

# Detailed Table of Contents

	<i>Main Volume</i>	<i>Supple- ment</i>
PREFACE.....	v	v
ABOUT THE AUTHOR AND CONTRIBUTOR.....	ix	ix
ACKNOWLEDGMENTS.....	xi	xi
DEDICATION.....	xiii	xiii
SUMMARY TABLE OF CONTENTS .....	xv	xv
CHAPTER 1    A DEVELOPING CRISIS .....	1	1-1
I.    Introduction .....	1	1-1
II.   Magnitude of the Problem .....	5	1-2
A.   Potential Liability From Private Consumers ...	6	—
B.   Regulatory and State Actions .....	10	—
C.   Damages Incurred by Credit Card Companies and Banks Facing Breaches.....	12	—
<b>Part I</b>		
<b>SOURCES OF LIABILITY</b>		
CHAPTER 2    DATA PROTECTION AND DISCLOSURE OBLIGATIONS FOR FINANCIAL INSTITUTIONS .....	   17	   2-1
I.    Introduction .....	18	2-2
II.   The Gramm-Leach-Bliley Act of 1999 .....	18	2-3
A.   Who Is Obligated to Take Action Under the Gramm-Leach-Bliley Act? .....	 20	 —
B.   Who Is Protected by the Gramm-Leach-Bliley Act? .....	 21	 —
C.   What Must Be Done to Comply With the Gramm-Leach-Bliley Act? .....	 21	 —
D.   Enforcement Under the Gramm-Leach-Bliley Act.....	 22	 2-3
E.   Criminal Liability Under the Gramm-Leach- Bliley Act.....	 23	 —

	<i>Main Volume</i>	<i>Supple- ment</i>
III. Fair Credit Reporting Act .....	24	2-3
A. Ensuring the Accuracy of Consumer Reports [Substitute Text] .....	—	2-3
1. Defining Consumer Reports [Substitute Text] .....	—	2-4
2. Obligations of Consumer Credit Reporting Agencies [Substitute Text] .....	—	2-5
3. Obligations of Furnishers of Information [New Topic].....	—	2-10
B. Overview of Procedures Governing the Use of Credit and Investigative Reports.....	27	2-12
C. Requirement of an Identity Theft Prevention Program.....	29	—
D. Disposal Plans .....	30	2-12
E. Damages Under the Fair Credit Reporting Act 1. Existence of a Private Right of Action [New Topic].....	32	2-13
2. Damages Applicable to Negligent and Willful Violations [New Topic].....	—	2-15
F. Civil Money Penalties Under the Fair Credit Reporting Act.....	34	2-15
G. Criminal Offenses Under the Fair Credit Reporting Act.....	34	—
1. Obtaining Information From a Consumer Credit Reporting Agency by False Pretenses: 15 U.S.C. §1681q.....	35	—
2. Unauthorized Disclosures by Officers or Employees: 15 U.S.C. §1681r.....	36	—
IV. Bank Secrecy Act .....	37	2-15
A. Filing Suspicious Activity Reports .....	38	—
B. Structuring Transactions to Avoid Reporting Transactions .....	39	—
V. Plastic Card Security Acts.....	40	—
VI. Electronic Fund Transfer Act .....	42	2-15
A. Applicability of the Electronic Fund Transfer Act.....	42	—
B. Notice and Disclosure Requirements Under the Electronic Fund Transfer Act .....	42	2-15
1. Initial Disclosures Required by Financial Institutions.....	43	—
2. Notices Required for Preauthorized Transfers .....	43	—
3. Limitation on Consumer Liability.....	44	2-15

