issues, and she regularly works with multi-country data privacy and security projects in global human information systems. She also assists clients with complying with the EU Data Protection Directive, the U.K. Data Protection Act, and cross-border transfers of personal data and has substantial knowledge in drafting model contractual clauses to comply with EU law. Peta-Anne also speaks regularly on international data privacy and security matters at in-house and external conferences.

John Beardwood (Chapter 13) is a partner at Fasken Martineau, engaged in a corporate/commercial practice, with an emphasis on outsourcing and procurement, technology, and privacy law–related matters. John is regularly listed among the world’s preeminent Internet and e-commerce lawyers in Who’s Who Legal—The International Who’s Who of Business Lawyers, where, in addition to being referred to as “an authority on outsourcing” in the guide to Internet and E-Commerce Lawyers, he has been identified as being both one of the two most highly nominated Canadian lawyers in the guide and one of the ten “most highly regarded individuals” globally. Mr. Beardwood is also consistently included as a leading lawyer in the
“Internet & e-Commerce” chapter of Who’s Who Legal: Canada. He is listed in Chambers Global—The World’s Leading Lawyers for Business, for information technology as “very effective, efficient and remarkably accessible.” He is consistently recognized in The Best Lawyers in Canada for information technology law and is highly recommended as an outsourcing practitioner in the PLC Which Lawyer? yearbook and in the PLC Outsourcing Handbook. His biography is included in the Canadian Who’s Who. John is the Past President of the International Technology Lawyers Association (“ITechLaw”). John is Co-Chair of the National Technology and Intellectual Property Practice Group; Co-Chair of the National Outsourcing Practice Group; and Vice-Chair of the Privacy and Information Protection Practice Group.

Bruce Boyden (Chapter 6) is an associate professor of law at Marquette University Law School in Milwaukee, Wisconsin, where he teaches and writes in the areas of Internet law, privacy, copyright, and civil procedure. His research primarily focuses on the effect of technological and social change on law, and he has published articles on that issue in the University of Chicago Legal Forum, Cardozo Law Review, George Mason Law Review, Alabama Law Review, and Arkansas Law Review. He also contributes to two blogs: Madisonian.net and the Marquette Law Faculty Blog. Prior to entering academia, Professor Boyden practiced law at Proskauer Rose LLP in its Washington, D.C. and New York offices. Professor Boyden is a 1997 graduate of Yale Law School and a member of the New York, District of Columbia, and Wisconsin Bars.

Courtney Bowman (Chapter 14) is an associate in the Litigation Department at Proskauer Rose LLP. She assists clients in a wide variety of industries with issues related to privacy, data security, and general commercial litigation. Courtney is a regular contributor to Proskauer’s Privacy Law Blog and frequently speaks to the media on issues relating to international privacy and data security, and has authored articles on data security and e-commerce issues in the Middle East. She is accredited by the International Association of Privacy Professionals as a certified information privacy professional (CIPP) in both the U.S. private sector (CIPP/US) and Europe (CIPP/E).

Roger A. Cohen (Chapter 3) is a senior counsel in the Health Care Department at Proskauer Rose LLP. He represents healthcare providers, life science companies, health information technology companies, and others in a wide array of healthcare regulatory matters. Roger has significant experience in, among other things, matters relating to fraud and abuse, reimbursement, and health information
security and privacy. Roger has also played a lead role in the successful defense of healthcare providers in a number of significant government investigations and in litigation of actions under the False Claims Act. In 2014, Law360 recognized Roger as one of five “Rising Stars” in the nation in the field of healthcare law. SuperLawyers named Roger a New York Metro “Rising Star” in healthcare law in both 2013 and 2014.

Erika C. Collins (Chapter 14) is a partner in the Proskauer labor law department and co-chair of the international labor and employment group. Ms. Collins provides strategic advice and counseling to multinational employers on a wide range of global employment law and human resources matters. Ms. Collins assists employers with global employment issues and advises companies when they are expanding or downsizing around the world. She has handled office openings and workforce expansions, employment terminations, including mass lay-offs and office closures; executive hirings and terminations and the attendant negotiations; and has prepared employment, separation, expatriate, and consulting agreements in dozens of countries. She conducts multi-country audits of employment laws and practices, and provides strategic compliance advice regarding a wide range of issues, including data privacy, fixed-term contracts, M&A transactions, outsourcing, and working time and leave regulations. She has been named in The International Who’s Who of Management Labour & Employment Lawyers, 2007 to 2014. She is recognized as a leading New York employment defense lawyer in the 2007 to 2014 Chambers USA America’s Leading Lawyers for Business, and was selected for inclusion in the 2007 to 2014 New York Super Lawyers Magazine; The International Who’s Who of Business Lawyers, 2009 to 2014; and The Best Lawyers in America, 2010 to 2014.

Scott P. Cooper (Chapter 5) is a senior litigation partner in the Los Angeles office of Proskauer Rose LLP. In addition to heading Proskauer’s privacy and data security practice on the West Coast, Scott is an experienced litigator, handling disputes of all kinds affecting the entertainment and media industry. For such clients, Scott has been involved in precedent-setting copyright cases. He also handles commercial disputes, antitrust, and securities law matters for the entertainment industry. Scott also is known for his representation in significant art law cases, including a matter on behalf of the Republic of Austria before the United States Supreme Court.

Margaret A. Dale (Chapter 17) is a partner in Proskauer’s Litigation Department. Her practice focuses on complex commercial disputes,
privacy and data security, corporate defense and investigations, and securities litigation and enforcement. In privacy and data security-related matters, Margaret has represented Internet retailers, arts-related organizations, financial institutions, and consumer product companies, among others, in a wide range of matters including class action lawsuits stemming from data breaches, and disputes involving the CAN-SPAM Act, and the Computer Fraud and Abuse Act, among others. Margaret is a frequent speaker on various topics, including privacy and data security.

Mary Edquist (Chapter 7) is an attorney in the Business Department of McDonald Hopkins LLC, and is based in the firm’s Cleveland office. Mary’s practice focuses primarily on business counseling, particularly in the areas of national security, international trade, regulatory compliance, mergers and acquisitions, government contracting issues, and commercial finance and lending. Her experience includes handling international transactions, export control and compliance matters, national security issues, government disclosures, and internal investigations. Previously, Mary worked as a Deputy Public Defender for the Office of the Colorado State Public Defender and served as an attorney with the United Nations International Criminal Tribunal for the former Yugoslavia. She received an LL.M. in National Security Law from Georgetown University Law Center, a J.D. from the University of Denver Sturm College of Law, an M.A. in International Security Studies from the University of Denver Josef Korbel School of International Studies, and a B.A. from Cornell University.

Daniel Fabiano (Chapter 13) is a partner at Fasken Martineau. His practice focuses on technology, procurement, and information protection matters, with particular emphasis on the health sector. Daniel frequently advises corporate and government clients on privacy law compliance and access to information matters (at both the federal and provincial level). He was also recently seconded to a major provincial health agency, where he advised on privacy and freedom of information compliance. Daniel was the lead author of a comprehensive health sector privacy and freedom of information manual, which is in use at all hospitals in Ontario.

Robert Forbes (Chapter 10) is the Assistant General Counsel of the Washington Redskins. Prior to joining the Redskins, he was an associate in the Litigation Department of Proskauer Rose LLP, where he was a member of the firm’s Privacy and Data Security Practice Group. Robert is a 2007 graduate of the University of Virginia School of Law.
Steven R. Gilford [Chapter 16] is a partner in Proskauer’s Litigation Department, co-head of the Insurance Recovery & Counseling Group, and head of the Chicago office. Steven has broad experience in trial court and appellate litigation, domestic and international arbitration, mediation, and other forms of alternative dispute resolution. His practice focuses on representing policyholders in a wide range of insurance issues, including CGL, D&O, E&O, employment practices, first-party property, business interruption, and cyber risks. Steven is a nationally recognized practitioner in the areas of insurance and reinsurance, having represented clients in all areas of the insurance industry, including policyholders, insurers, reinsurers, captives, and brokers. According to Chambers USA, clients and peers recognize Steve for his “great strategic acumen” and say he is “the person to go to when you have a large conceptual problem to get around.” Leading Lawyers Magazine named Steven one of the “Top Business Lawyers in Illinois—Insurance, Insurance Coverage & Reinsurance Law,” in 2010, and he has been ranked among the Best Lawyers in America 2006–2013 and by Illinois Super Lawyers 2005–2012. In addition to his broad experience in insurance, Steven has worked across a broad range of industries and subject areas, including major contract and commercial disputes, consumer class actions, antitrust and securities cases, technology outsourcing disputes, defamation, trademark, and trade secret matters, and restrictive covenants. Steven received his J.D., With Distinction, Order of the Coif, from Duke University School of Law, where he was an Administrative Law Editor and Editorial Board Member of the Duke University Law Journal; he has an M.A. in Public Policy Sciences from Duke University; and an A.B., summa cum laude, from Dartmouth College.

Michael Hintze [Chapter 10] is a partner at Hintze Law PLLC with a focus on privacy and data protection law, policy, and strategy. Formerly, Mr. Hintze was Chief Privacy Counsel and an Associate General Counsel in Microsoft Corporation’s Legal and Corporate Affairs (LCA) group. He joined Microsoft in 1998, and his practice included a number of regulatory and public policy issues, focused on privacy and related matters worldwide. He also teaches privacy law at the University of Washington School of Law, serves as an advisor to the American Law Institute’s project on Information Privacy Principles, and is on the Educational Advisory Board of the International Association of Privacy Professionals. Prior to joining Microsoft, Mr. Hintze was an associate with the Washington, D.C.-based law firm of Steptoe & Johnson LLP, where his practice focused on export controls, the regulation of encryption technologies, and commercial matters for technology companies. He joined the firm following a judicial clerkship on the Washington State Supreme Court. Mr. Hintze is a
graduate of the University of Washington and the Columbia University School of Law, where he served as editor in chief of the *Columbia Human Rights Law Review*. He is a regular speaker on data privacy issues and has published articles on a range of subjects including privacy, U.S. export regulations, and capital punishment.

**Marcia Hofmann** (Chapter 4) is an attorney who litigates, writes, and speaks about a broad range of technology law issues, including computer security, electronic privacy, free expression, and intellectual property. In 2013, she launched a boutique law practice focusing on electronic privacy, computer crime and security, free expression, and intellectual property. Prior to that, she was a senior staff attorney at the Electronic Frontier Foundation, where she continues to serve as special counsel. She is also a non-residential fellow at Stanford’s Center for Internet and Society and an adjunct professor at University of California Hastings College of the Law.

**Nuala O’Connor Kelly** (Chapter 12) is the President & CEO of the Center for Democracy & Technology, a global nonprofit committed to advancing digital rights. Prior to her current position, her most recent corporate experience was at Amazon.com, where she served as Vice President, Compliance & Consumer Trust, and Associate General Counsel Data & Privacy Protection. In 2005, she was appointed chief privacy leader of General Electric. In that capacity, Ms. O’Connor Kelly led global privacy policy and practice for one of the world’s largest diversified multinational companies. Prior to joining GE, O’Connor Kelly was appointed Chief Privacy Officer of the U.S. Department of Homeland Security in April 2003. As the first statutorily required chief privacy officer for any federal agency, O’Connor Kelly had oversight of all privacy policy matters for the department, including compliance with the Privacy Act of 1974, the Freedom of Information Act of 1966 (as amended), and the completion of Privacy Impact Assessments on new programs and data collection technologies. Before joining DHS, O’Connor Kelly served as Chief Privacy Officer for the U.S. Department of Commerce. While at Commerce, she also served as Chief Counsel for Technology and as Deputy Director of the Office of Policy and Strategic Planning.

Prior to public service, O’Connor Kelly served as Vice President–Data Protection and Chief Privacy Officer for Emerging Technologies for the online media services company DoubleClick. O’Connor Kelly helped found the company’s first data protection department and was responsible for the creation of privacy and data protection policies and procedures throughout the company and for the company’s clients and partners. O’Connor Kelly also served as the company’s first deputy general counsel for privacy. Ms. O’Connor Kelly has practiced law with
the firms of Sidley & Austin, Hudson Cook, and Venable, Baetjer, Howard & Civiletti in Washington, D.C. She is a member of the Board of Directors of the International Association of Privacy Professionals. Ms. O’Connor Kelly received her A.B. from Princeton University, Master of Education from Harvard University, and J.D. from the Georgetown University Law Center. She is a member of the bars of Washington, D.C. and Maryland.

Mark MacCarthy (Chapter 15) is an adjunct faculty member at Georgetown University’s Communication, Culture, and Technology Program. He teaches courses and conducts research in information privacy, global Internet freedom, tech policy, trade, and the development of electronic media. He also teaches courses in political philosophy, philosophy and privacy, and philosophy and free speech in the Philosophy Department. He is also an adjunct member of Georgetown University’s Department of Philosophy, where he teaches courses in political philosophy. He does research and consults in the areas of information privacy and security, electronic commerce, and other technology policy issues. He was Senior Vice President, Visa Inc., where he represented Visa before Congress, the administration, the Federal Trade Commission, the banking regulators, and other regulatory agencies. He was responsible for Visa’s public policy initiatives and strategies in the areas of data security and privacy, electronic commerce liability issues such as Internet gambling and Internet pharmacies, patent reform, international trade, and product innovations such as Visa’s contactless payment platform and prepaid cards. He regularly testified on behalf of Visa before various congressional committees and regulatory agencies. Prior to joining Visa, Mr. MacCarthy was a principal and senior director with the Wexler Group, a Washington government affairs consulting firm, where he worked with a variety of clients on electronic commerce, privacy, and telecommunications. In addition, Mr. MacCarthy was Vice President in charge of Capital Cities/ABC’s Washington Office from 1988 to 1994. From 1981 to 1988, he was a professional staff member of the Committee on Energy and Commerce, U.S. House of Representatives, where he handled communications policy and other issues for the Chairman of the Committee, Representative John D. Dingell.

