
CONTENTS

<i>Preface: Plan and Purpose of the Book</i>	xxiii
A Caselaw Approach	xxiii
A Distinctive Set of Cybersecurity Issues	xxiii
Who Is This Book For?	xxiv
The Technology Notes	xxiv
Why We Include In-Depth Examination of the Computer Fraud and Abuse Act	xxiv
Why We Include the Fourth and Fifth Amendments	xxv
<i>Acknowledgments</i>	xxvi

PART I

INTRODUCTION AND PRELIMINARY MATTERS 1

CHAPTER 1

Basics: Key Terms, CyberSecurity, Risk Assessment, and Insurance	3
A. Disparate Views About What a Computer Is	3
1. Some Legal Definitions	3
<i>Riley v. California</i>	4
Questions	5
2. A Computer Science Perspective	6
Questions	9
B. Disparate Views About What a Network Is	10
1. Some legal Definitions	10
Question	11
2. A Computer Science Perspective	11
Question	12
C. Disparate Views About What Constitutes Accessing a Computer or Network	12
1. Some Legal Definitions	13
<i>United States v. Drew</i>	13
Note: After <i>Drew</i>	14
2. A Computer Science Perspective	14
Technology Note: Access Control Systems	15

D. The Fundamentals of Attacking And Defending Computers and Networks	15
1. The CIA Triad	15
2. Software Vulnerabilities	16
3. Security Management Vulnerabilities	17
4. Human Vulnerabilities	17
5. Exploiting Vulnerabilities	17
E. Defending Computers and Networks: A Tale of Doors, Guards, and Authentication	18
1. Eliminating Doors	18
2. Locking Doors	19
3. Multiplying Doors	19
4. Posting Guards	20
5. Authentication	20
F. Risk Assessment	21
1. Risk Assessment and the Language of Litigation	24
G. Cyber Insurance	25
<i>Landry's, Incorporated v. The Insurance Company of The State of Pennsylvania</i>	26
Note: Applying Terms in the Internet Context	31

PART II

LIABILITY FOR FAILURE TO PREVENT ACCESS TO A COMPUTER OR NETWORK	33
---	-----------

CHAPTER 2

Liability in Tort	35
A. Liability Based on Negligence	35
1. Liability for Failing to Safeguard Data: The Landlord/Tenant Analogy	35
<i>Kline v. 1500 Massachusetts Avenue Apartment Corporation</i>	36
Technology Note: Physical Security	40
Note: Summary of the Majority's Argument	41
Questions	42
Note: Jury Reception of Cost/Benefit Analysis	44
<i>Dittman v. UPMC</i>	44
Technology Note: Security Devices and Techniques	52
Questions	54
Note: Criminal Acts of Third Parties	57
<i>In Re: Blackbaud, Inc., Customer Data Breach Litigation</i>	57
Technology Note: Incident Response	63
Question	63

2. Limits on the Extent of Liability: The Economic Loss Rule	64
<i>Dittman v. UPMC</i>	64
Question	69
Note: The Independent Duty Exception	70
<i>In re Target Corporation Customer Data Security Breach Litigation</i>	71
Technology Note: The Target Breach Story	77
Note: An Exception to the Economic Loss Rule for Intentional Misrepresentation	79
<i>In re TJX Companies Retail Security Breach Litigation</i>	80
Technology Note: TJX Security Flaws	83
Questions	84
B. Liability Based on Breach of Confidence	84
<i>In re Capital One Consumer Data Security Breach Litigation</i>	85
Technology Note: Server-Side Request Forgery	88
Note: Breach of Confidence Versus Public Disclosure of Private Facts	89
Questions	89
<i>Warren v. DSG Retail</i>	91
Questions	95
 CHAPTER 3	
Liability Based on Breach of Contract or Equity	99
A. Liability Based on Breach of Contract	99
1. Privacy Policies as Offers	99
<i>In re Capital One Consumer Data Security Breach Litigation</i>	99
Note: Conditions for Making an Offer	103
Questions	104
2. Implied Contracts	105
<i>In re Michaels Stores Pin Pad Litigation</i>	105
Technology Note: Skimming	108
Note: The Implied Contract in <i>Michaels Stores</i>	108
Questions	109
3. Damages for Breach of Contract	109
<i>Hendricks v. DSW Shoe Warehouse</i>	110
Technology Note: DSW's Security Problems	113
Questions	114
4. Waivers and Limitations of Damages	115
<i>In re: Heartland Payment Systems, Inc. Customer Data Security Breach Litigation</i>	115
Note: What Are Consequential Damages?	118
5. Waivers and Limitations as Contractual Risk Management	119
<i>In re Yahoo! Inc Customer Data Breach Litigation</i>	119
Note: Unconscionability Doctrine	126