	<i>Main Volume</i>	<i>Supple- ment</i>
CHAPTER 3 SPECIAL PROBLEMS IN THE HEALTH CARE INDUSTRY .....	47	3-1
<i>John E. Wyand</i>		
<i>Squire Patton Boggs, Washington, D.C.</i>		
I. Introduction .....	48	—
II. The Health Insurance Portability and Accountability Act of 1996 .....	49	3-2
A. Statutory and Regulatory Scheme .....	49	—
B. Relationship With State Laws and Preemption .....	50	—
C. The HIPAA Rules Cover the Use and Disclosure of Protected Health Information by a “Covered Entity” or “Business Associate” .....	51	—
1. What Information Is Covered by the HIPAA Rules? .....	51	—
2. Who Is Subject to the HIPAA Rules?.....	54	—
a. Covered Entities .....	54	—
i. Health Plans .....	54	—
ii. Health Care Clearinghouses .....	55	—
iii. Health Care Providers .....	55	—
iv. Organizational Options for Covered Entities .....	56	—
b. Business Associates .....	57	—
D. Requirements of the Privacy Rule .....	60	3-2
1. General Principles.....	60	—
2. Permitted Uses and Disclosures of Protected Health Information .....	60	—
3. Authorized Uses and Disclosures of Protected Health Information .....	61	—
4. Limiting Uses and Disclosures to the Minimum Necessary.....	61	—
5. Notice and Other Individual Rights.....	61	—
6. Personal Representatives and Minors .....	62	3-2
7. Special Concerns for Psychotherapy Notes and Mental Health and Substance Abuse Providers; Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act.....	62	3-3
E. Requirements of the Security Rule.....	63	—
1. General Principles.....	63	—
2. Security Management Process.....	63	—
3. Other Administrative Safeguards .....	64	—
4. Physical Safeguards .....	65	—
5. Technical Safeguards .....	65	—

	<i>Main Volume</i>	<i>Supple- ment</i>
F. Requirements of the Breach Notification Rule .....	65	—
1. Definitions .....	65	—
2. Definition of Breach Discovery .....	66	—
3. Analysis of Security Incident .....	66	—
4. Risk Assessment.....	67	—
5. Notification by a Business Associate.....	68	—
6. Notification of Breach to the Individual ...	69	—
7. Notification to the Media .....	70	—
8. Notification to the Secretary of HHS.....	70	—
G. The Enforcement Rule.....	70	—
H. Requirements for Policies and Procedures.....	72	—
I. HIPAA Training .....	76	—
J. Enforcement Actions [Substitute Text] .....	77	3-3
K. OCR HIPAA Audits.....	79	3-6
1. General Principles [New Heading] .....	—	3-6
2. Phase 2 HIPAA Audit Program [New Topic].....	—	3-6
III. Red Flags Rule for Health Care Providers.....	80	—
 CHAPTER 4 THE FEDERAL STATUTORY LANDSCAPE BEYOND THE FINANCIAL AND HEALTH CARE INDUSTRIES .....		
	83	4-1
I. Introduction .....	84	—
II. The Federal Trade Commission Act.....	85	4-3
A. Application of the FTC Act to Cybersecurity [New Topic] .....	—	4-4
1. The Requirement of an “Unfair or Deceptive Practice [New Topic].....	—	4-5
2. The Requirement of “Substantial Injury” [New Topic].....	—	4-9
3. The Requirement that the Injury is not “Reasonably Avoidable by Consumers” [New Topic].....	—	4-11
4. The Requirement that the Risk of Injury is Not Outweighed by Countervailing Benefits [New Topic].....	—	4-12
B. The Lack of a Private Right of Action Under the FTC Act [New Topic] .....	—	4-13
III. The Children’s Online Privacy Protection Act of 1998 .....	92	—
A. The Statutory Scheme .....	92	—
B. The Regulatory Scheme .....	92	—
C. Judicial Construction of COPPA.....	96	—

