

About the Author xvii

Foreword to the Fourth Edition (2026) xix

Foreword to the Third Edition (2023) xxi

Foreword to the Second Edition (2019) xxiii

Acknowledgment and Disclaimers xxvii

Introduction to First Edition xxix

1 Data Security Laws and Enforcement Actions 1

1.1 FTC Data Security 2

1.1.1 Overview of Section 5 of the FTC Act 2

1.1.2 Wyndham: Does the FTC Have Authority to Regulate Data Security Under Section 5 of the FTC Act? 6

1.1.3 LabMD: What Constitutes “Unfair” Data Security? 10

1.1.4 FTC June 2015 Guidance on Data Security, and 2017 Updates 13

1.1.5 FTC Data Security Expectations and the NIST Cybersecurity Framework 18

1.1.6 Lessons from FTC Cybersecurity Complaints 18

1.1.6.1 Failure to Secure Highly Sensitive Information 19

1.1.6.1.1 Use Industry- standard Encryption for Sensitive Data 20

1.1.6.1.2 Routine Audits and Penetration Testing Are Expected 20

1.1.6.1.3 Health- Related Data Requires Especially Strong Safeguards 21

1.1.6.1.4 Data Security Protection Extends to Paper Documents 23

1.1.6.1.5 Business- to- Business Providers Also Are Accountable to the FTC for Security of Sensitive Data 25

1.1.6.1.6 Companies Are Responsible for the Data Security Practices of Their Contractors 27

1.1.6.1.7 Make Sure that Every Employee Receives Regular Data Security Training for Processing Sensitive Data 28

1.1.6.1.8 Privacy Matters, Even in Data Security	28
1.1.6.1.9 Limit the Sensitive Information Provided to Third Parties	29
1.1.6.1.10 Children's Data Requires Special Protection	29
1.1.6.1.11 Promptly Notify Customers of Breaches of Sensitive Data	30
1.1.6.2 Failure to Secure Payment Card Information	31
1.1.6.2.1 Adhere to Security Claims about Payment Card Data	31
1.1.6.2.2 Always Encrypt Payment Card Data	32
1.1.6.2.3 Payment Card Data Should Be Encrypted Both in Storage and at Rest	32
1.1.6.2.4 In- store Purchases Pose Significant Cybersecurity Risks	33
1.1.6.2.5 Minimize Duration of Storage of Payment Card Data	35
1.1.6.2.6 Monitor Systems and Networks for Unauthorized Software	35
1.1.6.2.7 Apps Should Never Override Default App Store Security Settings	36
1.1.6.3 Failure to Adhere to Security Claims	36
1.1.6.3.1 Companies Must Address Commonly Known Security Vulnerabilities	37
1.1.6.3.2 Ensure That Security Controls Are Sufficient to Abide by Promises About Security and Privacy	38
1.1.6.3.3 Omissions about Key Security Flaws Also Can Be Misleading	40
1.1.6.3.4 Companies Must Abide by Promises for Security- related Consent Choices	41
1.1.6.3.5 Companies That Promise Security Must Ensure Adequate Authentication Procedures	42
1.1.6.3.6 Adhere to Promises About Encryption	43
1.1.6.3.7 Promises About Security Extend to Vendors' Practices	44
1.1.6.3.8 Companies Cannot Hide Vulnerable Software in Products	44
1.1.7 FTC and Software Patching	44
1.2 State Data Breach Notification Laws	45

1.2.1 When Consumer Notifications Are Required	46
1.2.1.1 Definition of Personal Information	47
1.2.1.2 Encrypted Data	48
1.2.1.3 Risk of Harm	48
1.2.1.4 Safe Harbors and Exceptions to Notice Requirement	49
1.2.2 Notice to Individuals	49
1.2.2.1 Timing of Notice	49
1.2.2.2 Form of Notice	50
1.2.2.3 Content of Notice	50
1.2.3 Notice to Regulators and Consumer Reporting Agencies	51
1.2.4 Penalties for Violating State Breach Notification Laws	51
1.3 State Data Security Laws	51
1.3.1 Oregon	53
1.3.2 Rhode Island	54
1.3.3 Nevada	55
1.3.4 Massachusetts	56
1.3.5 Ohio	58
1.3.6 Alabama	59
1.3.7 New York	60
1.4 State Data Disposal Laws	60
2 Cybersecurity Litigation	63
2.1 Article III Standing	64
2.1.1 Applicable Supreme Court Rulings on Standing	66
2.1.2 Lower Court Rulings on Standing in Data Breach Cases	71