Cécile Martin (Chapter 14) is Special International Labor & Employment Counsel in Proskauer’s Paris office, and is a member of the firm’s International Labor & Employment Group and the Privacy & Data Security Group. She has experience with all employment law aspects, with extensive experience in data privacy law, and is generally responsible for cases involving privacy issues at the crossroads of
employment law and the law of new technologies, particularly issues concerning the cyber-surveillance of employees and the dismissal of employees for abusing technologies put at their disposal during their work time. She also deals with issues related to international transfer of data. Prior to joining Proskauer, Cécile served as in-house counsel for the legal department of the French Data Protection Agency (CNIL). She was a speaker, on several occasions, for the American Bar Association’s Technology at the Workplace conference, and she is Co-Chair of the KnowledgeNet of the IAPP in France.

**Kristen J. Mathews** (Editor; author Chapters 2 and 5) is a partner in Proskauer’s New York office, is head of Proskauer’s Privacy and Data Security Practice Group, and is a member of the Technology, Media and Telecommunications Practice Group. For over a decade, Ms. Mathews has specialized in technology, e-commerce, and media-related transactions and advice, with concentrations in the areas of data privacy, data security, direct marketing, and online advertising. She regularly advises clients on a wide range of matters, including privacy and data security compliance, responding to data security breach incidents, preparing privacy and data security policies, data profiling, behavioral marketing, open-source software issues, financial privacy, payment card data security, and telematics. She is ranked as a top practitioner in her field by *Chambers USA*, *Chambers Global*, and *Legal 500*. She is certified as an information privacy professional (CIPP) by the International Association of Privacy Professionals and sits on its Certification Advisory Board. She is the editor of Proskauer’s *A Moment of Privacy* e-newsletter and its Privacy Law Blog. Ms. Mathews also chairs Proskauer’s annual Proskauer on Privacy Conference.

**Kathleen M. McKenna** (Chapter 9) is a partner in the Labor and Employment Law Department of Proskauer Rose LLP in New York. In addition to focusing on workplace privacy issues, Kathleen has extensive experience litigating employment disputes of all types and has significant jury trial experience. Kathleen also has significant experience dealing with traditional labor matters. In addition to lecturing regularly on employment law topics, Kathleen also has published articles on subjects including sexual harassment, arbitration provisions in employment agreements, religious accommodations, the ADA, age discrimination, and personal liability for discrimination. Kathleen graduated from Boston College Law School in 1978 and earned her undergraduate degree summa cum laude at St. Peter’s College in 1975. In 2004, Kathleen McKenna was elected to the prestigious College of Labor and Employment Lawyers.
Jeremy M. Mittman (Chapter 14) is William Morris Endeavor/IMG’s global employment counsel, based in Los Angeles, California, where he is responsible for overseeing domestic and international employment and employee data privacy-related matters. WME is the world’s largest talent agency, and IMG is a global sports and media business with offices in thirty jurisdictions. Prior to joining WME/IMG, Mr. Mittman was an associate at the international law firm of Proskauer Rose LLP, where he was the Co-Chair of the firm’s International Privacy Group, and a member of its International Labor Group and its Privacy and Data Security Practice Group, where he counseled multinational employers on cross-border human resources and data privacy issues affecting multiple countries and jurisdictions. Mr. Mittman received his B.A. from the University of Pennsylvania in 1999 and his J.D. from the University of Southern California in 2003.

Brian Morrison (Chapter 7) is an executive with General Dynamics, a global aerospace and defense company. He has worked in the field of intelligence law since 2004. A former Assistant General Counsel at the Central Intelligence Agency, Brian served as Deputy Staff Director and General Counsel for the Permanent Select Committee on Intelligence in the U.S. House of Representatives. From 2011 to 2012, he served as Deputy Assistant Secretary of Defense for Legislative Affairs. He has taught as an adjunct professor of law at Georgetown University Law School. He is a graduate of the Harvard Law School and Brandeis University.

Kenneth P. Mortensen (Chapter 12), at the time he contributed to this treatise, was the Acting Chief of Staff for the Privacy Office at the U.S. Department of Homeland Security. Ken joined the Privacy Office in 2005 as the Senior Advisor for privacy policy dealing with information sharing, data security and integrity, and border protection. In that role, he advised the Chief Privacy Officer and Department senior leadership about privacy matters concerning the use, harmonization, and implementation of technologies using risk assessment management techniques. Additionally, he researches the privacy implications of the use of new technologies, including biometrics, radio frequency identifiers, data mining, federated identity management, and metadata collection. Prior to his government service, Ken was a founding and managing partner of the law firm Harvey & Mortensen, which was located in Berwyn, Pennsylvania in the Philadelphia metropolitan region. From 1997 through 2005, Ken served as outside counsel for the Pennsylvania Office of Attorney General regarding technology and Internet matters. Ken earned his B.S.E. in electrical and computer engineering from Drexel University, his J.D. from Villanova University School of Law, and his M.B.A. from Villanova University College of Commerce and Finance.
David A. Munkittrick (Chapters 17 & 18) is an associate in the Litigation Department of Proskauer Rose LLP in New York and is a member of Proskauer’s Antitrust Group as well as the Privacy and Data Security Practice Group. David has experience in a variety of complex litigation matters, and in privacy, intellectual property, and appellate issues. He has particular experience with privacy laws applicable in the retail setting and is a regular contributor to Proskauer’s Privacy Law Blog. David is the author of “Nonprofit Education: A Historical Basis for Tax Exemption in the Arts,” published in the New York State Bar Association Entertainment, Arts, and Sports Law Journal (2010), and “Music as Speech: A First Amendment Category Unto Itself,” published in the Federal Communications Law Journal (2010). He is a 2010 graduate of the Indiana University Maurer School of Law and earned undergraduate degrees in history and piano performance from Oberlin College and Conservatory of Music.

Anthony J. Oncidi (Chapter 9) is a partner at Proskauer Rose LLP and Chair of the Labor and Employment Department in the firm’s Los Angeles office, as well as a member of the Privacy and Data Security Practice Group. Tony represents employers in all aspects of labor relations and employment law. A substantial portion of his practice involves the defense of employers in class action wage and hour, employment discrimination, and wrongful termination litigation in both state and federal court. He also has particular experience in trade secret and unfair competition litigation and the defense of sexual harassment, discrimination, breach of contract, violation of privacy, and defamation lawsuits. Tony is the author of the treatise “Employment Discrimination Depositions” (Juris Pub. 2013; www.jurispub.com). Los Angeles Magazine has identified Mr. Oncidi as one of the “Top 100 Southern California Super Lawyers,” and he is listed in The Best Lawyers in America and described as one of “America’s Leading Business Lawyers” by Chambers USA (“Band 1”). Tony has served as an Adjunct Professor of Law at the University of Southern California Law School and as a guest lecturer at the UCLA School of Law. He received his undergraduate degree, cum laude, Phi Beta Kappa, from Pomona College, and his law degree from the University of Chicago Law School.

Pieter Penning (Chapter 15) is a partner in PricewaterhouseCoopers LLP’s Advisory Security practice based out of Atlanta and specializes in security threat and vulnerability management and security compliance. Pieter has extensive experience in leading payment card industry (PCI) compliance, as well as payment card data breach response and remediation engagements at some of the largest organizations in the United States. Pieter specializes in security controls rationalization, compliance cost and risk reduction, and helping organizations develop
and implement sustainable information security compliance programs by leveraging his extensive experience in regulatory, industry, and global compliance requirements and frameworks, such as HIPAA, privacy, PCI, and ISO 27001/2. Pieter is a PCI Qualified Security Assessor, Certified Information Systems Auditor, and holds the Certified in Risk and Information Systems Control and ISO 27001 Lead Implementer certifications. He received his postgraduate degree in Information Science, cum laude, from the University of Pretoria in South Africa.

Nancy L. Savitt (Chapter 11) is an attorney in private practice. Ms. Savitt’s practice focuses on both complex commercial litigation and Internet privacy issues. She served as an Assistant United States Attorney in the Southern District of New York, Civil Division, for many years, where she represented the interests of the United States in civil litigation, regulatory, constitutional, and civil rights matters, and appellate practice. She currently serves as a volunteer mediator in the United States District Court for the Southern District of New York alternative dispute resolution program. Ms. Savitt received her law degree, cum laude, from the New York University School of Law.

Daniel J. Solove (Chapter 1) is the John Marshall Harlan Research Professor of Law at the George Washington University Law School. He is also the founder of TeachPrivacy, a company that provides privacy and data security training programs to businesses, schools, healthcare institutions, and other organizations. Professor Solove is co-reporter of the American Law Institute’s Restatement of Information Privacy Principles. An internationally known expert in privacy law, Solove has been interviewed and quoted by the media in several hundred articles and broadcasts, including the New York Times, Washington Post, Wall Street Journal, USA Today, Chicago Tribune, the Associated Press, ABC, CBS, NBC, CNN, and NPR. Professor Solove is the author of several books, including, Nothing to Hide: The False Tradeoff Between Privacy and Security (Yale University Press 2011), Understanding Privacy (Harvard University Press 2008), The Future of Reputation: Gossip, Rumor, and Privacy on the Internet (Yale University Press 2007), and The Digital Person: Technology and Privacy in the Information Age (NYU Press 2004). His books have been translated into many languages. He has also written several textbooks including Information Privacy Law (Aspen, 5th ed. 2015), Privacy Law Fundamentals (IAPP, 3d ed. 2015), Privacy and the Media (Aspen, 2d ed. 2015), Privacy, Law Enforcement, and National Security (Aspen, 1st ed. 2015), Consumer Privacy and Data Protection (Aspen,
Gabriel M.A. Stern (Chapter 13) is a senior associate at Fasken Martineau who practices in the area of information technology law as part of the firm’s Business Law section and Information Technology group. Gabriel graduated from the University of Toronto Faculty of Law, where he served as editor in chief of the University of Toronto Faculty of Law Review. Gabriel has also obtained a Ph.D. from McGill University, where he has taught as a sessional lecturer. Gabriel summered and articled with Fasken Martineau and joined the firm as an associate in September 2008. While summering with the firm, Gabriel was seconded to TD Bank.

Hugo Teufel III (Chapter 8) is Senior Counsel, Global Privacy, at the Raytheon Company. Previously, he was co-lead of the U.S. privacy practice at PricewaterhouseCoopers LLP, focusing on commercial, federal government, and international privacy matters. From 2006 to 2009, he served as Chief Privacy Officer for the U.S. Department of Homeland Security, with primary responsibility for privacy policy at the department, reporting directly to the secretary and deputy secretary. Hugo was one of two DHS principals on the High Level Contact Group, a joint U.S.–EU effort on transatlantic exchanges of data, and he regularly interacted with various European data protection authorities, parliamentarians, and the European Commission. Hugo graduated from the Washington College of Law of the American University and was the Senior Articles Editor of The Administrative Law Journal. He also holds a master’s degree in national security and strategic studies from the Naval War College. A member of the bars of Colorado and Maryland (inactive), Hugo is CIPP/G and CIPP/US certified with the International Association of Privacy Professionals. Hugo also currently serves as a judge advocate in the Army National Guard.
Table of Chapters

Chapter 1    A Brief History of Information Privacy Law
Chapter 2    Financial Privacy Law
Chapter 3    Medical Privacy
Chapter 4    Federal Trade Commission Enforcement of Privacy
Chapter 5    State Privacy Laws
Chapter 6    Privacy of Electronic Communications
Chapter 7    The Foreign Intelligence Surveillance Act
Chapter 8    Privacy and Homeland Security
Chapter 9    Workplace Privacy Law
Chapter 10   Privacy and Commercial Communications
Chapter 11   The Children’s Online Privacy Protection Act (COPPA)
Chapter 12   The Privacy Act of 1974 and Its Progeny
Chapter 13   Canadian Privacy Law
Chapter 14   International Privacy Law
Chapter 15   Compliance with the Payment Card Industry Data Security Standard
Chapter 16   Insurance Coverage for Data Breaches and Unauthorized Privacy Disclosures
Chapter 17   Data Breach Litigation
Chapter 18   Location Privacy: Technology and the Law
Preface to the Second Edition .............................................................. vii
Preface to the First Edition ................................................................. ix
About the Editor ..................................................................................... xi
About the Contributors ........................................................................ xiii
Table of Chapters ................................................................................... xxv
Introduction .......................................................................................... lxvii