	<i>Main Volume</i>	<i>Supple- ment</i>
IV. Computer Fraud and Abuse Act of 1984 .....	97	4-14
A. The Statutory Scheme .....	98	—
1. Prohibitions Regarding Non-Protected Computer Systems.....	98	—
2. Prohibitions Regarding “Protected Computer” Systems .....	99	—
B. Construction of the CFAA.....	100	4-14
1. Elements of the Offense .....	100	4-14
2. Venue Considerations.....	104	—
3. Existence of a Private Cause of Action [Substitute Text] .....	105	4-16
V. Identity Theft.....	105	4-18
VI. Electronic Communications Privacy Act.....	107	4-21
A. Interception of Electronic Communications..	109	4-21
1. Intent Requirement .....	110	—
2. Requirement of an “Interception” .....	110	4-21
3. By “Electronic, Mechanical or Other Device” .....	114	—
4. “Communication” Defined.....	115	—
a. Oral Communications and the Expectation of Privacy.....	115	—
b. Wire Communications .....	115	—
5. “Content” [New Topic].....	—	4-21
B. Use or Disclosure of Intercepted Communication .....	117	—
C. Exceptions to the ECPA .....	118	4-24
1. Consent.....	119	4-24
2. Assistance to Users by Switchboard Operators and Providers.....	122	—
3. Protecting Property Rights .....	122	—
4. Government Officials.....	124	—
D. Private Cause of Action .....	124	—
VII. Stored Communications Act.....	126	4-26
A. Prohibited Access.....	127	4-26
1. The Definition of an ECS Facility [Substitute Text] .....	128	4-26
2. Defining “Unauthorized” Access.....	130	—
3. Requirement of an Interception.....	131	—
B. Prohibited Disclosures.....	131	—
C. Required Disclosures to the Government [Substitute Text] .....	133	4-27
D. Liability Under the Stored Communications Act.....	137	—
1. Criminal Liability .....	137	—
2. Civil Liability.....	138	—

	<i>Main Volume</i>	<i>Supple- ment</i>
VIII. Foreign Intelligence Surveillance Act of 1978 .....	138	4-28
A. Procedures Governing the Use of Electronic Surveillance by the Government .....	139	4-28
B. Criminal Violations Under FISA.....	142	—
C. Civil Actions for Violating FISA .....	143	—
IX. The PATRIOT Act of 2001 .....	144	—
X. The USA FREEDOM Act of 2015 [New Topic] .....	—	4-28
XI. Economic Espionage Act .....	148	4-30
A. The Statutory Scheme .....	148	—
B. Judicial Construction of the Statute .....	149	—
1. Defining “Secret” Information Broadly .....	150	—
2. The Element Dealing With Interstate Commerce .....	151	—
XII. The Cable Act.....	153	4-30
XIII. Telecommunications Act .....	154	4-30
XIV. The Family Educational Rights and Privacy Act....	157	4-30
XV. Video Privacy and Protection Act.....	159	4-31
XVI. Controlling the Assault of Non-Solicited Pornography and Marketing Act [New Topic] .....	—	4-31
1. The Criminal Statutory Scheme.....	—	4-32
2. Civil and Enforcement Provisions Under the CAN-SPAM Act.....	—	4-33
3. Existence of a Private Right of Action .....	—	4-36
XVII. The Cybersecurity Act of 2015 [New Topic].....	160	4-38
A. Monitoring of Existing Systems [New Topic] .	—	4-38
B. Defensive Measures [New Topic] .....	—	4-41
C. Sharing or Use of Cybersecurity Information [New Topic] .....	—	4-42
1. Restrictions on Non-Federal Entities Receiving Cybersecurity Information [New Topic].....	—	4-42
2. Restrictions on Federal Entities Receiving Cybersecurity Information [New Topic] ...	—	4-44
XVIII. Communications Assistance to Law Enforcement Act [New Topic] .....		4-46
 CHAPTER 5     PRIVACY ISSUES RELATING TO GOVERNMENT RECORDS .....	 165	 5-1
I. Introduction .....	166	5-2
II. Federal Privacy Act of 1974.....	167	—
A. Overview of the Statutory Scheme.....	167	—
B. Judicial Construction of the Statutory Scheme	168	—
1. Maintaining the Integrity of Records.....	169	—
a. Disclosures .....	170	—
b. Notice Provisions .....	170	—
2. Applicability of the Act to Government Agencies.....	171	—