2.1.2.1 Injury- in- fact	71
2.1.2.1.1 Broad View of Injury- in- fact	71
2.1.2.1.2 Narrow View of Injury- in- fact	76
2.1.2.1.3 Attempts at Finding a Middle Ground for Injury- in- fact	80
2.1.2.2 Fairly Traceable	81
2.1.2.3 Redressability	83
2.2 Common Causes of Action Arising from Data Breaches	84
2.2.1 Negligence	84
2.2.1.1 Legal Duty and Breach of Duty	84
2.2.1.2 Cognizable Injury	87
2.2.1.3 Causation	91
2.2.2 Negligent Misrepresentation or Omission	93
2.2.3 Breach of Contract	95
2.2.4 Breach of Implied Warranty	102
2.2.5 Invasion of Privacy	106
2.2.6 Unjust Enrichment	108
2.2.7 State Consumer Protection Laws	110
2.3 Class Action Certification in Data Breach Litigation	113
2.3.1 <i>Kostka v. Dickey's Barbecue Restaurants</i> , Case No. 3:20- cv- 3424 (N.D. Tex. Oct. 14, 2022)	115
2.3.2 <i>In re Wawa, Inc. Data Security Litigation</i> , No. 19- cv- 6019 (E.D. Pa. July 30, 2021)	116
2.3.3 <i>In re Hannaford Bros. Co. Customer Data Security Breach Litigation</i> , No. 2:08- MD- 1954 (D. Me. Mar. 13, 2013)	117
2.3.4 <i>In re Heartland Payment Systems, Inc. Customer Data Security Breach Litigation: Consumer Track Litigation</i> , 851 F. Supp. 2d 1040 (S.D. Tex. 2012)	120