Chapter 1  A Brief History of Information Privacy Law

Daniel J. Solove

§ 1:1 Introduction .................................................................................. 1-3
§ 1:2 Colonial America .......................................................................... 1-4
§ 1:3 The Nineteenth Century ............................................................... 1-5
  § 1:3.1 New Threats to Privacy ......................................................... 1-5
    [A] The Census and Government Records ................................... 1-6
    [B] The Mail .............................................................................. 1-6
    [C] Telegraph Communications ............................................ 1-7
  § 1:3.2 The Fourth and Fifth Amendments .................................... 1-8
  § 1:3.3 Privacy of the Body ............................................................. 1-9
  § 1:3.4 Warren and Brandeis’s “The Right to Privacy” .............. 1-10
§ 1:4 The Twentieth Century .............................................................. 1-12
  § 1:4.1 1900 to 1960 ........................................................................ 1-12
    [A] Warren and Brandeis’s Privacy Torts .................................. 1-12
    [A][1] Early Recognition ......................................................... 1-12
    [A][2][a] Intrusion upon Seclusion ........................................... 1-13
    [A][2][b] Public Disclosure of Private Facts .......................... 1-14
    [A][2][c] False Light ............................................................... 1-15
    [A][2][d] Appropriation ........................................................... 1-15
    [B] The Emergence of the Breach of Confidentiality Tort .... 1-16
    [C] The Growth of Government Record Systems ............... 1-17
    [D] The Telephone and Wiretapping ....................................... 1-17
§ 1:5 The Twenty-First Century .............................................. 1-39
§ 1:5.1 After September 11: Privacy in a World
of Terror ........................................................................ 1-39
  [A] The USA PATRIOT Act of 2001 ............................. 1-39
  [B] The FISA “Wall” ................................................. 1-40
  [D] The Real ID Act of 2005 ...................................... 1-41
  [E] NSA Warrantless Surveillance; Edward Snowden Revelations ........................................ 1-42
§ 1:5.2 New Directions in Fourth Amendment Jurisprudence ........................................ 1-42
§ 1:5.3 Expansion of Consumer Privacy Protections ........ 1-43
  [A] The Rise of the Privacy Profession and the Chief Privacy Officer ........................................ 1-43
  [C] The National Do-Not-Call Registry ....................... 1-44
  [D] The CAN-SPAM Act of 2003 ............................... 1-44
  [E] Tort Law ................................................................ 1-44
  [F] Privacy Policies and Contract Law ....................... 1-45
  [G] FTC Enforcement ............................................... 1-45
  [H] FCC Enforcement ................................................ 1-46
  [I] The First Amendment and Privacy Law ................ 1-46
§ 1:5.4 The Rise of Data Security Law............................... 1-47
§ 1:5.5 The Launch and Evolution of HIPAA ..................... 1-48
§ 1:5.6 Education Privacy Comes of Age ......................... 1-48
§ 1:5.7 International Privacy Law ................................. 1-49
  [B] International Data Protection Laws ....................... 1-49
  [C] Canada’s Anti-Spam Legislation (CASL) ................ 1-50
  [D] The Right to Be Forgotten .................................... 1-50
  [E] The Sinking of Safe Harbor ................................. 1-50
  [F] The General Data Protection Regulation (GDPR) .... 1-50
§ 1:6 Conclusion .......................................................... 1-51

(Proskauer, Rel. #1, 5/17) xxix
Chapter 2  Financial Privacy Law

Kristen J. Mathews

§ 2:1  Summary and Introduction .................................................. 2-3
§ 2:1.1  Evolution of Financial Privacy Law Parallels
Developments in Computing ........................................ 2-4
§ 2:2  Fair Credit Reporting Act and the Fair and Accurate
Credit Transactions Act .................................................. 2-5
§ 2:2.1  Purpose and Background of the Fair Credit
Reporting Act ...................................................................... 2-5
§ 2:2.2  Coverage Under the FCRA ............................................. 2-6
[A] Definition of “Consumer” Under the FCRA ...... 2-6
[B] Definition of “Consumer Report” Under the FCRA ... 2-7
[C] Definition of “Consumer Reporting Agency”
Under the FCRA ............................................................... 2-10
§ 2:2.3  Permissible Use and Disclosure of Consumer
Reports: The Obligation to Protect Against
Unauthorized Access or Use of Consumer
Information ........................................................................ 2-13
§ 2:2.4  General Procedural Requirements for CRAs
Under the FCRA ............................................................... 2-16
§ 2:2.5  Procedural Requirements for CRAs When
Preparing and Issuing Consumer Reports for
Employment Purposes ..................................................... 2-17
§ 2:2.6  Notice and Disclosure Requirements for CRAs
Under the FCRA ............................................................... 2-18
§ 2:2.7  Unique Obligations with Respect to
Investigative Consumer Reports ........................................ 2-19
§ 2:2.8  Obligations for Users of Consumer Reports
Under the FCRA ............................................................... 2-20
§ 2:2.9  Obligations for Resellers of Consumer Reports
Under the FCRA ............................................................... 2-23
§ 2:2.10 Consumer Rights Under the FCRA to Dispute
Information Contained in Consumer Reports .... 2-23
§ 2:2.11 Security Requirements of the FCRA Pertaining
to Consumer Fraud and Identity Theft ................... 2-25
§ 2:2.12 Affiliate Marketing Limits Under FACTA ............ 2-31
[A] Opt-Out Requirements ........................................ 2-32
[B] Exceptions................................................................. 2-33
[C] Delivery of Opt-Out Notices ..................................... 2-34
[D] Reasonable Opportunity and Means to Opt Out..... 2-34
[E] Duration of Opt-Out .................................................. 2-35
[F] Model Forms and Safe Harbor ............................... 2-35
§ 2:2.13 FACTA’s Identity Theft Red Flags and Notices
of Address Discrepancy Rules ........................................ 2-36
[A] Identity Theft Red Flags ........................................ 2-36
[B] Scope of the Red Flag Rules ..................................... 2-37
Table of Contents

[C] Examples of Red Flags ............................................. 2-39
[D] Change of Address Requests .................................... 2-41
[E] Address Discrepancy Notices ................................... 2-42
§ 2:2.14 Preemption of State Law by the FCRA ................. 2-43
§ 2:2.15 Penalties for Violations of or Noncompliance with the FCRA ........................................... 2-46
§ 2:3 Right to Financial Privacy Act .................................. 2-47
  § 2:3.1 Purpose and History of the Right to Financial Privacy Act .......................................... 2-47
  § 2:3.2 Procedural Operation of the RFPA ....................... 2-48
  § 2:3.3 Substantive Aspects of the RFPA ......................... 2-50
  § 2:3.4 Interplay with State Statutes ............................ 2-51
§ 2:4 Gramm-Leach-Bliley Act ....................................... 2-53
  § 2:4.1 Purpose and History of the Gramm-Leach-Bliley Act ........................................... 2-53
  § 2:4.2 Internal Procedures and Systems to Ensure Confidentiality of Information ..................... 2-53
  § 2:4.3 Financial Institution’s Notice Obligations .......... 2-62
  § 2:4.4 Required Substance of Notice ........................... 2-67
    [A] Parties Who Must Serve Customers with Notice .................................................. 2-67
  § 2:4.5 Limitations on Disclosure ................................ 2-69
    [A] Customer Must Opt Out of Third-Party Disclosures ............................................. 2-69
    [B] Exceptions to Opt-Out Requirement ........................ 2-70
  § 2:4.6 Enforcement of the GLBA's Privacy Provisions ...... 2-71
  § 2:4.7 GLBA's Relationship to Other Laws .................... 2-72
    [A] GLBA Does Not Preempt State Laws ...................... 2-72
    [B] GLBA's Relationship with Other Federal Privacy Statutes ..................................... 2-73
§ 2:5 Wall Street Reform and Consumer Protection Act ....... 2-75
  § 2:5.1 Purpose and Background of Wall Street Reform and Consumer Protection Act .................. 2-75
  § 2:5.2 Scope of CFPB Authority ................................... 2-75
  § 2:5.3 Powers and Duties of the CFPB ......................... 2-78
    [A] Rulemaking Authority ........................................ 2-78
    [B] Evaluation of Existing Standards ......................... 2-78
    [C] Regulation of Unfair, Deceptive, and Abusive Acts or Practices ................................ 2-79
    [D] Examination of Financial Industry Participants ........ 2-79
  § 2:5.4 Enforcement Authority of the CFPB .................... 2-80
§ 2:6 Bank Secrecy Act .................................................. 2-81
  § 2:6.1 Purpose and Background of the Bank Secrecy Act ........................................... 2-81
  § 2:6.2 BSA Requirements ........................................... 2-82
Chapter 3 Medical Privacy

Roger A. Cohen

§ 3:1 Introduction ............................................................................................... 3-3

§ 3:2 HIPAA Administrative Simplification ......................................................... 3-3

§ 3:2.1 Background .............................................................................................. 3-3

§ 3:2.2 Definitions ................................................................................................ 3-4

§ 3:2.3 HIPAA Privacy .......................................................................................... 3-7

[A] Basic Rules .................................................................................................... 3-7

[B] Limitations on Sale of PHI ........................................................................... 3-7

[C] Limitation on Use of PHI for Paid Marketing .............................................. 3-7

§ 3:2.4 HIPAA Security: Basic Rules ................................................................. 3-9

§ 3:2.5 Business Associates ................................................................................. 3-10

§ 3:2.6 HIPAA Security Breach Notification ....................................................... 3-11

§ 3:2.7 Sanctions for Violations of Privacy and Security Rules ................................ 3-13

§ 3:3 State Law and HIPAA Privacy Preemption .............................................. 3-18

§ 3:4 Heightened Protection for Specialized Types of Medical Information .......... 3-20

§ 3:4.1 Communicable Diseases ......................................................................... 3-20

[A] HIV/AIDS ....................................................................................................... 3-20

[B] Confidentiality and Disclosure of HIV Test Results ...................................... 3-21

§ 3:4.2 Authorized Disclosure .............................................................................. 3-22

§ 3:4.3 Remedies for Breach of Confidentiality ................................................. 3-23

§ 3:4.4 Sexually Transmitted Disease ................................................................. 3-26

§ 3:4.5 Tuberculosis .............................................................................................. 3-28

§ 3:4.6 Genetic Information .................................................................................. 3-30

[A] Genetic Discrimination .................................................................................. 3-30

[B] DNA Sampling by Law Enforcement ............................................................ 3-31

§ 3:5 Privacy of Substance Abuse Records ......................................................... 3-32

§ 3:5.1 Introduction .............................................................................................. 3-32

§ 3:5.2 Scope of Applicability .............................................................................. 3-32

§ 3:5.3 Exceptions to Substance Abuse Confidentiality Laws ................................ 3-34

§ 3:5.4 Other Exceptions Permitting Information Release ................................... 3-35

[A] Release with Patient’s Consent ....................................................................... 3-35

[B] Voluntary Disclosure to the Criminal Justice System ..................................... 3-36

[C] Release Without a Patient’s Consent ............................................................. 3-36

[D] Releases Authorized by a Court Order ......................................................... 3-37

[E] Request for Records in a Criminal Proceeding .............................................. 3-38

[E][1] Confidential Information ............................................................................ 3-39

§ 3:5.5 Conclusion ............................................................................................... 3-40

§ 3:6 Medical Privacy at Common Law ............................................................... 3-41
§ 3:6.1 Actions Arising Out of the Disclosure of Confidential Medical Information........................... 3-41
   [A] Theory of Recovery.................................................. 3-41
   [B] Exceptions to Liability ............................................. 3-43

§ 3:6.2 The Duty to Warn ................................................... 3-45

§ 3:7 Privilege.......................................................................... 3-47

§ 3:7.1 State Law..................................................................... 3-47
   [A] Physician-Patient Privilege....................................... 3-47
      [A][1] Majority of States Have Enacted Privilege by Statute.................................................. 3-47
      [A][2] Scope of the Privilege ........................................ 3-48
      [A][2][a] Types of Providers Covered ......................... 3-48
      [A][2][b] Subject Matter of the Privilege ...................... 3-48
      [A][2][c] Who May Assert the Privilege ....................... 3-49
      [A][2][d] Waiver.......................................................... 3-49
      [A][2][e] Exceptions/Exemptions ................................ 3-50
   [B] Psychotherapist-Patient Privilege ............................. 3-51
      [B][1] Every State Has Enacted Privilege by Statute ...... 3-51
      [B][2] Scope of the Privilege ........................................ 3-51
      [B][2][a] Types of Providers Covered ......................... 3-51
      [B][2][b] Subject Matter of the Privilege ...................... 3-52
      [B][2][c] Who May Assert the Privilege ....................... 3-52
      [B][2][d] Waiver.......................................................... 3-53
      [B][2][e] Exceptions/Exemptions ................................ 3-53

§ 3:7.2 Federal Law.............................................................. 3-54
   [A] Psychiatrist-Patient Privilege.................................... 3-54
      [A][1] Rule .................................................................. 3-54
      [A][2] Waiver ............................................................. 3-55
      [A][3] Exceptions ....................................................... 3-55
      [A][3][a] The Dangerous-Patient Exception .................. 3-56
      [A][3][b] The Crime-Fraud Exception ............................ 3-56
      [A][3][c] Other Exceptions ........................................... 3-57
   [B] Physician-Patient Privilege....................................... 3-57
   [C] Diversity and Supplemental Jurisdiction ................... 3-58
      [C][1] Diversity Jurisdiction ......................................... 3-58
      [C][2] Supplemental Jurisdiction ................................ 3-58

§ 3:8 Employers and Medical Privacy...................................... 3-59

§ 3:8.1 Americans with Disabilities Act.................................. 3-59

§ 3:8.2 HIPAA and Employer-Sponsored Health Plans........... 3-61
   [A] Overview of HIPAA Privacy Rules and Aplicability to Health Plans........................................... 3-62
   [B] Sharing Information with Plan Sponsors Under HIPAA ............................................................. 3-63
Chapter 4  Federal Trade Commission Enforcement of Privacy

Marcia Hofmann

§ 4:1  FTC Privacy Enforcement Authority Under the Federal Trade Commission Act and Other Laws .......... 4-3

§ 4:1.1  Introduction and Overview ............................................... 4-3

§ 4:1.2  Primary Enforcement Authority: The Federal Trade Commission Act ........................................... 4-4

[A]  Unfairness ........................................................................ 4-4

[A][1]  Injury to Consumers......................................................... 4-4

[A][2]  Violation of Established Public Policy ....................... 4-5

[A][3]  Unethical or Unscrupulous Conduct ............................. 4-6

[B]  Deception ...................................................................... 4-6

[B][1]  Representation, Omission, or Practice Likely to Mislead ................................................................. 4-6

[B][2]  Perspective of a Reasonable Consumer in the Circumstances ......................................................... 4-7

[B][3]  Materiality of Representation, Omission, or Practice ........................................................................ 4-7

§ 4:1.3  Other Privacy Enforcement Authorities ................. 4-8

[A]  Children’s Online Privacy Protection Act .................. 4-8

[B]  Gramm-Leach-Bliley Act ................................................. 4-9

