

Cybersecurity Law

Second Edition

Jeff Kosseff

WILEY

Contents

	About the Author	<i>xv</i>
	Acknowledgment and Disclaimers	<i>xvii</i>
	Foreword to the Second Edition (2019)	<i>xix</i>
	Introduction to First Edition	<i>xxiii</i>
	About the Companion Website	<i>xxxi</i>
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	<i>Wyndham</i> : 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	17
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	19
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	22
1.1.6.1.5	Business-to-Business Providers Also Are Accountable to the FTC for Security of Sensitive Data	24
1.1.6.1.6	Companies Are Responsible for the Data Security Practices of Their Contractors	25
1.1.6.1.7	Make Sure that Every Employee Receives Regular Data Security Training for Processing Sensitive Data	26
1.1.6.1.8	Privacy Matters, Even in Data Security	26
1.1.6.1.9	Limit the Sensitive Information Provided to Third Parties	27
1.1.6.1.10	Children’s Data Requires Special Protection	27

1.1.6.2	Failure to Secure Payment Card Information	28
1.1.6.2.1	Adhere to Security Claims about Payment Card Data	28
1.1.6.2.2	Always Encrypt Payment Card Data	29
1.1.6.2.3	Payment Card Data Should Be Encrypted Both in Storage and at Rest	30
1.1.6.2.4	In-Store Purchases Pose Significant Cybersecurity Risks	31
1.1.6.2.5	Minimize Duration of Storage of Payment Card Data	33
1.1.6.2.6	Monitor Systems and Networks for Unauthorized Software	33
1.1.6.2.7	Apps Should Never Override Default App Store Security Settings	33
1.1.6.3	Failure to Adhere to Security Claims	34
1.1.6.3.1	Companies Must Address Commonly Known Security Vulnerabilities	34
1.1.6.3.2	Ensure that Security Controls Are Sufficient to Abide by Promises about Security and Privacy	35
1.1.6.3.3	Omissions about Key Security Flaws Also Can Be Misleading	38
1.1.6.3.4	Companies Must Abide by Promises for Security-Related Consent Choices	38
1.1.6.3.5	Companies that Promise Security Must Ensure Adequate Authentication Procedures	39
1.1.6.3.6	Adhere to Promises about Encryption	40
1.1.6.3.7	Promises About Security Extend to Vendors' Practices	41
1.1.6.3.8	Companies Cannot Hide Vulnerable Software in Products	41
1.2	State Data Breach Notification Laws	42
1.2.1	When Consumer Notifications Are Required	43
1.2.1.1	Definition of Personal Information	44
1.2.1.2	Encrypted Data	45
1.2.1.3	Risk of Harm	45
1.2.1.4	Safe Harbors and Exceptions to Notice Requirement	45
1.2.2	Notice to Individuals	46
1.2.2.1	Timing of Notice	46
1.2.2.2	Form of Notice	46
1.2.2.3	Content of Notice	47
1.2.3	Notice to Regulators and Consumer Reporting Agencies	47
1.2.4	Penalties for Violating State Breach Notification Laws	48
1.3	State Data Security Laws	48
1.3.1	Oregon	50
1.3.2	Rhode Island	51
1.3.3	Nevada	51
1.3.4	Massachusetts	52
1.3.5	Ohio	55
1.4	State Data Disposal Laws	56

2	Cybersecurity Litigation	57
2.1	Article III Standing	58
2.1.1	Applicable Supreme Court Rulings on Standing	59
2.1.2	Lower Court Rulings on Standing in Data Breach Cases	64
2.1.2.1	Injury-in-Fact	64
2.1.2.1.1	Broad View of Injury-in-Fact	64
2.1.2.1.2	Narrow View of Injury-in-Fact	68
2.1.2.2	Fairly Traceable	72
2.1.2.3	Redressability	72
2.2	Common Causes of Action Arising from Data Breaches	73
2.2.1	Negligence	74
2.2.1.1	Legal Duty and Breach of Duty	75
2.2.1.2	Cognizable Injury	76
2.2.1.3	Causation	79
2.2.2	Negligent Misrepresentation or Omission	80
2.2.3	Breach of Contract	82
2.2.4	Breach of Implied Warranty	88
2.2.5	Invasion of Privacy by Publication of Private Facts	92
2.2.6	Unjust Enrichment	93
2.2.7	State Consumer Protection Laws	95
2.3	Class Action Certification in Data Breach Litigation	97
2.4	Insurance Coverage for Cybersecurity Incidents	104
2.5	Protecting Cybersecurity Work Product and Communications from Discovery	108
2.5.1	Attorney-Client Privilege	110
2.5.2	Work Product Doctrine	112
2.5.3	Nontestifying Expert Privilege	115
2.5.4	<i>Genesco v. Visa</i>	116
2.5.5	<i>In re Experian Data Breach Litigation</i>	119
2.5.6	<i>In re Premera</i>	120
2.5.7	<i>In re United Shore Financial Services</i>	121
3	Cybersecurity Requirements for Specific Industries	123
3.1	Financial Institutions: Gramm-Leach-Bliley Act Safeguards Rule	124
3.1.1	Interagency Guidelines	124
3.1.2	Securities and Exchange Commission Regulation S-P	126
3.1.3	FTC Safeguards Rule	128
3.2	New York Department of Financial Services Cybersecurity Regulations	130
3.3	Financial Institutions and Creditors: Red Flags Rule	133
3.3.1	Financial Institutions or Creditors	136
3.3.2	Covered Accounts	137