	<i>Main Volume</i>	<i>Supple- ment</i>
3. Persons Protected by the Act and the Right of Access.....	172	—
4. Records Protected by the Act .....	173	—
5. Defining “Records” .....	173	—
6. Defining a “System of Records”.....	174	—
7. Maintenance of Records for Improper Purposes.....	176	—
8. Permitted Disclosures .....	178	—
a. Intra-Agency Disclosures .....	178	—
b. Disclosures Required Under FOIA.....	179	—
c. Routine Use .....	179	—
d. Bureau of the Census .....	180	—
e. Statistical Research .....	180	—
f. National Archives .....	181	—
g. Law Enforcement .....	181	—
h. Emergency Disclosures.....	182	—
i. Congress.....	182	—
j. Government Accounting Office .....	182	—
k. Court Order .....	182	—
l. Consumer Reporting Agency .....	183	—
m. Social Security Numbers .....	183	—
9. Private Rights of Action .....	183	—
III. Freedom of Information Act .....	184	5-3
A. The Statutory Scheme .....	185	—
1. Exemption Three: Relating to the Material Protected from Disclosure by Other Statutory Schemes.....	186	—
2. Exemption Four: Relating to Privileged and Confidential Trade or Financial Records ..	187	—
3. Exemption Six: Relating to Personnel and Medical Records.....	187	—
4. Exemption Seven: Relating to Investigative Records .....	189	—
B. Governmental Responses to FOIA Requests...	190	5-3
1. Searching for and Producing Responsive Documents [New Topic] .....	—	5-3
2. Refusing to Produce Responsive Documents Based on Exemption [New Topic].....	—	5-5
3. Refusals to Acknowledge Responsive Documents.....	190	5-5
4. Use of Redactions or Disclosure of Summaries .....	191	5-5
IV. Right to Financial Privacy Act.....	193	—

	<i>Main Volume</i>	<i>Supple- ment</i>
CHAPTER 6		
STATE LAWS GOVERNING CYBERSECURITY, CONSUMER DATA, AND PRIVACY PROTECTION .....	197	6-1
I. Introduction .....	197	—
II. The Uniform Commercial Code .....	198	—
III. Breach Notification Statutes .....	200	—
IV. Statutes Prohibiting Deceptive Practices .....	201	—
V. Uniform Theft of Trade Secrets Act.....	204	—
VI. Selected State Statutes.....	206	6-2
A. California.....	206	6-2
1. Data Protection .....	207	—
2. Online Privacy Protection Act.....	208	—
3. Unfair Competition Law.....	209	6-2
B. Massachusetts Personal Information Law .....	212	—
C. Nevada Encryption Law.....	215	—
D. Delaware Data Destruction Act.....	217	—
E. Minnesota Laws Regulating Disclosures by Internet Service Providers.....	218	—
VII. Special Problems or Tactics .....	218	6-4
A. Pretext Calling .....	219	—
B. Spyware.....	220	—
C. Browser Hijacking and Botnets.....	222	—
D. Spam [New Topic].....	—	6-4
E. Phishing and Spoofing [New Topic] .....	—	6-7
CHAPTER 7		
DATA BREACH AND PRIVACY LIABILITY BEYOND FEDERAL AND STATE STATUTES ....	225	7-1
I. Introduction .....	225	—
II. Negligence .....	226	7-1
III. Negligent Misrepresentation or Omission .....	230	7-2
IV. Negligence Per Se .....	232	—
V. Breach of Fiduciary Duty .....	234	7-3
VI. Fraud and Fraudulent Misrepresentations .....	235	—
VII. Breach of Implied Contracts .....	236	7-4
VIII. Unjust Enrichment.....	239	7-4
IX. Invasion of Privacy.....	241	7-4
A. Defining the Elements of the Cause of Action	242	7-4
1. The California Approach.....	242	7-4
2. Standards Outside California .....	245	—
B. Must Disclosures be Made to the Public, or Only to any Third Party?.....	246	—
X. Bailment.....	249	—