[B][1]  Pretexting .................................................................... 4-10

[B][2]  Financial Privacy Rule ................................................... 4-10

[B][3]  Safeguards Rule .............................................................. 4-11

[C]  Telemarketing and Consumer Fraud Abuse and Prevention Act ................................................................. 4-12

[D]  Fair Credit Reporting Act ..................................................... 4-12

§ 4:2  FTC Enforcement Practice .............................................. 4-13

§ 4:2.1  Overview ..................................................................... 4-13

§ 4:2.2  Investigation ................................................................ 4-14

§ 4:2.3  Initiation of Enforcement Action ............................ 4-14

[A]  Administrative Enforcement ........................................... 4-14

[B]  Judicial Enforcement .......................................................... 4-15

§ 4:3  FTC Enforcement of Privacy and Security Promises ..... 4-15

§ 4:3.1  Overview ..................................................................... 4-15

§ 4:3.2  Commission Authority to Investigate and Enforce ........................................................................ 4-16

§ 4:3.3  Security and Privacy Enforcement Actions .......... 4-16

[A]  Enforcing General Privacy Policies and Promises ... 4-16

[B]  Enforcing Affirmative Data Security Promises ......... 4-25

[C]  Enforcing Data Security Absent an Affirmative Promise ....................................................................... 4-38

[D]  Material Change to Privacy Policy .................................... 4-51

[F] Spyware ................................................................. 4-58
[F][1] Tracking, Monitoring, Locating Rent-to-Own Computers .... 4-60
[F][2] Online Behavioral Advertising ............................... 4-62
§ 4:4 FTC Enforcement of Children's Privacy ................. 4-68
§ 4:4.1 Overview .......................................................... 4-68
§ 4:4.2 Commission Authority to Investigate and Enforce...... 4-68
§ 4:4.3 Children's Privacy Enforcement Actions ............ 4-69
[A] Pre-COPPA Enforcement Actions ......................... 4-70
[B] COPPA Enforcement Actions .................................. 4-72
[C] COPPA Enforcement Actions Involving Mobile Applications .................................................. 4-85
[D] Children's Privacy Offline ...................................... 4-89
§ 4:5 FTC Enforcement of Financial Privacy ............. 4-90
§ 4:5.1 Overview .......................................................... 4-90
§ 4:5.2 Commission Authority to Investigate and Enforce... 4-90
§ 4:5.3 Financial Privacy Enforcement Actions ............ 4-90
[A] Pretexting ............................................................ 4-90
[B] Telemarketing ......................................................... 4-94
[C] Unsolicited Commercial Email ............................. 4-96
[D] Phishing ............................................................... 4-98
[E] Data Security .......................................................... 4-100
§ 4:6 FTC Enforcement of Credit Information Privacy ...... 4-106
§ 4:6.1 Overview .......................................................... 4-106
§ 4:6.2 Commission Authority to Investigate and Enforce...... 4-106
§ 4:6.3 Credit Information Privacy Enforcement Actions .................. 4-106
[A] Consumer Reporting Agencies .......................... 4-106
[B] Use of Credit Reports ........................................... 4-114
[C] Data Security .......................................................... 4-118

Chapter 5 State Privacy Laws

Scott P. Cooper & Kristen J. Mathews

§ 5:1 Introduction ......................................................... 5-3
§ 5:1.1 Overview: Role of State Governments ............... 5-3
§ 5:1.2 Origins of State Privacy Laws ......................... 5-5
[B] Constitutional ....................................................... 5-6
[C] Statutory .............................................................. 5-7
[C][1] The California Invasion of Privacy Standard ....... 5-9
§ 5:2 Online Privacy ..................................................... 5-11
§ 5:2.1 State Online Privacy Protection Statutes .......... 5-11
[B][9] Penalties for Violation......................................... 5-55
[B][11] State Credit Freeze Laws ..................................... 5-59
§ 5:5.6 Data Security and Destruction Requirements .......... 5-61
§ 5:6 Financial Privacy .................................................. 5-62
§ 5:6.1 California Financial Information Privacy Act........... 5-62
§ 5:6.2 Other States ....................................................... 5-64
§ 5:6.3 Preemption .......................................................... 5-65
§ 5:6.4 Credit Card Transactions ...................................... 5-66
[A] Restrictions on Merchants ....................................... 5-66
[B] Prohibition on Disclosure of Marketing Information .......... 5-69
§ 5:7 Privacy of Insurance-Related Information ................. 5-69
§ 5:7.2 Definitions of “Personal Information” and Similar Terms .......................................................... 5-72
§ 5:7.3 The GLBA Joint Marketing Exception and 2002 Model Act States ................................................... 5-73
§ 5:8 Laws Governing Disclosure and Use of Social Security Numbers .................................................. 5-74
§ 5:8.1 The California Framework ................................... 5-75
[A] Jurisdictional Modification to the California Framework .................................................. 5-76
[A][1] Prohibiting SSNs in Customer Mailings .................. 5-76
[A][2] Expanded Exemptions from the California Framework .................................................. 5-77
§ 5:8.2 Other State Law Regulation of the Use of Social Security Numbers .................................................. 5-78
[A] Requiring a Consumer’s SSN to Complete a Transaction .................................................. 5-78
[B] Privacy Policy for Handling SSNs ................................. 5-79
[C] Employers .............................................................. 5-80
[D] Other Modifications .................................................. 5-80
§ 5:9 Unsolicited Telephone Marketing ................................ 5-81
§ 5:9.1 Telemarketing: State Do-Not-Call Laws .................. 5-81
§ 5:9.2 Laws Restricting Cell Phone Marketing .................. 5-83
§ 5:10 Electronic Eavesdropping .......................................... 5-85
§ 5:10.1 State Statutory Schemes ...................................... 5-85
§ 5:11 Radio Frequency Identification ................................... 5-87
## Table of Contents

### Chapter 6  Privacy of Electronic Communications

*Bruce Boyden*

| § 6:1 | Introduction ...................................................................... | 6-2 |
| § 6:1.1 | Purpose and History of the ECPA .................................. | 6-4 |
| § 6:1.2 | Amendments to the ECPA ........................................... | 6-9 |
| § 6:2 | Title I—The Wiretap Act ............................................. | 6-10 |
| § 6:2.1 | Communications Covered ............................................. | 6-12 |
| [A] | Oral Communications .................................................... | 6-12 |
| [A][1] | Expectation of Privacy .............................................. | 6-12 |
| [A][2] | Silent Video ............................................................. | 6-19 |
| [B] | Wire Communications .................................................. | 6-20 |
| [B][1] | Cordless Phones ......................................................... | 6-21 |
| [B][2] | Voice Mail ................................................................. | 6-23 |
| [C] | Electronic Communications ........................................... | 6-23 |
| § 6:2.2 | Intentional Interception of Communications ............... | 6-25 |
| [A] | “Intercept” ................................................................. | 6-26 |
| [A][1] | Contemporaneous Acquisition Requirement ................ | 6-26 |
| [A][2] | Access to Temporarily Stored Emails ......................... | 6-31 |
| [A][3] | Access to Telephone Numbers or Other Associated Information | 6-41 |
| [A][4] | Keyloggers and Screen Captures .................................. | 6-43 |
| [B] | Intent .......................................................................... | 6-47 |
| § 6:2.3 | Use or Disclosure of an Intercepted Communication .... | 6-49 |
| § 6:2.4 | Exceptions ................................................................. | 6-53 |
| [A] | Communications Service in Normal Course of Business ........ | 6-53 |
| [B] | Consent by a Party to a Communication ........................ | 6-58 |
| [B][1] | Implied Consent ....................................................... | 6-63 |
| [B][2] | Tortious or Criminal Purpose Exception .................... | 6-65 |
| [B][3] | The Case of “Cookies” ............................................... | 6-67 |
| Figure 6-1 | Placing Third-Party Advertisements on a Website .......... | 6-68 |
| [C] | Business Extensions .................................................... | 6-71 |
| [D] | Communications to the Public .................................... | 6-77 |
| [E] | First Amendment ....................................................... | 6-79 |
| § 6:2.5 | Private Cause of Action ............................................. | 6-82 |
| [A] | Litigating Wiretap Act Claims .................................... | 6-85 |
| [B] | Limitations ............................................................... | 6-88 |
| [C] | Damages ................................................................. | 6-89 |
| [D] | Good-Faith Defense ................................................... | 6-92 |
| § 6:2.6 | State Wiretap Acts ..................................................... | 6-94 |
| § 6:3 | Title II—Stored Communications Act .......................... | 6-96 |
| § 6:3.1 | Access to Stored Communications ............................. | 6-97 |
| [B] | “Unauthorized Access” ............................................... | 6-103 |
| [B][1] | Privacy Policies ....................................................... | 6-106 |

(Proskauer, Rel. #1, 5/17)  xxxix
PROSKAUER ON PRIVACY

[B][2] Subpoenas ......................................................... 6-107
[B][3] Exceeding Authorized Access ....................... 6-109
[C] “Electronic Storage”........................................... 6-110
[C][1] Cookies and Other Data Stored on Computers ........................................ 6-112
[D] Exceptions ............................................................. 6-114
[D][1] Access Authorized by a Service Provider ........ 6-114
[D][2] Access Authorized by a Party ........................... 6-115

§ 6:3.2 Disclosures by Communications Services ............ 6-117
[A] Disclosures Prohibited Under Section 2702........... 6-117
[A][1] Contents of Communications........................... 6-121
[A][1][a] Exceptions .................................................. 6-122
[A][2] Customer Records ......................................... 6-128
[A][2][a] Exceptions .................................................. 6-130
[A][3] Anti-Pretexting Laws ....................................... 6-131
[B] Disclosures to the Government Required Under Section 2703........................................ 6-133

§ 6:3.3 Private Cause of Action .................................... 6-135
[A] Damages .................................................................. 6-138

§ 6:4 Title III—Pen Registers and Trap-and-Trace Devices ........................................ 6-139

Chapter 7 The Foreign Intelligence Surveillance Act

Mary Edquist & Brian Morrison

§ 7:1 Introduction .............................................................. 7-2
§ 7:1.1 Purpose ................................................................. 7-3
§ 7:1.2 “Special-Needs” Exception to Warrant Requirement ........................................ 7-3
§ 7:1.3 Evolution of FISA .................................................. 7-4
[A] The Church Committee ......................................... 7-5
[B] Amendments to FISA .............................................. 7-6

§ 7:2 The Foreign Intelligence Surveillance Act ............... 7-7
§ 7:2.1 The Scope of FISA ................................................. 7-7
[A] Intelligence-Gathering Activities Targeting Persons Within the United States ............ 7-7
[B] Intelligence-Gathering Activities Targeting Persons Outside the United States ........... 7-10

§ 7:2.2 Required Elements for Authorized Intelligence-Gathering Pursuant to FISA........ 7-11
[A] Probable Cause ..................................................... 7-11
[B] Significant Purpose ............................................... 7-13
[C] Identification and Description of the Targeted Individual, Facility, Place, or Property ....... 7-14
Table of Contents

[D] Target Is a Foreign Power or an Agent of a Foreign Power .......................................................... 7-16
[E] The Method and Time Frame of Intelligence Collection .......................................................... 7-18
[F] Minimization Procedures ........................................ 7-20
[G] Certification Requirements ...................................... 7-21

§ 7:2.3 Exceptions to FISA Authorization or Order Requirement.................................................. 7-23
[A] Surveillance of Certain Foreign Powers ................... 7-23
[B] During Emergencies While FISC Order Is Being Pursued .......................................................... 7-25
[C] Declaration of War................................................... 7-28
[D] Testing of Equipment............................................... 7-28
[E] Discovery of Unauthorized Surveillance Equipment........................................................................ 7-29

§ 7:2.4 Remedies ................................................................. 7-30
[A] Motion to Suppress ................................................. 7-30
[B] Request to Modify or Set Aside Order..................... 7-32
[C] Civil Liability........................................................... 7-33
[D] Criminal Liability...................................................... 7-35

§ 7:3 The Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review ...... 7-35

§ 7:3.1 Membership and Structure...................................... 7-35
§ 7:3.2 Authority, Jurisdiction, and Scope of Review........... 7-36
§ 7:3.3 Secret/Sensitive Nature of FISC and FISCR Matters......................................................... 7-37
[A] Secrecy of Proceedings ............................................. 7-37
[B] Publication of Opinions........................................... 7-38
[C] Disclosure and Reporting Requirements; Measures to Increase Transparency ......................... 7-41

§ 7:3.4 Procedure for Obtaining a FISC Order ................. 7-42

§ 7:4 Controversies and Amendments .................................... 7-46

§ 7:4.1 The Terrorist Surveillance Program and Retroactive Immunity .............................................. 7-46
§ 7:4.2 Targeting U.S. and Non-U.S. Persons Abroad ......... 7-48
[A] Bulk Collection of Telephonic Metadata .................... 7-49
[B] PRISM and the Collection of Internet Communications in Transit .............................................. 7-50
§ 7:4.3 Expansion of the Business Records Provision .... 7-53
§ 7:4.4 Roving Wiretaps ...................................................... 7-54
§ 7:4.5 Lone Wolf Provision ................................................ 7-55