Question	127
Note: The <i>In Re Yahoo!</i> Settlement	127
B. Liability Based on Equity: Unjust Enrichment	127
<i>In re Target Corporation Customer Data Security Breach Litigation</i>	128
Questions	130
Note	131
<i>In re Rutter's Inc. Data Security Breach Litigation</i>	131
Note: Deference to Thin Claims	136
Questions	136
CHAPTER 4	
Compliance Liability Imposed by Agency Action or Statute	139
A. Liability Imposed by Agency Action	139
1. Action by the Federal Trade Commission	139
<i>Federal Trade Commission v. Wyndham Worldwide Corporation</i>	141
Technology Note: Wyndham's Poor Security	154
Questions	156
Note: Wyndham Ultimately Agreed to a Comprehensive Security Program	157
<i>LabMD v. Federal Trade Commission</i>	158
Note: The Specificity Requirement	166
Questions	167
a. Cybersecurity Implications from a Privacy Case	168
<i>Federal Trade Commission v. Kochava, Inc.</i>	168
Note: The "Likely to Cause Harm" Issue	177
Questions	178
Note: The FTC's Amended Complaint	178
2. Action by the Federal Communications Commission	178
<i>Huawei Technologies USA v. Federal Communications Commission</i>	179
Note: The FCC's Authority	183
Question	183
Technology Note: Autonomous Systems and the Border Gateway Protocol	183
<i>In the Matter of Secure Internet Routing</i>	184
Question	188
3. Action by the Cybersecurity and Infrastructure Security Agency	188
Question	189
4. Action by the Securities and Exchange Commission	189
The SEC Safeguards Rule	189
a. The SEC's Investigative Powers	190
<i>Securities and Exchange Commission v. Covington & Burling</i>	190

Technology Note: Hafnium Cyberattack	200
Question	200
b. The Cybersecurity Role of SEC Disclosure Requirements	201
c. The SEC Action against R.R. Donnelley & Sons Co.	202
<i>In the Matter of R.R. Donnelley & Sons Co.</i>	202
Questions	204
Note: A Procedural Point	204
B. Liability Imposed by Statute	205
1. Health Insurance Portability and Accountability Security Rule	205
45 CFR §164.306—Security Standards: General Rules	206
a. HIPPA Violations as Evidence of Unreasonableness or Breach of Confidence	207
<i>Emily Byrne v. Avery Center for Obstetrics and Gynecology</i>	207
Questions	214
Note: How Broad is the <i>Byrne</i> Holding	214
2. Gramm-Leach-Bliley Act Safeguards Rule	215
16 CFR §314—Standards for Safeguarding Customer Information	215
§314.1 Purpose and Scope	215
§314.3—Standards for Safeguarding Customer Information	216
§314.4 Elements	216
a. No Private Right of Action	220
<i>Wells Fargo Bank v. Jenkins</i>	220
Question	222
3. Liability Imposed by State Statute	222
a. California’s Consumer Privacy Protection Act: Security Requirements	223
b. Data Breach Notification Statutes	224
 CHAPTER 5	
Liability Based on Defensive Measures	227
A. Liability For Wrongfully Preventing Access	227
1. Liability for Intentional Interference with Contract	227
<i>hiQ Labs v. LinkedIn</i>	228
Questions	235
a. The Legitimate Business Purpose Defense	236
<i>Zango, Inc. v. PC Tools Pty Ltd.</i>	236
Questions	241
Note: Is There a Contractual Solution?	242
2. Immunity under the Communications Decency Act	243
<i>Zango Inc. v. Kaspersky Lab</i>	243
Question	252
B. Wrongfully Monitoring Access: The Wiretap Act	252
1. A Private Right of Action	253
<i>Luis v. Zang</i>	253