2.4 Insurance Coverage for Data Breaches 122

2.5 Protecting Cybersecurity Work Product and Communications from Discovery 126

2.5.1 Attorney– Client Privilege 128

2.5.2 Work Product Doctrine 131

2.5.3 Nontestifying Expert Privilege 133

2.5.4 Genesco v. Visa 134

2.5.5 In re Experian Data Breach Litigation 137

2.5.6 In re Premera 138

2.5.7 In re United Shore Financial Services 140

2.5.8 In re Dominion Dental Services USA, Inc. Data Breach Litigation 140

2.5.9 In re Capital One Consumer Data Security Breach Litigation 142

2.5.10 Securities and Exchange Commission v. Covington & Burling 142

3 Cybersecurity Requirements for Specific Industries 145

3.1 Financial Institutions: GLBA Safeguards Rule 146

3.1.1 Interagency Guidelines 146

3.1.2 SEC's Regulation S- P 148

3.1.3 FTC Safeguards Rule 150

3.2 Financial Institutions: Banking Organization Computer- Security Incident Notification Regulation 153

3.3 New York Department of Financial Services Cybersecurity Regulations 153

3.4 Financial Institutions and Creditors: Red Flags Rule 156

3.4.1 Financial Institutions or Creditors 159

3.4.2 Covered Accounts 160

3.4.3 Requirements for a Red Flags Identity Theft Prevention Program 161

3.4.4 Enforcement of the Red Flags Rule 162

3.5 Companies that Use Payment and Debit Cards: PCI DSS 162

3.6 Health Providers: HIPAA Security Rule 165

3.7 Electric Transmission: FERC Critical Infrastructure Protection Reliability Standards 171

3.7.1 CIP- 003- 8: Cybersecurity— Security Management Controls 171

3.7.2 CIP- 004- 7: Personnel and Training 172

3.7.3 CIP- 005- 7: Electronic Security Perimeters 172

3.7.4 CIP- 006- 6: Physical Security of Cyber Systems 172

3.7.5 CIP- 007- 6: Systems Security Management 173

3.7.6 CIP- 008- 6: Incident Reporting and Response Planning 173

3.7.7 CIP- 009- 6: Recovery Plans for Cyber Systems 173

3.7.8 CIP- 010- 4: Configuration Change Management and Vulnerability Assessments 174

3.7.9 CIP- 011- 2: Information Protection 174

3.7.10 CIP- 012- 1: Communications Between Control Centers 174

3.7.11 CIP- 013- 2: Supply Chain Risk Management 174

3.7.12 CIP- 14- 3: Physical Security of Cyber Systems 175

3.8 NRC Cybersecurity Regulations 175

3.9 State Insurance Cybersecurity Laws 176

3.10 Cyber Incident Reporting for Critical Infrastructure Act (cirtia) 179

4 Cybersecurity and Corporate Governance 181

4.1 SEC Cybersecurity Expectations for Publicly Traded Companies 182

4.1.1 Example of SEC Expectations: Yahoo! Data Breach 185

4.2 Fiduciary Duty to Shareholders and Derivative Lawsuits Arising from Data Breaches 186

4.3 CFIUS and Cybersecurity 190

4.4 Law Firms and Cybersecurity 192

5 Antihacking Laws 195

5.1 Computer Fraud and Abuse Act 196

5.1.1 Origins of the CFAA 196

5.1.2 Access Without Authorization and Exceeding Authorized Access 197

5.1.2.1 Narrow View of “Exceeds Authorized Access” and “Without Authorization” 200

5.1.2.2 Broader View of “Exceeds Authorized Access” and “Without Authorization” 205

5.1.2.3 Finding Some Clarity: Van Buren v. United States 207

5.1.2.4 Impact of Van Buren 210

5.1.3 The Seven Sections of the CFAA 212

5.1.3.1 CFAA Section (a)(1): Hacking to Commit Espionage 213

5.1.3.2 CFAA Section (a)(2): Hacking to Obtain Information 214

5.1.3.3 CFAA Section (a)(3): Hacking a Federal Government Computer 218

5.1.3.4 CFAA Section (a)(4): Hacking to Commit Fraud 220

5.1.3.5 CFAA Section (a)(5): Hacking to Damage a Computer 222

5.1.3.5.1 CFAA Section (a)(5)(A): Knowing Transmission that Intentionally Damages a Computer Without Authorization 223

5.1.3.5.2 CFAA Section (a)(5)(B): Intentional Access Without Authorization that Recklessly Causes Damage 226

5.1.3.5.3 CFAA Section (a)(5)(C): Intentional Access Without Authorization that Causes Damage and Loss 227

5.1.3.5.4 CFAA Section (a)(5): Requirements for Felony and Misdemeanor Cases 228

5.1.3.6 CFAA Section (a)(6): Trafficking in Passwords 230

5.1.3.7 CFAA Section (a)(7): Threatening to Damage or Obtain Information from a Computer 232

5.1.4 Civil Actions Under the CFAA 235

5.1.5 Criticisms of the CFAA	239
5.1.6 CFAA and Coordinated Vulnerability Disclosure Programs	241
5.1.7 Justice Department's 2022 CFAA Charging Policy	244
5.2 State Computer Hacking Laws	246
5.3 Section 1201 of the Digital Millennium Copyright Act	248
5.3.1 Origins of Section 1201 of the DMCA	249
5.3.2 Three Key Provisions of Section 1201 of the DMCA	250
5.3.2.1 DMCA Section 1201(a)(1)	250
5.3.2.2 DMCA Section 1201(a)(2)	255
5.3.2.2.1 Narrow Interpretation of Section (a)(2): Chamberlain Group v. Skylink Technologies	256
5.3.2.2.2 Broad Interpretation of Section (a)(2): MDY Industries, LLC v. Blizzard Entertainment	259
5.3.2.3 DMCA Section 1201(b)(1)	264
5.3.3 Section 1201 Penalties	267
5.3.4 Section 1201 Exemptions	267
5.3.5 The First Amendment and DMCA Section 1201	275
5.4 Economic Espionage Act	279
5.4.1 Origins of the EEA	279
5.4.2 Criminal Prohibitions on Economic Espionage and Theft of Trade Secrets	281
5.4.2.1 Definition of "Trade Secret"	282
5.4.2.2 "Knowing" Violations of the EEA	285
5.4.2.3 Purpose and Intent Required under Section 1831: Economic Espionage	285
5.4.2.4 Purpose and Intent Required under Section 1832: Theft of Trade Secrets	287
5.4.3 Civil Actions for Trade Secret Misappropriation: The Defend Trade Secrets Act of 2016	290

5.4.3.1 Definition of “Misappropriation” 290

5.4.3.2 Civil Seizures 294

5.4.3.3 Injunctions 294

5.4.3.4 Damages 295

5.4.3.5 Statute of Limitations 296

5.5 Budapest Convention on Cybercrime 296

6 U.S. Government Cyber Structure and Public– Private Cybersecurity Partnerships 299

6.1 U.S. Government’s Civilian Cybersecurity Organization 299

6.2 Department of Homeland Security Information Sharing under the Cybersecurity Act of 2015 303

6.3 Critical Infrastructure Executive Order and the NIST Cybersecurity Framework 307

6.4 U.S. Military Involvement in Cybersecurity and the Posse Comitatus Act 310

6.5 Vulnerabilities Equities Process 312

6.6 Executive Order 14028 315

6.6.1 Section 2: Removing Barriers to Sharing Threat Information 315

6.6.2 Section 3: Modernizing Federal Government Cybersecurity 316

6.6.3 Section 4: Enhancing Software Supply Chain Security 316

6.6.4 Section 5: Establishing a Cyber Safety Review Board 316

6.6.5 Section 6: Standardizing the Federal Government’s Playbook for Responding to Cybersecurity Vulnerabilities and Incidents 317