**Part II**  
**AVOIDING OR MINIMIZING LITIGATION RISK**

CHAPTER 8	INTERNAL CONTROLS .....	253	8-1
I.	Introduction .....	253	—
II.	Director and Officer Involvement and Reporting .....	254	8-1
A.	Liability of Officers and Directors .....	254	8-2
B.	Statutory Duties Imposed on Public Companies to Disclose Risks .....	257	8-3
III.	The Role of the Chief Information Officer and Data Privacy and Security Team .....	259	—
IV.	The Privacy Notice .....	262	—
V.	Developing a Cybersecurity and Data Privacy Plan .....	263	8-4
A.	Plan Components .....	264	8-4
1.	Mandatory Security Plan Considerations ..	267	—
2.	Recommended Plan Components .....	271	—
3.	Employee Management and Training .....	271	8-5
4.	Handling Confidential, Nonpublic Information .....	274	8-6
B.	The Disposal Plan .....	276	—
C.	The Incident Response .....	277	8-7
VI.	Examination of Internal Controls .....	277	8-7
A.	Consumer Financial Protection Board.....	277	—
B.	Securities and Exchange Commission .....	280	8-7
C.	New York State Department of Financial Services .....	280	—
CHAPTER 9	INCIDENT RESPONSE .....	285	9-1
I.	Introduction .....	285	—
II.	Developing a Plan .....	286	9-1
A.	Define Conduct Meriting a Response .....	288	9-1
B.	Policy, Plan, and Procedure Elements.....	288	9-2
1.	Policy Elements .....	289	9-2
2.	Plan Elements.....	289	—
3.	Procedure Elements.....	290	—
III.	Cooperating With Law Enforcement .....	291	—
IV.	Duties to Provide Notice of a Breach .....	294	—
A.	Timing of Notice.....	296	—
B.	Parties to Receive Notice.....	299	—
C.	Content of Notice .....	299	—

**Part III**  
**LITIGATION TACTICS**

CHAPTER 10	PRE-LITIGATION ISSUES .....	305	10-1
I.	Introduction .....	305	10-1
II.	Preparing for Litigation or Other Proceedings.....	305	10-1
A.	The Litigation Team [New Topic].....	—	10-2
B.	Data Preservation.....	306	10-3
C.	The Litigation Hold.....	307	10-3
III.	The Initial Inquiry.....	311	10-3
CHAPTER 11	LITIGATION STRATEGIES ARISING FROM DATA BREACH AND CYBERSECURITY DISPUTES .....	315	11-1
I.	Introduction .....	317	—
II.	Dealing With Multiple Lawsuits.....	317	—
III.	The Motion to Dismiss .....	318	11-3
A.	Allegations of a Causal Connection Must Be Sufficient to Withstand a Motion to Dismiss...	319	—
B.	Fraud Must Be Pled With Sufficient Particularity to Withstand a Motion to Dismiss.....	319	—
C.	Focusing on Temporal Breaks Between the Breach and the Use of Data or Information ...	323	11-3
D.	Pleading Damages with Sufficient Specificity [New Topic] .....	—	11-4
IV.	Direct vs. Derivative Actions .....	324	—
A.	Demand Futility Generally .....	325	—
1.	Demand Futility Under the ABA Model Business Corporation Act.....	326	—
2.	Demand Futility Under the ALI Restatement	326	—
3.	Demand Futility Under State Common Law	327	—
B.	Demand Futility in the Data Breach Context .	328	—
1.	Demonstrate That the Claimed Conduct Did Not Arise by Virtue of Any Self-Interest	328	—
2.	Demonstrate the Need for the Board to Investigate the Causes of the Data Breach Given Its Complexity.....	329	—
3.	Consider Whether Any Ongoing Law Enforcement Investigation and Cooperation with Law Enforcement Would Be Jeopardized by Rushing into a Derivative Suit .....	330	—