(Proskauer, Rel. #1, 5/17) xli
Chapter 8 Privacy and Homeland Security

Hugo Teufel III

§ 8:1 Background: Intelligence, Surveillance, and Privacy Pre-9/11

§ 8:2 Establishment of Department of Homeland Security

§ 8:2.1 DHS Organization and Functions

§ 8:2.2 Authorities for Privacy Protection at DHS

Figure 8-1 DHS Organizational Chart

§ 8:3 Privacy Protection at Other Agencies

§ 8:3.1 Internal Privacy Protection Requirements for Executive-Branch Agencies

§ 8:3.2 Executive-Branch Privacy/Civil Liberties

[A] Board on Safeguarding Americans’ Civil Liberties

[B] Privacy and Civil Liberties Oversight Board

§ 8:4 DHS Privacy Office Functions

§ 8:4.1 Policy

[A] Fair Information Practice Principles

[B] Use of Social Media

[C] Extending Privacy Act Protections

[D] Other Guidance

§ 8:4.2 Compliance

§ 8:4.3 Oversight

§ 8:4.4 Incidents and Breaches

§ 8:4.5 Education and Training

§ 8:4.6 Outreach

§ 8:5 High-Profile Privacy Issues in Homeland Security

§ 8:5.1 Information-Sharing

[A] Breaking Down the Wall of Separation

[B] Information Sharing Environment (ISE)

§ 8:5.2 Fusion Centers

[A] Organization and Mission

[B] Civil Liberties Concerns

§ 8:5.3 Watchlists

[A] Watchlists, Pre-9/11

[B] Integration and Use of Screening Information

[C] Redress and Oversight

§ 8:5.4 Data Mining

[A] Privacy Concerns Versus Combating Terrorism

[B] Establishing a Uniform Definition of “Data Mining”

[C] High-Profile Data Mining

[C][1] Program “Able Danger”

[C][2] JetBlue Data Transfer

[C][3] Total Information Awareness/Terrorism Information Awareness (TIA)
Chapter 9  Workplace Privacy Law

Kathleen M. McKenna & Anthony J. Oncidi

§ 9:1  Selection of Employees .......................................................... 9-4
  § 9:1.1  Pre-Employment Inquiries ................................................. 9-4
    [A]  Inquiries Regarding Race, Sex, Religion, and
    Other Protected Characteristics .................................. 9-4
    [B]  Disability-Related Inquiries ....................................... 9-6
    [C]  Psychological Testing and Examinations ................... 9-7
    [D]  Union Status .......................................................... 9-8
    [E]  Litigation History .................................................. 9-8
    [F]  Social Media ........................................................ 9-9
  § 9:1.2  References .................................................................. 9-9
  § 9:1.3  Blacklisting .............................................................. 9-11

§ 9:2  Collection of Personal Information ................................... 9-12
  § 9:2.1  Medical Information .................................................... 9-14
    [A]  Health Insurance Portability and Accountability
    Act of 1996 ............................................................... 9-14
    [B]  HIV/AIDS ............................................................ 9-17
    [C]  Confidentiality of Patient Medical Records ............. 9-19
    [C][1]  Federal Law ....................................................... 9-19
    [C][2]  State Law ......................................................... 9-20
    [D]  Employee Wellness Programs ................................ 9-25
  § 9:2.2  Past Criminal and Arrest Records ............................... 9-26
    [A]  Federal Law .......................................................... 9-26
    [A][1]  Title VII .......................................................... 9-26
    [A][2]  Intelligence Reform and Terrorism
    Prevention Act ......................................................... 9-30
    [B]  State and Local Law ................................................ 9-30
    [B][1]  Generally ......................................................... 9-30
    [B][2]  “Ban-the-Box” Laws .......................................... 9-32
  § 9:2.3  Fingerprints and Photographs ...................................... 9-34
  § 9:2.4  Financial Data .......................................................... 9-36
    [A][2]  Fair and Accurate Credit Transactions Act ......... 9-38
§ 9:2.5 Educational Records ................................................ 9-40


[B] State Law................................................................... 9-40

§ 9:2.6 Personal Identification Information ........................ 9-41

[A] Information Stored on Computers .......................... 9-41

[B] Social Security Numbers.......................................... 9-42

[C] Motor Vehicle Information...................................... 9-44

[D] Verification of Employment Eligibility: E-Verify ..... 9-45

§ 9:2.7 Access to Personnel Records .............................. 9-47

§ 9:2.8 Genetic Information ............................................. 9-49

§ 9:3 Policies Regulating Employee Conduct............................. 9-51

§ 9:3.1 Sexual Conduct, Intimate Relationships, Fraternization, Procreation, Marriage..................... 9-51

[A] Common-Law Claims—Private Employees .............. 9-51

[A][1] Invasion of Privacy.............................................. 9-51

[A][1][a] Public Disclosure of Private Facts..................... 9-51

[A][1][b] Intrusion upon Seclusion ................................. 9-53

[A][2] Wrongful Termination in Violation of Public Policy.......................................................... 9-54

[B] Statutory Claims ..................................................... 9-55

[C] Constitutional Privacy Right ................................... 9-56

§ 9:3.2 Grooming and Dress Codes .................................... 9-58


[B] Hair Length and Style.............................................. 9-59

[B][1] Federal Law......................................................... 9-59

[B][2] State Law............................................................. 9-62

[C] Beards and Moustaches ........................................... 9-63

[C][1] Federal Law......................................................... 9-63

[C][2] State Law............................................................. 9-65

[D] Dress Codes............................................................. 9-65

[D][1] Federal Law......................................................... 9-65

[D][2] State Law............................................................. 9-67

[E] Gender Identity/Expression Issues........................... 9-68

[E][1] Federal Law......................................................... 9-68

[E][2] State Law............................................................. 9-69

§ 9:3.3 Polygraphs and Lie Detector Tests ......................... 9-71

§ 9:3.4 Genetic Testing.................................................... 9-72

§ 9:3.5 Drug and Alcohol Use ............................................ 9-73

[A] Federal Law.............................................................. 9-74

[A][1] Constitution........................................................ 9-74

[A][2] Americans with Disabilities Act (ADA).............. 9-75

[A][3] Other Federal Statutes and Regulations.............. 9-77

[B] State Laws.............................................................. 9-78

[B][1] Constitutions ...................................................... 9-78

[B][2] Statutes .............................................................. 9-79
Table of Contents

[C] Medical Marijuana in the Workplace ...................... 9-80
[D] Contractual and Common Law Theories of
   Liability ................................................................ 9-82
§ 9:3.6 Smoking ...................................................... 9-83
 [A] Restrictions on Smoking in the Workplace .......... 9-83
 [B] Off-Duty Smoking ........................................... 9-85
§ 9:3.7 Disclosure of Wages ..................................... 9-85
 [B] State Law ........................................................ 9-87
§ 9:3.8 Blogging and Cybersmearing ......................... 9-87
 [A] Validity of Employee Confidentiality Policies ....... 9-88
 [B] Potential Causes of Action ............................... 9-90
   [B][1] Private Blogs and the Stored
   Communication Act ........................................... 9-90
   [B][2] Trespass to Chattels ................................... 9-92
   [B][3] Defamation ................................................. 9-93
§ 9:4 Surveillance of Employees ................................. 9-95
§ 9:4.1 Employer Investigations Generally ................. 9-95
§ 9:4.2 Physical Searches ....................................... 9-95
   [A] Introduction .................................................. 9-95
   [B] Public Employer Searches ............................. 9-96
   [C] Private Employer Searches ............................ 9-99
      [C][1] Third-Party Consent ............................... 9-101
      [C][2] Fifth Amendment Considerations .......... 9-101
   [D] NLRA ........................................................... 9-102
§ 9:4.3 Email and Internet Use Searches ..................... 9-102
   [A] Notice ........................................................ 9-102
      [B][1] Federal Law ......................................... 9-106
      [B][1][a] The Electronic Communications Privacy Act ..9-106
      [B][1][a][i] Exceptions ................................... 9-110
      [B][1][b] The Federal Computer Fraud and Abuse Act ..9-112
      [B][1][c] NLRA .............................................. 9-115
   [C] State Law ................................................... 9-116
§ 9:4.4 Instant Electronic Communications ................. 9-117
   [A] Instant Messaging ....................................... 9-117
   [B] Text Messaging .......................................... 9-118
   [C] Social Media ............................................. 9-119
§ 9:4.5 Eavesdropping, Recording Telephone
   Conversations, and Video Monitoring .................... 9-121
§ 9:4.6 Human Tracking Devices ............................. 9-124
   [B] Radio Frequency Identification (RFID) ............. 9-127
   [C] Biometrics ................................................. 9-128
§ 9:4.7 USA PATRIOT Act ....................................... 9-129

(Proskauer, Rel. #1, 5/17)
| § 10:1 | Overview .................................................................................................................. 10-3 |
| § 10:1.1 | Connection to Privacy Principles and Laws ................................................. 10-3 |
| § 10:1.2 | General Considerations ...................................................................................... 10-4 |
| § 10:2 | Email Communications .......................................................................................... 10-4 |
| § 10:2.1 | Source and Scope of Rules ............................................................................... 10-4 |
| § 10:2.2 | What Is a “Commercial Electronic Mail Message”? ...................................... 10-6 |
| § 10:2.3 | Who Is the “Sender”? ......................................................................................... 10-9 |
| § 10:2.4 | Consent Requirements ......................................................................................... 10-11 |
| § 10:2.5 | Information to Be Included in Each Message .............................................. 10-12 |
| § 10:2.6 | Forward-to-a-Friend Features .......................................................................... 10-13 |
| § 10:2.7 | Specific Rules for Messages Sent to Wireless Domains ................................ 10-15 |
| § 10:2.8 | Prohibitions on Fraudulent, Deceptive, and Abusive Practices ...................... 10-17 |
| § 10:2.9 | Additional Rules Regarding Sexually Oriented Material .................................. 10-18 |
| § 10:3 | Telephone Communications .................................................................................. 10-20 |
| § 10:3.1 | Source and Scope of Rules ............................................................................... 10-20 |
| § 10:3.2 | Consent Requirements ......................................................................................... 10-21 |
| [A] | Company-Specific Consent Requirements ...................................................... 10-22 |
| [B] | National Do Not Call Registry ........................................................................ 10-23 |
| [C] | State Do-Not-Call Lists ..................................................................................... 10-24 |
| § 10:3.3 | Required Call Content ....................................................................................... 10-25 |
| § 10:3.4 | Time and Frequency Restrictions ..................................................................... 10-27 |
| § 10:3.5 | Use of Autodialers, Prerecorded Messages, and Other Technologies .............. 10-27 |
| § 10:3.6 | Prohibitions on Deceptive or Abusive Telemarketing Practices ...................... 10-31 |
| § 10:3.7 | Record-Keeping and Compliance Requirements ............................................ 10-32 |
| § 10:4 | Fax Communication ............................................................................................. 10-33 |
| § 10:4.1 | Source and Scope of Rules ............................................................................... 10-33 |
| § 10:4.2 | Consent Requirements ......................................................................................... 10-34 |
| § 10:4.3 | Information to Be Included in Each Message .............................................. 10-35 |
| § 10:5 | Direct Mail Communications ............................................................................... 10-36 |
| § 10:5.1 | Source and Scope of Rules ............................................................................... 10-36 |
| § 10:5.2 | Restrictions and Prohibitions on Mailing Certain Content ................................ 10-36 |
| [A] | Fraudulent or Deceptive Content .................................................................... 10-37 |
| [B] | Prohibited or Restricted Advertising Content ............................................. 10-37 |
| [C] | Mailings Containing Certain Goods, Samples, Etc. ........................................ 10-38 |
| § 10:5.3 | Consent Requirements ......................................................................................... 10-38 |
Chapter 11 The Children’s Online Privacy Protection Act (COPPA)

Nancy L. Savitt

§ 11:1 Introduction/Overview.................................................... 11-3
§ 11:1.1 Enactment ..................................................................... 11-3
§ 11:1.2 Statutory Overview.................................................... 11-4
§ 11:1.3 Who Enforces the Statute......................................... 11-5
§ 11:2 Who Is Subject to the Statute ....................................... 11-6
§ 11:2.1 “Operator” ............................................................... 11-6
[A] Factors Determining Operator Status......................... 11-9
[B] Special Cases ........................................................... 11-10
[B][1] Internet Service Providers and Other “Mere
Conduits”........................................................................... 11-10
[B][2] Advertisers, Plug-Ins, and Related Services .... 11-11
[B][3] Non-U.S. Operators ........................................... 11-12
[B][4] Nonprofits ............................................................. 11-12
§ 11:2.2 “Website or Online Service Directed to
Children”........................................................................... 11-13
[A] Primary Content Provider Versus
Advertisers and Plug-Ins.................................................. 11-14
[B] Age-Screening Where Children Are Not
“Primary Audience” ...................................................... 11-16
§ 11:2.3 General Audience Website .................................. 11-17
[A] “Actual Knowledge” .................................................... 11-18
§ 11:3 What Activities Does COPPA Cover?..................... 11-19
§ 11:3.1 “Personal Information” ............................................. 11-19
§ 11:3.2 “Collection” ............................................................ 11-21
[A] Requesting a Child to Submit Personal
Information Online ........................................................... 11-21
[B] Enabling a Child to Publicly Disclose Personal
Information ......................................................................... 11-22
[B][1] To Monitor or Not to Monitor .................................... 11-23
[C] Passive Tracking .......................................................... 11-23
§ 11:3.3 “Disclosure” .............................................................. 11-24
[A] Release of Personal Information ............................... 11-24
[A][1] Third Party Versus Provider of “Support
for the Internal Operations of the Website” .......... 11-25
[B] Making Personal Information Publicly
Available ........................................................................ 11-26
§ 11:4 How to Comply with COPPA .............................. 11-27
§ 11:4.1 Need Prior Parental Consent Unless Fall
Within Exception .............................................................. 11-28
[A] “Verifiable Parental Consent”
(“Verifiable Consent”) ..................................................... 11-28
[B] “Parent” ......................................................................... 11-29

xlviii
§ 11:4.2 Exceptions to Consent............................................. 11-32
[A] To Obtain Parental Consent ..................................... 11-32
[B] To Respond to a Child’s Specific Request on
a One-Time Basis .................................................... 11-33
[C] To Respond More Than Once to a Child’s
Specific Request ...................................................... 11-35
[D] To Protect the Child’s Safety ................................... 11-36
[E] To Protect the Website ............................................. 11-37
[F] To Notify and Update Parents About
a Website That Does Not Collect
Personal Information............................................... 11-37
[G] To Collect a Persistent Identifier in
Limited Circumstances.......................................... 11-38
§ 11:4.3 How to Get Consent ............................................. 11-38
[A] Notice .................................................................... 11-39
[A][1] Requirements for Notice ................................... 11-39
[A][1][a] “Clear and Understandable”......................... 11-39
[A][1][b] Information Collected and How It Is Used... 11-39
[A][1][c] Disclosures to Third Parties and Others ...... 11-40
[A][1][d] Parental Review Rights ............................... 11-41
[A][1][e] Operators’ Contact Information ............... 11-41
[A][2] Privacy Policy Placement .................................... 11-41
[A][3] Direct Notice to Parents ................................. 11-43
[A][3][a] “Material Change” ........................................ 11-43
[B] Consent .................................................................. 11-44
[B][1] Full Consent...................................................... 11-44
[B][1][a] Print and Send or Scan ................................... 11-44
[B][1][b] Credit Card Transaction ............................... 11-45
[B][1][c] Toll-Free Number or Video Conference ...... 11-45
[B][1][d] Government-Issued Identification ............ 11-45
[B][1][e] Other Methods ............................................. 11-46
[B][2] Email Plus Consent .......................................... 11-47
[B][3] Online Consent Form Insufficient .................... 11-49
§ 11:4.4 What Happens If the Operator Does Not
Get Parental Consent .............................................. 11-49
[A] Delete Information ................................................. 11-49
[B] Limited Permission to Terminate Service .......... 11-50
[B][1] Cannot Terminate for Non-Consent to
Third-Party Disclosure ........................................... 11-50
§ 11:4.5 Security and Data Retention/Deletion .......... 11-51
§ 11:4.6 Safe Harbors ...................................................... 11-54
Chapter 12 The Privacy Act of 1974 and Its Progeny