Note: Does Outsourcing Cybersecurity Violate the Wiretap Act?	273
2. When Is a Person a Party to a Communication?	273
PART III	
CIVIL LIABILITY AND CRIMINAL RESPONSIBILITY FOR ACCESSING A COMPUTER OR NETWORK	275
<hr/>	
CHAPTER 6	
Civil Liability for Accessing a Computer or Network	277
A. Trespass to Chattels	277
<i>eBay v. Bidder's Edge</i>	278
Technology Note: Computing Power, Robot Exclusion Protocol, Proxy Servers	287
Note: The Breadth of the <i>eBay</i> Right to Exclude	288
Questions	288
Note: Internet-Connectedness as a Crucial Difference	288
<i>Intel v. Hamidi</i>	289
Questions	297
Note: Differing Views on Damage	298
<i>Sotelo v. Direct Revenue</i>	299
Technology Note: Spyware and Adware	303
Question	304
Note: Other Sources of Liability	305
B. Electronic Communications Privacy Act	305
<i>In re Google Inc. Cookie Placement Consumer Privacy Litigation</i>	305
Note: One or Two Parties?	320
Technology Note: Browser Communication with the Web	321
Questions	323
C. State Law	324
Statutes Chapter 720. Criminal Offenses §5/17-51. Computer Tampering	324
CHAPTER 7	
The Computer Fraud and Abuse Act: Criminal Responsibility and Civil Liability	327
A. History of the Computer Fraud and Abuse Act	327
B. The Scope of the CFAA	328
1. Protected Computer: The Extreme Limit of Legislative Jurisdiction	328
<i>United States v. Trotter</i>	329
Questions	332

2. Access from Outside the United States	332
<i>United States v. Ivanov</i>	333
Note: Obstacles to Extraterritorial Enforcement	337
C. Consequences of Hybridization	338
<i>WEC Carolina Energy Solutions LLC v. Willie Miller</i>	338
Note: The Specter of Parallel Criminal and Civil Actions	344
D. The Trespassory Nature of CFAA Offenses	344
E. Judging the Utility of the CFAA	347

CHAPTER 8

The Elements of Discontent: The Key Terms “Without Authorization” and “Exceeds Authorization”

A. Without Authorization	352
<i>Facebook v. Power Ventures</i>	354
Note: Registration as a Third-Party Developer	360
Questions	360
1. <i>hiQ v. LinkedIn</i> and the Significance of Public Accessibility	360
<i>hiQ Labs v. LinkedIn</i>	361
Technology Note: Web Scraping	374
Note: Limiting the Effectiveness of Cease-and-Desist Letters	375
Questions	376
Note: A Victory for hiQ?	377
B. Exceeding Authorization	378
<i>Cloudpath Networks, Inc. v. SecureW2 B.V.</i>	379
Note: An End to the Lower Court Fireworks	394
<i>Van Buren v. United States</i>	394
Technology Note: <i>Van Buren’s</i> Notion of “Areas of a Computer”	414
Question	414

CHAPTER 9

The *Mens Rea* Elements and Their Application

A. The <i>Mens Rea</i> Elements	417
1. Recklessly	417
2. Knowingly	418
a. What It Means to Act Knowingly or With Knowledge	418
b. Determining the Elements to Which “Knowingly” Applies	418
<i>United States v. Morris</i>	419
Technology Note: The Morris Worm	426
Question	427
3. Willfully	428
<i>United States v. George</i>	429
Note: What Does Willfulness Require?	439