	<i>Main Volume</i>	<i>Supple- ment</i>
V. Class Certification.....	330	11-6
A. Class Certification Generally [Substitute Text] .....	332	11-6
B. Arguments Bearing on Class Certification or, Alternatively, Creation of Sub-Classes.....	332	11-7
1. Numerosity .....	332	—
2. Commonality .....	334	11-7
3. Typicality .....	335	—
4. Adequacy of Representation .....	337	—
5. Predominance [Substitute Text] .....	339	11-7
6. Superiority .....	341	—
7. Ascertainability .....	342	—
C. Settling the Class Action.....	343	11-9
1. Required Findings to Settle the Class Action .....	344	—
2. Settlement Risks .....	344	11-9
a. Opt-Outs.....	344	—
b. Lack of a Sufficient Class .....	345	11-9
VI. Discovery Issues .....	345	11-9
A. Overbroad Discovery Demands .....	346	—
B. Preserving the Confidentiality of Material Received Pursuant to a Subpoena or Document Request.....	347	11-9
C. Shifting the Cost of Responding to Discovery Demands .....	349	—
D. Retention of Forensic Experts or Computer Consultants.....	350	—
E. Risk of Disclosures .....	352	—
1. Disclosure of In-house or Outside Nonlawyer Testimony or Evidence.....	352	—
2. Application of Privileges to Computer Consultants Hired in Connection With Litigation .....	352	—
3. Experts Hired in Connection With Trial ...	355	—
F. Disclosure of Remedial Measures .....	357	—
VII. Evidentiary Issues at Trial.....	359	11-10
A. Evidence Relating to the Standard of Care.....	359	11-10
1. Applicable Rules and Regulations .....	360	—
2. Industry Standards .....	362	11-10
3. The Type of Data or Information Being Safeguarded.....	362	—
4. The Number of Consumers or Customers Possibly Affected by a Breach .....	363	—
5. The Relative Cost of Additional Protections	364	—
6. A Balancing of Interests.....	364	—

	<i>Main Volume</i>	<i>Supple- ment</i>
B. Prior Incidents and Notice of Vulnerabilities .	364	—
C. Evidence of Subsequent Remedial Efforts .....	368	—
D. The Role of the Expert.....	369	—
1. Testimony About the Reasonableness of the Defendant’s Conduct .....	370	—
2. Testimony About the Impact of a Data Breach.....	373	—
3. Testimony About the Governmental Regulations and Other Policies.....	374	—
E. Admissibility of Governmental Reports.....	375	—
1. Admissibility in General.....	377	—
2. Factors Potentially Affecting Admissibility of Governmental Reports .....	379	—
a. The Nonfinal Nature of the Report .....	379	—
b. The Purposes to Be Served by the Report	381	—
c. Past Challenges to the Report .....	383	—
d. Investigative Techniques .....	384	—
e. The Sources for the Report .....	385	—
f. The Report’s Credibility Assessments...	387	—
g. The Timeliness of the Investigation .....	387	—
h. Special Skill or Expertise of the Authors of the Report.....	387	—
 CHAPTER 12 AFFIRMATIVE DEFENSES APPLICABLE TO DATA BREACH AND PRIVACY LITIGATION...	 389	 12-1
I. Introduction .....	389	—
II. Defenses to Federal Jurisdiction.....	390	—
III. Jurisdiction Under State Long-Arm Statutes [Substitute Text].....	393	12-2
IV. Venue .....	396	—
V. Lack of Standing.....	397	12-6
A. Standing Applied in Data Breach Cases Involving Lost or Stolen Information [Amended Heading] .....	308	12-7
B. Standing Based on Product Defects [New Topic] .....	—	12-8
1. Standing Based on Risk of Impending Harm [New Topic].....	—	12-8
2. Standing Based on Overpayment for the Product [New Topic] .....	—	12-9
C. Special Standing Issues Posed by a Loss of Privacy [New Topic] .....	—	12-10
D. Standing Under the Fair Credit Reporting Act.....	404	12-12
VI. Lack of Causation .....	408	—
VII. Lack of Foreseeability.....	413	—
VIII. Lack of Privity .....	415	—