Kenneth P. Mortensen & Nuala O’Connor Kelly

§ 12:1 Introduction ................................................................... 12-3
§ 12:2 Privacy Act Statutory Provisions ........................................ 12-4
 § 12:2.1 5 U.S.C. § 552a(a): Definitions .................................... 12-4
[A] “Agency” ............................................................................ 12-4
[A][1] Privacy Act Applies Only to Federal Agencies .................. 12-4
[A][2] Executive Office of the President ............................... 12-5
[A][3] State and Local Government Agencies .................... 12-7
[A][4] Other Entities ...................................................... 12-7
[B] “Individual” ............................................................. 12-8
[C] “Maintain” .......................................................... 12-10
[D] “Record” ................................................................. 12-10
[E] “System of Records” .................................................. 12-13
[F] “Statistical Record” .................................................... 12-16
[G] “Routine Use” ......................................................... 12-17
 § 12:2.2 5 U.S.C. § 552a(b): Conditions of Disclosure ...... 12-18
[A] Disclosure Within Agencies ................................... 12-19
[B] Disclosure to the Public ........................................ 12-19
[C] Disclosure for a “Routine Use” .................................... 12-20
[D] Disclosure to the Bureau of the Census ................ 12-22
[E] Disclosure for Statistical Research and Reporting .... 12-23
[F] Disclosure to National Archives ............................ 12-24
[H] Disclosure Under Emergency Circumstances ...... 12-25
[I] Disclosure to Congress .......................................... 12-26
[J] Disclosure to the General Accountability Office ................. 12-26
[K] Disclosure Pursuant to Court Order .................... 12-26
[L] Disclosure to a Consumer Reporting Agency .... 12-27
[A] Individual Access .................................................. 12-28
[B] Amending Records .................................................... 12-30
 § 12:2.4 5 U.S.C. § 552a(g)(4): Remedies ... 12-32
 § 12:3 Systems of Records Notice Guidance ........................... 12-32
 § 12:3.1 Definitions ............................................................. 12-32
 § 12:3.2 Contents .............................................................. 12-32
 § 12:3.3 How to Prepare a System of Records Notice ...... 12-33
Chapter 13  Canadian Privacy Law

John Beardwood, Gabriel M.A. Stern & Daniel Fabiano

§ 13:1  Nature of the Canadian Privacy Framework .......... 13-3
  § 13:1.1  Intersecting Federal and Provincial
            Privacy Regimes ........................................... 13-3
  [A]  Public Sector .............................................. 13-3
  [B]  Private Sector ............................................ 13-4
  [B][1]  Québec .................................................... 13-4
  [B][3]  Provincial [Other Than Québec] ...................... 13-6
  [C]  Personal Health Information ................................ 13-7
  [D]  Statutory Tort of Invasion of Privacy ..................... 13-8

§ 13:1.2  Privacy Principles from Common Law ................. 13-9
  [B]  Work Product .............................................. 13-12
  [C]  Surveillance ............................................... 13-12
      [C][1]  Reasonableness of Surveillance in the Workplace 13-12
      [C][2]  Surveillance Evidence in Litigation ................ 13-14

§ 13:1.3  Relationship Between the Canadian and
          European Privacy Regimes ................................ 13-14

§ 13:2  Personal Information ........................................ 13-16
  § 13:2.1  Scope of Definition of “Personal Information” ...... 13-16
  § 13:2.2  Employee Information ................................ 13-17
  § 13:2.3  Carve-Outs from the Obligations Applying to
            Personal Information ..................................... 13-17
  § 13:2.4  Sensitivity of Personal Information ................ 13-18
  § 13:2.5  Grandfathering Provisions ............................ 13-18

§ 13:3  Nature of Privacy Obligations ............................. 13-19
  § 13:3.1  Consent/Notice Obligations .......................... 13-19

lvi
| A | Generally ............................................................... 13-19 |
| B | Content of the Notice ........................................... 13-20 |
| C | Withdrawing Consent............................................ 13-20 |
| D | Extra-Jurisdictional Transfers of Personal Information ........................................ 13-21 |

§ 13:3.2 Administrative Obligations ........................................ 13-23

§ 13:3.3 Access Obligations ................................................ 13-24

§ 13:3.4 Breach Notification ................................................ 13-25

[A] Comparison of the Federal and Alberta Models ........ 13-25

[A][1] Critique of the Single-Threshold Test .................... 13-26

[A][2] Components of the Threshold Test Under PIPEDA ........................................ 13-28

[A][3] Components of Threshold Test Under Alberta PIPA ........................................ 13-28


[A][5] Third-Party Notifications .................................. 13-29

[A][6] Recording Obligation ........................................ 13-29

[A][7] Offenses ............................................................. 13-30

§ 13:3.5 Enforcement .......................................................... 13-30

[A] Generally ............................................................... 13-30

[B] Powers ................................................................... 13-30

[C] Offenses .................................................................. 13-31

[D] “Naming and Shaming” ........................................ 13-31

[E] Review of Findings/Appeals ................................... 13-31

[F] Remedies ............................................................... 13-32

§ 13:4 Canadian Privacy Law in Transition ..................... 13-32

§ 13:4.1 Overview of 2015 Additional Key Amendments to PIPEDA ........................................ 13-32

[A] Valid Consent ............................................................ 13-32

[B] New Disclosure Consent Exemptions ....................... 13-32

[C] New Collection, Use and Disclosure Exemptions .... 13-33


[E] New Consent Exemption for Employee Information ........................................ 13-33

[F] Extension of Complaint Time Period ...................... 13-34

[G] New Compliance Agreement ................................... 13-34

[H] Expansion of Privacy Commissioner Right to Publicize ........................................ 13-34

§ 13:4.2 Canada’s Anti-Spam Legislation (CASL) ............. 13-35


[B] Definition of “Commercial” Messages/ Communications ........................................ 13-37

[C] Consent ................................................................. 13-40


[C][2] “Natural Persons” Versus “Legal Persons” ............ 13-42
Chapter 14  International Privacy Law

Peta-Anne Barrow, Erika C. Collins, Cécile Martin, Jeremy M. Mittman & Courtney M. Bowman*

§ 14:1 Introduction ................................................................. 14-11
§ 14:2 EU Data Protection Directive........................................ 14-11
  § 14:2.1 Key Components of the EU Data Protection Directive .......... 14-12
  § 14:2.2 Terminology ............................................................. 14-13
  § 14:2.3 Compliance with the EU Data Protection Directive .............. 14-14
  § 14:2.4 Disclosure Requirements to Data Subjects ..................... 14-16
  § 14:2.5 Reporting to Supervisory Authorities .......................... 14-16
  § 14:2.6 Controllers and Processors ..................................... 14-17
    [A] Controllers .................................................................. 14-18
    [B] Processors .................................................................. 14-19
    [C] Determining Whether an Entity Is a Controller or Processor .... 14-20
  § 14:2.7 Anonymity of Data Subjects ..................................... 14-20
    [A] Anonymization of Data .................................................. 14-21
    [B] Pseudonymization of Data ............................................. 14-22
  § 14:2.8 Specific Issues Concerning Consent ............................ 14-23
    [A] When Consent Is Necessary ......................................... 14-23
    [B] Definition of Consent ................................................... 14-24
      [B][1] “Freely Given” ...................................................... 14-26
      [B][2] Specific and Informed Indication .............................. 14-27
      [B][3] Unambiguous Consent .......................................... 14-28
    [C] Withdrawal of Consent ............................................... 14-29
  § 14:2.9 Territorial Scope ...................................................... 14-29
    [A] Location of the Data Controller .................................... 14-31
    [A][1] Identifying the Data Controller ................................ 14-31

liv
## Table of Contents

[A][2] Determining the Existence of an “Establishment” ................................................ 14-32
[A][3] The Location of the Establishment .................................................... 14-33
[A][4] Involvement of Establishment in Activities Relating to Data Processing .......... 14-33
[B] International Law .................................................................................. 14-34
[C] Place of Processing ........................................................................... 14-35
[C][1] Difference Between Article 4(1)(a) and Article 4(1)(c) ...................................... 14-35
[C][4] When Equipment Is Used Only for Purposes of Transit Through the EU .......... 14-38

§ 14:2.10 General Data Protection Regulation (GDPR) .............................................. 14-38
[A] Differences Between the Directive and GDPR ............................................. 14-39
[B] Similarities Between the Directive and GDPR ............................................. 14-41
[C] Permitted Carve-Outs........................................................................... 14-42

§ 14:2.11 Safe Harbor and Privacy Shield ................................................................ 14-42

§ 14:2.12 Other Transfer Mechanisms .................................................................. 14-46
[A] Model Contractual Clauses ...................................................................... 14-46
[A][1] Overview ............................................................................................ 14-46
[A][2] Model Contracts Governing Controller-Controller Relationships ................ 14-47
[A][3] Model Contracts Governing Controller-Processor Relationships ................. 14-51
[B] Binding Corporate Rules .......................................................................... 14-55
[B][1] Overview ............................................................................................ 14-55
[B][2] Requirements ....................................................................................... 14-55
[B][4] BCRs for Data Processors ..................................................................... 14-59
[C] The Role of Model Contracts and BCRs in Cloud Computing ......................... 14-60

§ 14:2.13 Alternative Approach to Regulating Data Privacy—APEC Privacy Framework .......................................................... 14-61
[A] APEC Cross-Border Privacy Rules ............................................................... 14-61
[B] Comparison with the EU Data Privacy Model ............................................ 14-63

§ 14:3 Consumer Privacy ..................................................................................... 14-64
§ 14:3.1 Cookies .............................................................................................. 14-64
§ 14:3.2 Privacy Policies.................................................................................... 14-68
[A] Purpose of Privacy Policies ....................................................................... 14-68
[A][1] Obtaining Consent ................................................................................ 14-68
[A][2] Complying with the Directive’s “Purpose Limitation” Requirement ............... 14-69

(Proskauer, Rel. #1, 5/17)
§ 14:3.3 Data Breach Requirements and Best Practices ...... 14-73

§ 14:3.4 Direct Marketing ...................................................................... 14-74

[A] Direct Marketing by Email, SMS, MMS, Fax, and Automated Calling

[A][1] Notification of Purpose ........................................................................ 14-75

[A][2] Prior “Opt-in” Consent ......................................................................... 14-76

[A][3] Right to Opt Out ................................................................................ 14-78

[B] Non-Automated (“Person to Person”) Telephone Marketing ........................................ 14-78

[C] Postal Direct Marketing ........................................................................ 14-78

§ 14:4 Employee Privacy .............................................................................. 14-79

§ 14:4.1 Employee Notice Requirements .................................................. 14-79

§ 14:4.2 Monitoring of Employees ............................................................ 14-80

§ 14:4.3 Social Media Policies and Blogging ............................................. 14-82

[A] Limitations on Employer Monitoring of Social Media ............................ 14-82

[B] Global Laws Affecting Social Media ................................................... 14-83

[B][1] Argentina ........................................................................................ 14-83

[B][2] Brazil .............................................................................................. 14-84

[B][3] Canada ............................................................................................. 14-84

[B][4] China ................................................................................................ 14-85

[B][5] France .............................................................................................. 14-85

[B][6] Germany .......................................................................................... 14-85

[B][7] Hong Kong ....................................................................................... 14-86

[B][8] India ................................................................................................... 14-86

[B][9] Ireland ................................................................................................ 14-86

[B][10] Italy ................................................................................................... 14-87

[B][11] Japan ................................................................................................ 14-87

[B][12] The Netherlands ............................................................................... 14-88

[B][13] Spain ................................................................................................ 14-88

[B][14] United Kingdom ............................................................................. 14-89

§ 14:4.4 “Bring-Your-Own-Device” Policies .............................................. 14-89

§ 14:4.5 Diversity Initiatives ........................................................................ 14-91