3.3.3	Requirements for a Red Flag Identity Theft Prevention Program	138
3.4	Companies that Use Payment and Debit Cards: Payment Card Industry Data Security Standard (PCI DSS)	139
3.5	California Internet of Things Cybersecurity Law	141
3.6	Health Providers: Health Insurance Portability and Accountability Act (HIPAA) Security Rule	142
3.7	Electric Transmission: Federal Energy Regulatory Commission Critical Infrastructure Protection Reliability Standards	147
3.7.1	CIP-003-6: Cybersecurity—Security Management Controls	148
3.7.2	CIP-004-6: Personnel and Training	148
3.7.3	CIP-006-6: Physical Security of Cyber Systems	149
3.7.4	CIP-007-6: Systems Security Management	149
3.7.5	CIP-009-6: Recovery Plans for Cyber Systems	149
3.7.6	CIP-010-2: Configuration Change Management and Vulnerability Assessments	150
3.7.7	CIP-011-2: Information Protection	150
3.8	Nuclear Regulatory Commission Cybersecurity Regulations	150
3.9	South Carolina Insurance Cybersecurity Law	151
4	Cybersecurity and Corporate Governance	155
4.1	Securities and Exchange Commission Cybersecurity Expectations for Publicly Traded Companies	156
4.1.1	10-K Disclosures: Risk Factors	158
4.1.2	10-K Disclosures: Management’s Discussion and Analysis of Financial Condition and Results of Operations (MD&A)	159
4.1.3	10-K Disclosures: Description of Business	160
4.1.4	10-K Disclosures: Legal Proceedings	160
4.1.5	10-K Disclosures: Financial Statements	161
4.1.6	10K Disclosures: Board Oversight of Cybersecurity	161
4.1.7	Disclosing Data Breaches to Investors	161
4.1.8	Yahoo Data Breach	164
4.1.9	Cybersecurity and Insider Trading	165
4.2	Fiduciary Duty to Shareholders and Derivative Lawsuits Arising from Data Breaches	166
4.3	Committee on Foreign Investment in the United States and Cybersecurity	168
5	Anti-Hacking Laws	171
5.1	Computer Fraud and Abuse Act	172
5.1.1	Origins of the CFAA	172

5.1.2	Access Without Authorization and Exceeding Authorized Access	173
5.1.2.1	Narrow View of “Exceeds Authorized Access” and “Without Authorization”	176
5.1.2.2	Broader View of “Exceeds Authorized Access” and “Without Authorization”	181
5.1.2.3	Attempts to Find a Middle Ground	183
5.1.3	The Seven Sections of the CFAA	184
5.1.3.1	CFAA Section (a)(1): Hacking to Commit Espionage	186
5.1.3.2	CFAA Section (a)(2): Hacking to Obtain Information	187
5.1.3.3	CFAA Section (a)(3): Hacking a Federal Government Computer	191
5.1.3.4	CFAA Section (a)(4): Hacking to Commit Fraud	192
5.1.3.5	CFAA Section (a)(5): Hacking to Damage a Computer	195
5.1.3.5.1	CFAA Section (a)(5)(A): Knowing Transmission that Intentionally Damages a Computer Without Authorization	195
5.1.3.5.2	CFAA Section (a)(5)(B): Intentional Access Without Authorization that Recklessly Causes Damage	198
5.1.3.5.3	CFAA Section (a)(5)(C): Intentional Access Without Authorization that Causes Damage and Loss	200
5.1.3.5.4	CFAA Section (a)(5): Requirements for Felony and Misdemeanor Cases	200
5.1.3.6	CFAA Section (a)(6): Trafficking in Passwords	203
5.1.3.7	CFAA Section (a)(7): Threatening to Damage or Obtain Information from a Computer	205
5.1.4	Civil Actions Under the CFAA	208
5.1.5	Criticisms of the CFAA	212
5.1.6	CFAA and Coordinated Vulnerability Disclosure Programs	214
5.2	State Computer Hacking Laws	218
5.3	Section 1201 of the Digital Millennium Copyright Act	220
5.3.1	Origins of Section 1201 of the DMCA	221
5.3.2	Three Key Provisions of Section 1201 of the DMCA	222
5.3.2.1	DMCA Section 1201(a)(1)	222
5.3.2.2	DMCA Section 1201(a)(2)	227
5.3.2.2.1	Narrow Interpretation of Section (a)(2): <i>Chamberlain Group v. Skylink Technologies</i>	228
5.3.2.2.2	Broad Interpretation of Section (a)(2): <i>MDY Industries, LLC v. Blizzard Entertainment</i>	231
5.3.2.3	DMCA Section 1201(b)(1)	236
5.3.3	Section 1201 Penalties	238
5.3.4	Section 1201 Exemptions	239
5.3.5	The First Amendment and DMCA Section 1201	246
5.4	Economic Espionage Act	250

