Contents

Foreword xv
Michael Chertoff

Preface xix

Reflections on the Internet of Things xxiii
Senator Mark Warner

About the Editors xxix

About the Authors xxxiii

PART I
New and Emerging IoT Technologies 1

Chapter 1
Connected Cars: Impact on Cars and Other Intelligent Transportation Systems 3
Stephen S. Wu

I. Introduction 3
II. Overview 5
III. Overview of Connected Transportation Technology 8
IV. Regulation and Governance of Connected Transportation Systems 10
   A. Backdrop of Regulating and Governing Driving Practices and Motor Vehicle Safety 10
   B. Regulating Communications with and among Vehicles 11
   C. Truck Platooning Legislation 12
   D. Marketing Oversight 13
V. Liability Issues 13
   A. Types of Claims 17
   B. Potential Defenses 19
   C. Risk Management and Insurance 21
VI. Data Protection 22
VII. Transactions Involving Connected Transportation Technology 30  
VIII. Conclusion 34

**Chapter 2**  
**Health IoT: Trends and Legal Issues** 35  
*Jodi G. Daniel, Ashley N. Southerland, Maya Uppaluru*

I. Introduction and Scope 35  
A. Types of Connected Health Devices 37  
II. Real-World Operational Challenges 41  
III. Integration and Interoperability: Increasing the Flow of Patient Information 42  
A. Interoperability 43  
B. Standards and Certification 45  
C. Information Blocking 47  
IV. Privacy and Security and Data Use: Protecting Patients’ Health Data to Engender Patient Trust 48  
A. Health Insurance Portability and Accountability Act of 1996 (HIPAA) 48  
B. Other Laws Affecting the Privacy of Health Data 53  
C. Other Privacy and Security Resources 53  
V. Safety: Ensuring Appropriate, Responsible, and Quality-Based Use of Health IoT 54  
A. FDA and Connected Health Devices 54  
VI. Legal Uncertainty: Managing Risk and Compliance in a Changing Environment 58  
A. Liability and Risk Mitigation 58  
B. Compliance and Enforcement 60  
VII. Making Sense of It All: Recommendations for Navigating the Future of the Health Care IoT Landscape 62

**Chapter 3**  
**Drones: Taking the IoT into the Air** 67  
*Matthew Henshon*

I. Introduction 67  
II. Development of Drones 68  
A. Early Military “Drones” 68
Contents

B. Modern Military Drones 69
C. Expansion of the Civilian Market 70

III. The Current State of UAV Regulation 77
   A. FAA Modernization and Reform Act of 2012 77
   B. Section 333 and COAs 80
   C. Part 107 Regulations 82
   D. Possible Future Regulation and the “IoT Drone” 85
   E. Underwater Drones 89

IV. Privacy’s Future Up in the Air: UAVs and Aerial Surveillance 90

V. Conclusion 94

Chapter 4

5G Wireless Communications: Enabling a New Internet of Things 95

Thomas L. Jarvis
J.C. Masullo

I. Architecture of the IoT 96
II. Communications Networks 96
   A. History of Wireless Cellular Networks 97
   B. Primary Components of Wireless Cellular Networks 100

III. 5G Networks: The Specification Timeline 101
IV. 5G Applications and Performance Objectives 102
V. The Technology Behind the Performance 105
   A. 5G New Radio 105
   B. 5G Core Network 109

VI. Next Generation IoT Application Powered by 5G 111
VII. Convergence of Technology, Divergence of Ownership Claims, Legal Solutions 114
   A. Wireless Standards and Licensing Obligations 115
   B. Ownership Claims 118
   C. Legal Solutions 119

VIII. Conclusion 124

Chapter 5

Blockchain and the Internet of Things 127

Jay Johnson
Mark Rasmussen
Kerianne Tobitsch

I. Introduction to Blockchain Applications in the IoT 127
Contents

II. Consequences of Blockchain-Based IoT Platforms 131
   A. Cybersecurity 132
   B. IoT Device Communications 133

III. Potential Legal Issues Raised by Applying Blockchain Technologies to the IoT 134
   A. Jurisdiction and Dispute Resolution 134
   B. Privacy Concerns 136
   C. Contract Issues 139
   D. Liability 141

IV. Conclusion 143

PART II

The State (or Lack Thereof) of IoT Laws and Regulations 145

Chapter 6

U.S. Regulatory Framework for IoT 147

Laura Kim
Jennifer Johnson

I. Product Safety Regulations 148
   A. CPSC 148
   B. DOT and NHTSA 151
   C. FDA 152

II. Privacy and Cybersecurity Regulation 158
   A. The Federal Trade Commission 159
   B. FDA’s Approach to Cybersecurity of Medical Devices 166
   C. Cybersecurity and Government Procurement 168