6.6.6 Section 7: Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks 317

6.6.7 Section 8: Improving the Federal Government’s Investigative and Remediation Capabilities 317

6.6.8 Section 9: National Security Systems 317

7 Surveillance and Cyber 319

7.1 Fourth Amendment 320

7.1.1 Was the Search or Seizure Conducted by a Government Entity or Government Agent? 321

7.1.2 Did the Search or Seizure Involve an Individual's Reasonable Expectation of Privacy? 326

7.1.3 Did the Government Have a Warrant? 336

7.1.4 If the Government Did Not Have a Warrant, Did an Exception to the Warrant Requirement Apply? 339

7.1.5 Was the Search or Seizure Reasonable Under the Totality of the Circumstances? 342

7.2 Electronic Communications Privacy Act 343

7.2.1 Stored Communications Act 344

7.2.1.1 Section 2701: Third-party Hacking of Stored Communications 349

7.2.1.2 Section 2702: Restrictions on Service Providers' Ability to Disclose Stored Communications and Records to the Government and Private Parties 350

7.2.1.3 Section 2703: Government's Ability to Require Service Providers to Turn Over Stored Communications and Customer Records 354

7.2.2 Wiretap Act 359

7.2.3 Pen Register Act 363

7.2.4 National Security Letters 364

7.3 Communications Assistance for Law Enforcement Act (CALEA) 366

7.4 Encryption and the All Writs Act 367

7.5 Encrypted Devices and the Fifth Amendment 369

8 Cybersecurity and Federal Government Contractors 375

8.1 Federal Information Security Management Act 376

8.2 NIST Information Security Controls for Government Agencies and Contractors 378

8.3 Classified Information Cybersecurity 382

8.4 Covered Defense Information, CUI, and the Cybersecurity Maturity Model Certification 383

9 Privacy Laws 391

9.1 Section 5 of the FTC Act and Privacy 392

9.2 Health Insurance Portability and Accountability Act 394

9.3 Gramm–Leach–Bliley Act and California Financial Information Privacy Act 396

9.4 CAN-SPAM Act 397

9.5 Video Privacy Protection Act 398

9.6 Children’s Online Privacy Protection Act 400

9.7 California Online Privacy Laws 402

9.7.1 California Online Privacy Protection Act (CalOPPA) 402

9.7.2 California Shine the Light Law 404

9.7.3 California Minor “Online Eraser” Law 406

9.8 California Consumer Privacy Act and Other State Privacy Laws 407

9.9 Illinois Biometric Information Privacy Act 410

9.10 NIST Privacy Framework 412

10 International Cybersecurity Law 415

10.1 European Union 416

10.2 Canada 426

10.3 China 431

10.4 Mexico 437

10.5 Japan 441

11 Cyber and the Law of War 445

11.1 Was the Cyberattack a “Use of Force” that Violates International Law? 447

11.2 If the Attack Was a Use of Force, Was that Force Attributable to a State? 450

11.3 Did the Use of Force Constitute an “Armed Attack” that Entitles the Target to Self-defense? 451

11.4 If the Use of Force Was an Armed Attack, What Types of Self-defense Are Justified? 453

11.5 If the Nation Experiences Hostile Cyber Actions that Fall Short of Use of Force or Armed Attacks, What Options Are Available? 455

12 Ransomware 459

12.1 Defining Ransomware 459

12.2 Ransomware- related Litigation 461

12.3 Insurance Coverage for Ransomware 469

12.4 Ransomware Payments and Sanctions 473

12.5 Ransomware Prevention and Response Guidelines from Government Agencies 474

12.5.1 Department of Homeland Security 474

12.5.2 Federal Trade Commission 476

12.5.3 Federal Interagency Guidance for Information Security Executives 477

12.5.4 New York Department of Financial Services Guidance 478

13 Internet of Things 479

13.1 State Internet of Things Laws 480

13.2 Internet of Things Cybersecurity Improvement Act of 2020 and NIST Guidance 481

13.3 NIST Consumer IoT Cybersecurity Labelling 482

13.4 FCC U.S. Cyber Trust Mark Program 483

13.5 FTC Internet of Things Security Guidance 484

13.6 Food and Drug Administration Cybersecurity Guidance 486

13.7 National Highway Traffic Safety Administration’s Cybersecurity Guidelines 488

13.8 Department of Homeland Security Internet Guidance 489

Appendix A: Text of Section 5 of the FTC Act 491

Appendix B: Summary of State Data Breach Notification Laws 501

Appendix C: Text of Section 1201 of the Digital Millennium Copyright Act 563

Appendix D: Text of the Computer Fraud and Abuse Act 575

Appendix E: Text of the Electronic Communications Privacy Act 583

Appendix F: Key Cybersecurity Court Opinions 647

Appendix G: Hacking Cybersecurity Law 795

Appendix H: Upgrading Cybersecurity Law 839

Index 873