Detailed Table of Contents

xxxix

	<i>Main Volume</i>	<i>Supple- ment</i>
IX. Preemption .....	416	—
X. Economic Loss Rule .....	418	—
XI. Intervening Acts of Third Parties .....	420	—
XII. Reliance on Disclaimers .....	421	—
XIII. First Amendment Protections [New Topic] .....	—	12-15
A. Concerns Over the Content of Speech [New Topic] .....	—	12-15
B. Concerns Over the Privacy of Speech [New Topic] .....	—	12-17
 CHAPTER 13 DAMAGES.....	 425	 13-1
I. Introduction .....	425	—
II. General Legal Precepts Governing an Award of Damages.....	426	13-1
A. Actual Damages .....	426	13-1
B. Damages Must Not Be Unduly Speculative.....	428	—
C. Foreseeability .....	429	—
D. Causation.....	430	—
E. Standing as a Guide to Damages .....	430	13-2
III. Specific Types of Damages.....	432	13-2
A. Charges for the Illegal Use of Lost or Stolen Data or Information .....	432	—
B. Cost of Issuing New Cards.....	434	—
C. Cost of Credit Monitoring.....	436	—
D. Time Spent Dealing With Credit Issues [Substitute Text] .....	437	13-2
E. Lost “Opportunity Costs” .....	438	—
F. The Loss of Value.....	438	—
G. The Loss of Privacy .....	440	—
H. Mental Distress.....	440	—
I. Punitive Damages .....	442	—
 APPENDIX 1 STATE STATUTES.....	 445	 A1-3
<b>Appendix 1.A.</b> State Computer Crime Statutes.....	447	A1-5
<b>Appendix 1.B.</b> Security Breach Notification Laws .....	449	—
<b>Appendix 1.C.</b> State Identity Theft Laws.....	451	A1-7
<b>Appendix 1.D.</b> State Spyware Statutes .....	453	—
<b>Appendix 1.E.</b> State Wiretap Statutes .....	455	—
<i>Appendix 1.E.1.</i> State Statutes Outlawing the Interception of Wire(w), Oral(o), and Electronic Communications(e) .....	455	—
<i>Appendix 1.E.2.</i> Consent Interceptions Under State Law.....	457	—
<i>Appendix 1.E.3.</i> Statutory Civil Liability for Interceptions Under State Law .....	459	—
<i>Appendix 1.E.4.</i> Court Authorized Interception Under State Law.....	461	—

	<i>Main Volume</i>	<i>Supple- ment</i>
<i>Appendix 1.E.5.</i> State Statutes Regulating Stored Electronic Communications (SE), Pen Registers (PR), and Trap and Trace Devices (T)	463	—
<b>Appendix 1.F.</b> State Anti-Spam statutes [New Appendix] .....	—	A1-9
APPENDIX 2 ENFORCEMENT ACTIONS .....	465	—
<b>Appendix 2.A.</b> FTC Allegations/Settlements Relating to Data Privacy and/or Breaches .....	467	—
<b>Appendix 2.B.</b> Selected FTC Allegations/Settlements Relating to Violations of the Fair Credit Reporting Act Involving Data Privacy or Representations Regarding Financial Data.....	483	—
APPENDIX 3 GUIDELINES AND RESOLUTIONS.....	489	—
<b>Appendix 3.A.</b> Best Practices for Victim Response and Reporting of Cyber Incidents.....	491	—
<b>Appendix 3.B.</b> Computer Security Incident Handling Guide .....	507	—
<b>Appendix 3.C.</b> House Bill 624 on Sharing Certain Cyber Threat Intelligence.....	587	—
<i>Appendix 3.C.1.</i> S.2410, The Cybersecurity Disclosure Act of 2015, (114th Congress 1st Sess., 2015–2016) .....	—	A3-1
<b>Appendix 3.D.</b> Making Your Privacy Practices Public .....	615	—
TABLE OF CASES .....	643	T-1
INDEX .....	665	—