4. Intent	440
<i>United States v. Prugar</i>	440
Technology Note: What Prugar Did	446
5. Intent to Defraud	447
a. Legislative History and the Applicability of Mens Rea	448
<i>Arthur Andersen, LLP v. United States</i>	448
 CHAPTER 10	
Other Terms Used in the Offenses	457
A. Computer	457
1. Protected Computer	458
B. Loss and Damage	458
<i>Frisco Medical Center, L.L.P. v. Bledsoe</i>	458
Technology Note: Integrity or Confidentiality?	469
Question	470
C. Information	470
<i>Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.</i>	471
D. Obtaining Information	473
<i>Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey</i>	473
Technology Note: The robots.txt File	478
Note: Obtaining Information	479
Questions	479
E. Financial institution	480
F. Department of the United States	480
G. Agency	480
 CHAPTER 11	
The Computer Fraud and Abuse Act Offenses	483
A. The Choate Offenses	483
1. Section 1030(a)(1): Accessing a Computer and Obtaining National Security Information	483
2. Section 1030(a)(2): Accessing a Computer and Obtaining Information	484
<i>United States v. Willis</i>	485
Note: The Broad Reach of §1030(a)(2)(C)	489
Question	489
3. Aggravating Factors	490
<i>United States v. Cross</i>	490
Note: Just Statutes or Common Law Torts Also?	493
<i>United States v. Powers</i>	493
Note: Valuation of Information	496
4. Section 1030(a)(3): Accessing a Nonpublic Computer of a Department or Agency of the United States	496

5. Section 1030(a)(4): Accessing a Computer to Defraud and Obtain Value	497
<i>United States v. Czubinski</i>	498
Questions	503
<i>In re America Online, Inc.</i>	504
6. Section 1030(a)(5): Damaging a Computer or Computer Information	507
<i>United States v. Prugar</i>	508
Note: The Dictionary Definition of “Transmit”	511
<i>International Airport Centers, L.L.C. v. Citrin</i>	511
Questions	513
Note: Misdemeanors and Felonies	513
<i>United States v. Sablan</i>	514
Note: The Current Structure of 1030(a)(5)	517
7. Section 1030(a)(6): Trafficking in Passwords	518
<i>AtPac, Inc. v. Aptitude Solutions, Inc.</i>	519
Note: Violation of a License Agreement	523
Questions	524
<i>State Analysis, Inc. v. American Financial Services Associates</i>	524
Note: The Meaning of the Term “Password”	527
8. Section 1030(a)(7): Threatening to Damage a Computer	527
<i>United States v. Zhou</i>	528
B. The Inchoate Offenses	533
1. Section 1030(b)	533
a. Conspiracy	533
<i>United States v. Escobar de Bright</i>	534
b. Attempt	538
<i>United States v. Doyon</i>	538
C. State Statutes: Choate and Inchoate Offenses	543
Statutes Chapter 720. Criminal Offenses §17-51.	
Computer Tampering.	543

PART IV

RIGHTS PROTECTING DATA FROM SEIZURE BY THE GOVERNMENT

547

CHAPTER 12

Protection of Digital Data from the Government—When the Fourth Amendment Provides Protection

549

A. What Constitutes a Fourth Amendment Search	550
1. The Property-Based Approach	550
<i>United States v. Jones</i>	551
Questions	565