§ 14:4.6 Investigations and Discovery ....................................................... 14-92

§ 14:4.7 Background Screening ................................................................... 14-93

§ 14:4.8 Company Intranet .......................................................................... 14-95

§ 14:4.9 Human Resource Information Systems ....................................... 14-96

§ 14:5 Country Summaries .......................................................................... 14-97

§ 14:5.1 Europe (European Union) ............................................................... 14-97

[A] Belgium ................................................................................................ 14-97

[A][1] Overview ......................................................................................... 14-97

[A][2] Personal Information ....................................................................... 14-97

[A][3] Restrictions on Processing and Use ................................................. 14-98
Table of Contents

[A] Transfer and Disclosure ............................................. 14-99
[A] Sensitive Data .......................................................... 14-99
[A] Enforcement ............................................................ 14-99
[A] Data Breach Notification ........................................... 14-100
[B] France ................................................................. 14-101
[B] Overview .............................................................. 14-101
[B] Personal Data .......................................................... 14-101
[B] Restrictions on Processing and Use .............................. 14-102
[B] Sensitive Data .......................................................... 14-103
[B] Enforcement ............................................................ 14-104
[B] Data Breach Notification ........................................... 14-104
[B] Recent Developments ................................................ 14-105
[C] Germany ............................................................... 14-106
[C] Overview .............................................................. 14-106
[C] Personal Data .......................................................... 14-106
[C] Restrictions on Processing and Use .............................. 14-106
[C] Transfer and Disclosure ............................................. 14-107
[C] Sensitive Data .......................................................... 14-107
[C] Enforcement ............................................................ 14-108
[C] Data Breach Notification ........................................... 14-108
[C] Recent Developments ................................................ 14-108
[D] Italy ................................................................. 14-109
[D] Overview .............................................................. 14-109
[D] Personal Data .......................................................... 14-109
[D] Restrictions on Processing and Use .............................. 14-110
[D] Transfer and Disclosure ............................................. 14-110
[D] Sensitive Data .......................................................... 14-111
[D] Enforcement ............................................................ 14-112
[D] Data Breach Notification ........................................... 14-112
[D] Recent Developments ................................................ 14-114
[D] GDPR Implementation .............................................. 14-114
[E] The Netherlands ...................................................... 14-115
[E] Overview .............................................................. 14-115
[E] Personal Data .......................................................... 14-115
[E] Restrictions on Processing and Use .............................. 14-116
[E] Transfer and Disclosure ............................................. 14-117
[E] Sensitive Data .......................................................... 14-118
[E] Enforcement ............................................................ 14-118
[E] Data Breach Notification ........................................... 14-120
[F] Poland ................................................................. 14-120
[F] Overview .............................................................. 14-120
[F] Personal Data .......................................................... 14-121
[F] Restrictions on Processing and Use .............................. 14-121
[F] Transfer and Disclosure ............................................. 14-122
[F] Enforcement ............................................................ 14-122
## G Spain

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>[G][1]</td>
<td>Overview</td>
<td>14-123</td>
</tr>
<tr>
<td>[G][2]</td>
<td>Personal Data</td>
<td>14-124</td>
</tr>
<tr>
<td>[G][3]</td>
<td>Restrictions on Processing and Use</td>
<td>14-124</td>
</tr>
<tr>
<td>[G][5]</td>
<td>Sensitive Data</td>
<td>14-125</td>
</tr>
<tr>
<td>[G][6]</td>
<td>Enforcement</td>
<td>14-125</td>
</tr>
<tr>
<td>[G][7]</td>
<td>Data Breach Notification</td>
<td>14-126</td>
</tr>
</tbody>
</table>

## H United Kingdom

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>[H][1]</td>
<td>Overview</td>
<td>14-126</td>
</tr>
<tr>
<td>[H][2]</td>
<td>Personal Data</td>
<td>14-127</td>
</tr>
<tr>
<td>[H][3]</td>
<td>Restrictions on Processing and Use</td>
<td>14-127</td>
</tr>
<tr>
<td>[H][4]</td>
<td>Transfer and Disclosure</td>
<td>14-129</td>
</tr>
<tr>
<td>[H][5]</td>
<td>Sensitive Data</td>
<td>14-129</td>
</tr>
<tr>
<td>[H][6]</td>
<td>Enforcement</td>
<td>14-130</td>
</tr>
<tr>
<td>[H][7]</td>
<td>Data Breach Notification</td>
<td>14-132</td>
</tr>
</tbody>
</table>

### § 14:5.2 Europe (Non–European Union)

#### A Russian Federation

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>[A][1]</td>
<td>Overview</td>
<td>14-133</td>
</tr>
<tr>
<td>[A][2]</td>
<td>Personal Information</td>
<td>14-134</td>
</tr>
<tr>
<td>[A][3]</td>
<td>Restrictions on Processing and Use</td>
<td>14-134</td>
</tr>
<tr>
<td>[A][4]</td>
<td>Transfer and Disclosure</td>
<td>14-135</td>
</tr>
<tr>
<td>[A][5]</td>
<td>Sensitive Data</td>
<td>14-135</td>
</tr>
<tr>
<td>[A][6]</td>
<td>Enforcement</td>
<td>14-136</td>
</tr>
<tr>
<td>[A][7]</td>
<td>Recent Developments</td>
<td>14-137</td>
</tr>
</tbody>
</table>

#### B Switzerland

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>[B][1]</td>
<td>Overview</td>
<td>14-138</td>
</tr>
<tr>
<td>[B][2]</td>
<td>Personal Information</td>
<td>14-138</td>
</tr>
<tr>
<td>[B][3]</td>
<td>Restrictions on Processing and Use</td>
<td>14-139</td>
</tr>
<tr>
<td>[B][4]</td>
<td>Transfer and Disclosure</td>
<td>14-140</td>
</tr>
<tr>
<td>[B][5]</td>
<td>Sensitive Data</td>
<td>14-142</td>
</tr>
<tr>
<td>[B][6]</td>
<td>Enforcement</td>
<td>14-142</td>
</tr>
</tbody>
</table>

### § 14:5.3 Asia/Pacific

#### A Australia

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>[A][1]</td>
<td>Overview</td>
<td>14-144</td>
</tr>
<tr>
<td>[A][2]</td>
<td>Personal Data</td>
<td>14-145</td>
</tr>
<tr>
<td>[A][3]</td>
<td>Restrictions on Processing and Use</td>
<td>14-145</td>
</tr>
<tr>
<td>[A][4]</td>
<td>Sensitive Data</td>
<td>14-147</td>
</tr>
<tr>
<td>[A][5]</td>
<td>Transfer and Disclosure</td>
<td>14-148</td>
</tr>
<tr>
<td>[A][6]</td>
<td>Enforcement</td>
<td>14-149</td>
</tr>
<tr>
<td>[A][7]</td>
<td>Recent Developments</td>
<td>14-150</td>
</tr>
</tbody>
</table>

#### B China (People’s Republic of China)

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>[B][1]</td>
<td>Overview</td>
<td>14-150</td>
</tr>
<tr>
<td>[B][2]</td>
<td>Personal Information</td>
<td>14-151</td>
</tr>
<tr>
<td>[B][3]</td>
<td>Disclosure and Use</td>
<td>14-151</td>
</tr>
<tr>
<td>[B][4]</td>
<td>Transfer and Disclosure</td>
<td>14-152</td>
</tr>
</tbody>
</table>
Table of Contents

[B][5] Enforcement .................................................... 14-153
[B][6] Recent Developments ........................................ 14-153
[C] Hong Kong ........................................................... 14-154
[C][1] Overview ......................................................... 14-154
[C][2] Personal Data .................................................. 14-155
[C][3] Restrictions on Processing and Use ................ 14-155
[C][4] Transfer and Disclosure ...................................... 14-156
[C][5] Enforcement .................................................... 14-156
[C][6] Data Breach Notification .................................. 14-157
[C][7] Recent Developments ....................................... 14-157
[D] India .................................................................... 14-158
[D][1] Overview ......................................................... 14-158
[D][2] Personal and Sensitive Data............................ 14-160
[D][3] Restrictions on Processing and Use ................ 14-161
[D][4] Transfer and Disclosure ...................................... 14-161
[D][5] Enforcement .................................................... 14-162
[D][6] Data Breach Notification ................................... 14-162
[D][7] Recent Developments ....................................... 14-163
[E] Japan .................................................................... 14-164
[E][1] Overview ......................................................... 14-164
[E][2] Personal Information .......................................... 14-165
[E][3] Restrictions on Processing and Use ................ 14-165
[E][4] Transfer and Disclosure ...................................... 14-165
[E][5] Sensitive Data .................................................. 14-166
[E][6] Enforcement .................................................... 14-166
[F] Malaysia .............................................................. 14-166
[F][1] Overview ......................................................... 14-166
[F][2] Personal Information .......................................... 14-167
[F][3] Restrictions on Processing and Use ................ 14-168
[F][4] Transfer and Disclosure ...................................... 14-174
[F][5] Sensitive Personal Data ....................................... 14-174
[F][6] Enforcement .................................................... 14-176
[G] Philippines ........................................................... 14-177
[G][1] Overview ......................................................... 14-177
[G][2] Personal Information .......................................... 14-178
[G][3] Restrictions on Processing and Use ................ 14-178
[G][4] Transfer and Disclosure ...................................... 14-180
[G][5] Sensitive Data .................................................. 14-180
[G][6] Enforcement .................................................... 14-182
[H] Singapore ............................................................. 14-183
[H][1] Overview ......................................................... 14-183
[H][2] Personal Information .......................................... 14-183
[H][3] Restrictions on Processing and Use ................ 14-183
[H][4] Transfer and Disclosure ...................................... 14-184
[H][5] Sensitive Data .................................................. 14-184
[H][6] Enforcement .................................................... 14-185

(Proskauer, Rel. #1, 5/17) lix
<table>
<thead>
<tr>
<th>§ 14:5.5</th>
<th>Africa and the Middle East</th>
<th>14-213</th>
</tr>
</thead>
<tbody>
<tr>
<td>[A]</td>
<td>Ghana</td>
<td>14-213</td>
</tr>
<tr>
<td>[A][1]</td>
<td>Overview</td>
<td>14-213</td>
</tr>
<tr>
<td>[A][2]</td>
<td>Personal Data</td>
<td>14-214</td>
</tr>
<tr>
<td>[A][3]</td>
<td>Restrictions on Processing and Use</td>
<td>14-214</td>
</tr>
<tr>
<td>[A][5]</td>
<td>Sensitive Data</td>
<td>14-215</td>
</tr>
<tr>
<td>[A][6]</td>
<td>Enforcement</td>
<td>14-217</td>
</tr>
<tr>
<td>[A][7]</td>
<td>Data Breach Notification</td>
<td>14-218</td>
</tr>
<tr>
<td>[B]</td>
<td>Israel</td>
<td>14-219</td>
</tr>
<tr>
<td>[B][1]</td>
<td>Overview</td>
<td>14-219</td>
</tr>
<tr>
<td>[B][2]</td>
<td>Personal and Sensitive Data</td>
<td>14-220</td>
</tr>
<tr>
<td>[B][3]</td>
<td>Restrictions on Processing and Use</td>
<td>14-221</td>
</tr>
<tr>
<td>[B][4]</td>
<td>Transfer and Disclosure</td>
<td>14-221</td>
</tr>
<tr>
<td>[B][5]</td>
<td>Enforcement</td>
<td>14-223</td>
</tr>
<tr>
<td>[B][6]</td>
<td>Recent Developments</td>
<td>14-224</td>
</tr>
<tr>
<td>[C]</td>
<td>Nigeria</td>
<td>14-226</td>
</tr>
<tr>
<td>[C][1]</td>
<td>Overview</td>
<td>14-226</td>
</tr>
<tr>
<td>[C][2]</td>
<td>Personal Information</td>
<td>14-227</td>
</tr>
<tr>
<td>[C][3]</td>
<td>Restrictions on Processing and Use</td>
<td>14-228</td>
</tr>
<tr>
<td>[C][4]</td>
<td>Transfer and Disclosure</td>
<td>14-229</td>
</tr>
<tr>
<td>[C][5]</td>
<td>Sensitive Data</td>
<td>14-229</td>
</tr>
<tr>
<td>[C][6]</td>
<td>Enforcement</td>
<td>14-230</td>
</tr>
<tr>
<td>[D]</td>
<td>Saudi Arabia</td>
<td>14-231</td>
</tr>
<tr>
<td>[D][1]</td>
<td>Overview</td>
<td>14-231</td>
</tr>
<tr>
<td>[D][2]</td>
<td>Personal Information</td>
<td>14-232</td>
</tr>
<tr>
<td>[D][3]</td>
<td>Restrictions on Processing and Use</td>
<td>14-232</td>
</tr>
<tr>
<td>[D][4]</td>
<td>Transfer and Disclosure</td>
<td>14-233</td>
</tr>
<tr>
<td>[D][5]</td>
<td>Sensitive Data</td>
<td>14-233</td>
</tr>
<tr>
<td>[D][6]</td>
<td>Enforcement</td>
<td>14-233</td>
</tr>
<tr>
<td>[D][7]</td>
<td>Recent Developments</td>
<td>14-234</td>
</tr>
<tr>
<td>[E]</td>
<td>South Africa</td>
<td>14-234</td>
</tr>
<tr>
<td>[E][1]</td>
<td>Overview</td>
<td>14-234</td>
</tr>
<tr>
<td>[E][2]</td>
<td>Personal Information</td>
<td>14-235</td>
</tr>
<tr>
<td>[E][3]</td>
<td>Restrictions on Processing and Use</td>
<td>14-236</td>
</tr>
<tr>
<td>[E][4]</td>
<td>Transfer and Disclosure</td>
<td>14-238</td>
</tr>
<tr>
<td>[E][5]</td>
<td>Sensitive Data</td>
<td>14-239</td>
</tr>
<tr>
<td>[E][6]</td>
<td>Enforcement</td>
<td>14-239</td>
</tr>
<tr>
<td>[E][7]</td>
<td>Data Breach Notification</td>
<td>14-240</td>
</tr>
<tr>
<td>[F]</td>
<td>United Arab Emirates</td>
<td>14-241</td>
</tr>
<tr>
<td>[F][1]</td>
<td>Overview</td>
<td>14-241</td>
</tr>
<tr>
<td>[F][1][a]</td>
<td>UAE</td>
<td>14-242</td>
</tr>
<tr>
<td>[F][1][b]</td>
<td>DIFC</td>
<td>14-243</td>
</tr>
<tr>
<td>[F][1][c]</td>
<td>ADGM</td>
<td>14-243</td>
</tr>
<tr>
<td>[F][2]</td>
<td>Personal Information</td>
<td>14-243</td>
</tr>
<tr>
<td>[F][2][a]</td>
<td>UAE</td>
<td>14-243</td>
</tr>
</tbody>
</table>
Chapter 15  Compliance with the Payment Card Industry Data Security Standard