5.4.1	Origins of the Economic Espionage Act	250
5.4.2	Criminal Prohibitions on Economic Espionage and Theft of Trade Secrets	251
5.4.2.1	Definition of “Trade Secret”	252
5.4.2.2	“Knowing” Violations of the Economic Espionage Act	255
5.4.2.3	Purpose and Intent Required under Section 1831: Economic Espionage	255
5.4.2.4	Purpose and Intent Required under Section 1832: Theft of Trade Secrets	257
5.4.3	Civil Actions for Trade Secret Misappropriation: The Defend Trade Secrets Act of 2016	260
5.4.3.1	Definition of “Misappropriation”	261
5.4.3.2	Civil Seizures	263
5.4.3.3	Injunctions	264
5.4.3.4	Damages	265
5.4.3.5	Statute of Limitations	265
5.5	Budapest Convention on Cybercrime	266
6	U.S. Government Cyber Structure and Public–Private Cybersecurity Partnerships	269
6.1	U.S. Government’s Civilian Cybersecurity Organization	269
6.2	Department of Homeland Security Information Sharing under the Cybersecurity Act of 2015	272
6.3	Critical Infrastructure Executive Order and the National Institute of Standards and Technology’s Cybersecurity Framework	276
6.4	U.S. Military Involvement in Cybersecurity and the Posse Comitatus Act	284
6.5	Vulnerabilities Equities Process	286
7	Surveillance and Cyber	291
7.1	Fourth Amendment	292
7.1.1	Was the Search or Seizure Conducted by a Government Entity or Government Agent?	293
7.1.2	Did the Search or Seizure Involve an Individual’s Reasonable Expectation of Privacy?	297
7.1.3	Did the Government Have a Warrant?	305
7.1.4	If the Government Did Not Have a Warrant, Did an Exception to the Warrant Requirement Apply?	308
7.1.5	Was the Search or Seizure Reasonable Under the Totality of the Circumstances?	310
7.2	Electronic Communications Privacy Act	311
7.2.1	Stored Communications Act	313

7.2.1.1	Section 2701: Third-Party Hacking of Stored Communications	317
7.2.1.2	Section 2702: Restrictions on Service Providers' Ability to Disclose Stored Communications and Records to the Government and Private Parties	318
7.2.1.3	Section 2703: Government's Ability to Require Service Providers to Turn Over Stored Communications and Customer Records	324
7.2.2	Wiretap Act	328
7.2.3	Pen Register Act	332
7.2.4	National Security Letters	334
7.3	Communications Assistance for Law Enforcement Act (CALEA)	335
7.4	Encryption and the All Writs Act	336
7.5	Encrypted Devices and the Fifth Amendment	339
8	Cybersecurity and Federal Government Contractors	343
8.1	Federal Information Security Management Act	344
8.2	NIST Information Security Controls for Government Agencies and Contractors	346
8.3	Classified Information Cybersecurity	350
8.4	Covered Defense Information and Controlled Unclassified Information	353
9	Privacy Laws	361
9.1	Section 5 of the FTC Act and Privacy	362
9.2	Health Insurance Portability and Accountability Act	366
9.3	Gramm-Leach-Bliley Act and California Financial Information Privacy Act	368
9.4	CAN-SPAM Act	369
9.5	Video Privacy Protection Act	371
9.6	Children's Online Privacy Protection Act	372
9.7	California Online Privacy Laws	375
9.7.1	California Online Privacy Protection Act (CalOPPA)	375
9.7.2	California Shine the Light Law	376
9.7.3	California Minor "Eraser Law"	378
9.8	California Consumer Privacy Act	380
9.9	Illinois Biometric Information Privacy Act	382
10	International Cybersecurity Law	385
10.1	European Union	386
10.2	Canada	396
10.3	China	400

- 10.4 Mexico 405
- 10.5 Japan 409

- 11 Cyber and the Law of War 413**
- 11.1 Was the Cyberattack a “Use of Force” that Violates International Law? 414
- 11.2 If the Attack Was a Use of Force, Was that Force Attributable to a State? 417
- 11.3 Did the Use of Force Constitute an “Armed Attack” that Entitles the Target to Self-Defense? 418
- 11.4 If the Use of Force Was an Armed Attack, What Types of Self-Defense Are Justified? 420
- 11.5 If the Nation Experiences Hostile Cyber Actions that Fall Short of Use of Force or Armed Attacks, What Options Are Available? 422

Appendix A: Text of Section 5 of the FTC Act 425

Appendix B: Summary of State Data Breach Notification Laws 433

Appendix C: Text of Section 1201 of the Digital Millennium Copyright Act 493

Appendix D: Text of the Computer Fraud and Abuse Act 505

Appendix E: Text of the Electronic Communications Privacy Act 513

Appendix F: Key Cybersecurity Court Opinions 579

Index 715