2. Reasonable Expectations of Privacy	565
a. When a Reasonable Expectation of Privacy Exists	565
<i>Katz v. United States</i>	566
Note: The Untold Story	571
Questions	572
Note: Congressional Action After <i>Katz</i>	573
b. The Third-Party Doctrine	573
<i>Hoffa v. United States</i>	574
Note: The Role of Confidential Informants	578
Questions	579
Note: Access to Bank and Business Records	580
<i>Smith v. Maryland</i>	581
Technology Note: Pen Registers	589
Questions	589
Note: <i>Klayman v. Obama</i>	590
Technology Note: NSA Bulk Telephony Metadata Collection	591
<i>Carpenter v. United States</i>	592
Questions	602
Note: Difficulties With Modifying or Abandoning the Third-Party Doctrine	603
B. The Territorial Reach of the Fourth Amendment	604
1. The Territorial Reach of the Fourth Amendment to Extra Territorially Stored Data and Originated Communications	604
a. The Fourth Amendment and Searches of Property Outside the United States of Persons with No Connection to the United States	604
<i>United States v. Verdugo-Urquidez</i>	605
b. The Fourth Amendment and Searches of Communications Originating from Outside the United States and the Incidental Overhear Problem	614
2. The Territorial Reach of the Fourth Amendment to Searches of U.S. Citizens' Property and Communications Conducted Outside the United States	615
<i>United States v. Hasbajrami</i>	615
 CHAPTER 13	
The Fourth Amendment Warrant and Reasonableness Requirements	625
A. Fourth Amendment Requirements for Obtaining Search Warrants	625
1. Fourth Amendment Requirements for Searches for Physical Objects	626
Note: The Fourth Amendment and Subpoenas	628
2. The Application of the Fourth Amendment in Relation to Searches of Digital Data	628
a. Searches of Electronic Storage Devices	629

i. Orders Compelling the Use of Biometric Encryption	629
<i>In re Search Warrant No. 5165</i>	630
Note: Content of Search Warrants	637
b. Searches of Internet Service Providers	637
i. The Requirement of Probable Cause	637
<i>Carpenter v. United States</i>	637
Note: Cell-Site Location Information and Stored Communication Act Warrants	640
Question	641
Note: A Typical Example of Probable Cause	642
c. <i>Ex Ante</i> Restrictions on How Government Conducts Searches of Internet Service Providers	642
<i>In the Matter of a Warrant for All Content and Other Information Associated with the Email Account xxxxxxxx @ gmail.com Maintained at Premises Controlled by Google Inc.</i>	643
Question	656
Note: Overbreadth and Particularity	656
<i>In re Search of Information Associated with [Redacted]@mac .com Stored at Premises Controlled by Apple, Inc.</i>	658
Question	662
<i>United States v. Liburd</i>	663
Note: A Two-Step Process to Avoid Overbreadth	666
<i>United States v. Beard</i>	666
Note: Additional Criticisms of Service Provider Review	669
B. Fourth Amendment Reasonableness for Conducting Searches of Digital Data	669
1. Geofencing and the Fourth Amendment	670
<i>Matter of Search Warrant for Geofence Location Data Stored at Google Concerning an Arson Investigation</i>	671
Question	687
Note: The Practice of Seeking Warrants	688
 CHAPTER 14	
Fifth Amendment Basic Doctrine and Compelled Use of Methods to Access Data	695
A. The Nature and Scope of the Privilege Against Self-Incrimination	695
<i>Doe v. United States</i>	695
Note: Testimonial Acts and Communicative Content	704
Questions	705
Note: Encryption Keys, Passwords, and Biometrics	705
B. Orders Compelling the Use of Encryption Keys	706
<i>In re Subpoena Duces Tecum</i>	706
Note: Two Ways to Not Be Testimonial	713

Question	714
Note: Decrypted Contents and Passwords	714
C. Orders Compelling the Use of Passwords	714
<i>People v. Sneed</i>	714
Questions	730
D. Orders Compelling the Use of Biometrics	731
<i>In the Matter of the Search Warrant Application for</i> <i>[Redacted Text]</i>	732
Questions	738
<i>In re Search Warrant No. 5165</i>	739
Note	748
Question	749
<i>Technical Terms Glossary</i>	751
<i>Table of Cases</i>	757
<i>Index</i>	771