Mark MacCarthy, Pieter Penning & David Ames

§ 15:1  Introduction ................................................................. 15-2
§ 15:2  Background ................................................................. 15-6
  § 15:2.1  Industry Background ................................................ 15-6
  § 15:2.2  Federal Consumer Protection Laws .............................. 15-9
  § 15:2.3  Data Security Regulations ........................................ 15-10
    [A]  Federal Regulation .................................................. 15-10
    [B]  State Regulation .................................................. 15-12
§ 15:3  Development of the Payment Card Industry Data Security Standard .................................................. 15-13
§ 15:4  PCI Requirements ........................................................ 15-19
  § 15:4.1  The Basic Requirements ........................................... 15-19
  Figure 15-1  Payment Card Industry Data Security Standard........... 15-20
  § 15:4.2  Protecting Stored Data ........................................... 15-24
  Figure 15-2  PCI Requirement 3: Protect Stored Cardholder Data .................................................. 15-24
  § 15:4.3  Encrypt Transmission of Cardholder Data
            Across Open, Public Networks .................................. 15-29
  Figure 15-3  Requirement 4: Encrypt Transmitted Data .............. 15-30
Table of Contents

§ 15:4.4 Compensating Controls ........................................... 15-31
§ 15:4.5 Payment Applications ............................................. 15-31
§ 15:5 Validation ..................................................................... 15-33
§ 15:5.1 Merchant Levels .................................................... 15-35
Figure 15-4 Merchant Levels (Visa CISP) ................................. 15-36
§ 15:5.2 Service Provider Levels ........................................... 15-36
Figure 15-5 Service Provider Levels (Visa CISP) ....................... 15-37
§ 15:5.3 Merchant Validation Requirements .............................. 15-38
Figure 15-6 Merchant Levels and Validation Requirements (Visa CISP) ............................................................ 15-38
§ 15:5.4 Service Provider Validation Requirements ..................... 15-39
Figure 15-7 Service Provider Levels and Validation Requirements (Visa CISP) ..................................... 15-40
§ 15:5.5 Corporate Franchise Servicers .................................... 15-40
§ 15:6 After a Compromise ..................................................... 15-42
§ 15:6.1 Background ............................................................ 15-42
§ 15:6.2 Initial Steps ........................................................... 15-44
§ 15:6.3 Monitoring At-Risk Accounts ................................ 15-47
§ 15:6.4 Notification to Issuing Financial Institutions ............... 15-48
§ 15:7 Enforcement ................................................................. 15-50
§ 15:7.1 General ................................................................ 15-50
§ 15:7.2 Enforcement Efforts ............................................... 15-51
§ 15:7.3 CardSystems Solutions .......................................... 15-53
§ 15:7.4 Other Significant Data Breaches ............................... 15-54
§ 15:8 Continued Development of Cardholder Data Protection ............................................................ 15-56
§ 15:8.1 Increasing Global Compliance .............................. 15-56
§ 15:8.2 Chip and PIN Security .......................................... 15-57
§ 15:8.3 Tokenization .......................................................... 15-60
§ 15:8.4 Point-to-Point Encryption ...................................... 15-61
§ 15:8.5 Mobile Payments ................................................... 15-61
§ 15:8.6 Cloud Computing.................................................. 15-63
§ 15:8.7 E-Commerce .......................................................... 15-64
§ 15:8.8 Risk Assessments .................................................. 15-65

Chapter 16 Insurance Coverage for Data Breaches and Unauthorized Privacy Disclosures

Steven R. Gilford

§ 16:1 Overview......................................................................... 16-2
§ 16:2 Applicability of Historic Coverages ................................. 16-7
§ 16:2.1 First- and Third-Party Coverages for Property Loss ............................................................ 16-7
[A] First-Party Property Policies ............................................. 16-8
Chapter 17   Data Breach Litigation

Margaret A. Dale & David A. Munkittrick

§ 17:1   Introduction ......................................................... 17-2
§ 17:2   Consumer Plaintiff Theories of Liability ............. 17-2
  § 17:2.1   Causes of Action ............................................. 17-2
    [A]   Negligence ....................................................... 17-2
    [B]   Breach of Contract ............................................ 17-3
    [C]   Fraud ............................................................... 17-3
§ 17:2.2 Actual Damages................................................................. 17-3
§ 17:3 Defense Strategies .............................................................. 17-4
§ 17:3.1 Standing .................................................................... 17-4
[A] The Supreme Court on Standing........................................ 17-4
[B] Data Breach Standing in Circuit Courts of
Appeals ................................................................................... 17-7
§ 17:3.2 Failure to State a Claim upon Which Relief
Can Be Granted [Rule 12(b)(6)] ........................................... 17-14
§ 17:3.3 Surviving Other Motions ............................................. 17-17
[A] Motions for Summary Judgment ..................................... 17-17
[B] Motions for Class Certification ....................................... 17-17
§ 17:4 Non-Consumer Plaintiffs ............................................... 17-18
§ 17:4.1 Shareholder Derivative Suits .................................... 17-18
§ 17:4.2 Claims Brought by Financial Institutions .......... 17-19
§ 17:5 Noteworthy Settlements ................................................ 17-20

Chapter 18 Location Privacy: Technology and the Law

David A. Munkittrick

§ 18:1 Introduction ................................................................... 18-2
§ 18:2 Development and Uses of Location-Tracking
Technologies ........................................................................ 18-2
§ 18:2.1 Overview .................................................................. 18-2
§ 18:2.2 Global Positioning Systems ..................................... 18-5
§ 18:2.3 Cell Site Location Information ................................ 18-7
§ 18:2.4 Indoor Positioning Systems .................................. 18-10
[A] Radio Frequency Identification .................................. 18-10
[B] Other IPS Technologies ............................................. 18-11
§ 18:2.5 Vehicle Tracking .................................................... 18-12
§ 18:2.6 Unmanned Drones ................................................ 18-13
§ 18:3 Government Collection of Location Information .......... 18-14
§ 18:3.1 Location Privacy Under the Fourth Amendment .... 18-14
§ 18:3.2 Government Requests for CSLI ............................ 18-17
[A] Federal Statutes ......................................................... 18-17
[B] Case Law .................................................................... 18-20
[C] State Laws .............................................................. 18-25
§ 18:4 Private Collection and Use of Location Information ...... 18-27
§ 18:4.1 GPS Tracking ......................................................... 18-27
[A] State Laws .............................................................. 18-27
[B] Case Law ............................................................... 18-27
[C] Industry Self-Regulation .......................................... 18-30
§ 18:4.2 Mobile Devices and Applications ......................... 18-32
[A] Agency Guidance ........................................................ 18-32
[B] Litigation ................................................................. 18-34
§ 18:4.3 Other Location Technologies ......................... 18-40
  [B] Vehicle Tracking ........................................ 18-41
  [C] Unmanned Drones ....................................... 18-42
§ 18:5 Legislative Outlook ...................................... 18-44
§ 18:5.1 Federal Proposals ..................................... 18-44
§ 18:5.2 State Legislation ..................................... 18-45

Index .............................................................................. I-1
Introduction

The concept of individual privacy has evolved over the course of centuries, and that evolution has only intensified over the course of the last decade. This rapid evolution not only is a challenge to both writers and editors of a treatise focusing on the legal aspects of privacy issues—but also is what makes privacy and data security law such an exciting area of practice.

In a typical constitutional law class during the mid 1990s, discussions of privacy related to search and seizure, freedom of speech and association, and the right to have an abortion. Today, any discussion of privacy would have to include the words “targeted advertising,” “social media,” and “geolocation.”

Advances in technology—particularly in the areas of broadband, the web, cloud computing, mobile apps, big-data analytics—have made it possible, and in fact easy, to aggregate masses of data about individuals into a readily available and searchable format. Information that formerly was housed in file cabinets is now archived in electronic databases that can be accessed remotely. And with many companies still struggling to find a way to make their online or mobile businesses profitable, monetizing their consumer databases has been one of the most obvious choices.

The laws and policies that regulate our conduct are often slow to catch up, and laws that are enacted for a certain purpose sometimes raise unintended privacy issues.

Privacy cannot be discussed without also addressing the issue of data security. Reported data security breaches have increased every year since public reporting began to be required, with so-called mega breaches involving millions of consumers unfortunately becoming an all-too-common occurrence. Data security companies have been engaged in a seemingly endless cat-and-mouse game with online hackers, with each side’s tactics becoming more and more sophisticated. Whether it is from malware, phishing, ransomware, a point-of-sale data scraper, or other intrusion, the new trope—“it’s not if a company will hacked, but when”—has, in many industries, become the unfortunate new reality. Given the current security environment, cybersecurity is no longer merely the work of a company’s IT department, but one of the major concerns of the general counsel and board of directors.
While much attention has been paid to financial identity theft for the last several years, new attention has focused on medical identity theft. Hijacking of one's medical identity can actually cause more harm than mere financial loss by the inclusion of incorrect diagnostic and medical history information in one's medical records. Still, not all of the forty-seven U.S. state breach notification laws include medical information among the types of data that, if compromised, would trigger a consumer notification requirement. The HITECH Act rectified this at the federal level. Still unaddressed, however, is the lack of an efficient method by which victims of medical identity theft can clear their medical records of incorrect and potentially harmful information.

In some cases, the difficulty in updating the laws comes from competing, contradictory policy objectives. Since 9/11, a tension has been growing between the right to privacy and the desire of governments to have access to information about individuals for purposes of law enforcement and counterterrorism. In the wake of the Snowden revelations regarding the extent of U.S. surveillance activities and the ongoing discussion over whether the government should have access to encrypted mobile communications for investigative purposes, the national debate continues over where to draw the line on personal privacy. At the same time that laws are being enacted that require companies to retain consumer information for law enforcement purposes, other laws are being enacted that require companies to dispose of consumer information to protect privacy.

Behavioral marketing is increasingly undergoing both media and legislative scrutiny, but not federal regulation (yet) in the United States. At its inception years ago, online behavioral marketing was largely limited to “contextual ads” tailored to website content and “keyword ads” tailored to user-chosen search terms, each of which raised relatively few eyebrows. More recent forms of behavioral marketing, or targeted advertising, track users as they travel around the web and across multiple devices, and are, therefore, more concerning to privacy advocates than their older siblings. Ad networks and deep packet inspection technology enable ads to be targeted to online users based on the various online properties they visit over time. Also, the accumulation of information derived from such advertising efforts has raised privacy concerns. Privacy advocates even remain concerned about the real risk of reidentification of anonymized data, given the advances of technology. Similarly, cable television providers (and so-called over-the-top [OTT] providers that serve video over the Internet) have begun, in some cases, to serve targeted television ads based on household demographics. So the ad you see may be different from the ad your neighbor sees on the same channel at the same time. The pioneers of these enhanced forms of behavioral marketing will be
challenged by regulators and legislators to either show that they will effectively self-regulate their privacy practices, or else bear the burden of new laws that will impose legally enforceable privacy protections.

Mobile privacy is another area that will see increased regulatory and legislative oversight in the near future. Geolocation technologies enable ads to be targeted to consumers based on their physical location in real time, using the GPS technology on smart phones. Similarly, GPS devices in automobiles are being used by law enforcement to apprehend criminals, by rental car companies to track vehicle whereabouts, and by auto insurers to assess insurance rates. While there has been little regulation in this area so far, more attention to mobile privacy can be expected going forward.

Diverse views on individual privacy internationally also make navigating the privacy arena challenging for global enterprises. Not only is the European privacy regime vastly different from the approach in the United States, but even within the EU, there are some member states that take a strict stance on privacy in their national laws, and other member states that take a less rigid stance. EU privacy regulation has undergone major changes in recent years (for example, the invalidated EU-U.S. Safe Harbor, the approval of the General Data Protection Regulation (GDPR), the uncertainty surrounding “Brexit,” the withdrawal of the United Kingdom from the EU), compelling companies that conduct business internationally to alter their practices. Beyond Europe, countries in the Far East, Asia, and Latin America that previously may not have had strong privacy protections have enacted new laws to keep pace with the new realities of global commerce and online data collection, adding new compliance risks for companies. Doing business globally, therefore, still means defining privacy practices that comply with a host of different national laws.

What we have seen in the area of privacy over the last several years can be said to call into question the legal standard on which privacy rights have been based for decades: Is there a reasonable expectation of privacy? With the rapid evolution of new technologies that manipulate individual data in new, novel, and previously unexpected ways, the answer to that question changes faster than you can say “privacy.”

This treatise attempts to capture the broad range of privacy issues of most interest to enterprises; at the same time it seeks to present those issues with sufficient depth to provide a useful reference and a solid foundation for more detailed research in this fast-paced area of the law.