III. IoT Connectivity and Spectrum Regulations 173

IV. Banking 177

V. The Electricity Grid 179

VI. Federal Aviation Administration Regulation of Drones 181

VII. State Level Regulatory Trends 185
   A. Connected and Automated Vehicles 185
   B. Privacy 188

Chapter 7

IoT International Regulatory Challenges: The European Approach 191

Aida Joaquin Acosta

I. IoT Is a Complex Technology 191
Contents

II. The Importance of a Clear and Flexible Regulatory Framework for IoT 192
III. The Shared Challenges of Building an Adequate Regulatory Framework for IoT 193
IV. The EU Approach to the Legal Challenges of IoT: Privacy, Security, Safety, and Liability 195
   A. The EU IoT Policy Objectives 195
   B. The EU Regulatory Efforts on Privacy, Security, Safety, and Liability 198
   C. Privacy and Security 199
   D. Safety and Liability 207
   E. Other Issues: Ethics 212
V. Recommendations and Concluding Remarks 214

PART III
IoT Risks and Potential Solutions 217

Chapter 8
Privacy and the IoT: Consumer Rights and Emerging Legal Issues 219

Mauricio Paez
Cynthia Cwik
Kerianne Tobitsch

I. Introduction 219
II. Constitutional Right to Privacy under the Fourth Amendment 221
III. Statutory Privacy Rights 224
   A. Consumer Privacy 224
   B. Special Privacy Issues 228
IV. IoT Privacy Litigation 235
   A. Potential Statutory Claims Related to the IoT 238
   B. Potential Common Law Claims Related to IoT Privacy 245
V. Conclusion 250

Chapter 9
(In)security of the Internet of Things (IoT): A Roadmap for Assessing the Risks 253

Lucy L. Thomson
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Widespread IoT Cybersecurity Risks Create</td>
<td>254</td>
</tr>
<tr>
<td>Daunting Challenges</td>
<td></td>
</tr>
<tr>
<td>II. The Need for Risk-Based Assessment</td>
<td>258</td>
</tr>
<tr>
<td>III. Changing Nature of the Global Threat</td>
<td>259</td>
</tr>
<tr>
<td>IV. Risks to Confidentiality, Integrity, and Availability</td>
<td>261</td>
</tr>
<tr>
<td>V. The Current State of IoT Security—</td>
<td></td>
</tr>
<tr>
<td>The Complex Technology Infrastructure</td>
<td>264</td>
</tr>
<tr>
<td>B. Types of Attacks Involving IoT Devices</td>
<td>274</td>
</tr>
<tr>
<td>VI. The Path Forward: The Security Strategy for Executives, Corporate Boards, and Government Officials Includes Risk-Based Assessment</td>
<td>284</td>
</tr>
<tr>
<td>A. Comprehensive Information Security Program</td>
<td>285</td>
</tr>
<tr>
<td>B. IoT Risk Assessment</td>
<td>286</td>
</tr>
<tr>
<td>C. Implementing Technology and IoT Devices with Known Vulnerabilities Is Not “Reasonable Security”</td>
<td>292</td>
</tr>
<tr>
<td>D. Strengthening Security</td>
<td>293</td>
</tr>
<tr>
<td>E. OWASP Principles of IoT Security</td>
<td>296</td>
</tr>
</tbody>
</table>

**Chapter 10**

### Incentives to Address Homeland Security Risks with IoT Technology

*Adam Isles*

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Security Risks</td>
<td>302</td>
</tr>
<tr>
<td>A. Lack of Incentives</td>
<td>308</td>
</tr>
<tr>
<td>II. Leveraging Homeland Security Procurement Authorities</td>
<td>309</td>
</tr>
<tr>
<td>III. Leveraging Homeland Security Grants and Related</td>
<td>314</td>
</tr>
<tr>
<td>Guidance to State and Local Authorities and Critical</td>
<td></td>
</tr>
<tr>
<td>Infrastructure Operators</td>
<td></td>
</tr>
<tr>
<td>IV. Leveraging Existing Federal Authorities to Assess</td>
<td>315</td>
</tr>
<tr>
<td>and Regulate Critical Infrastructure</td>
<td></td>
</tr>
<tr>
<td>A. Non-DHS Regulations</td>
<td>318</td>
</tr>
<tr>
<td>V. Leveraging R&amp;D Funding to Promote Security Effectiveness of IoT Systems</td>
<td>320</td>
</tr>
<tr>
<td>VI. Leveraging Liability Limitation Authorities to promote Security Effectiveness of IoT Systems</td>
<td>322</td>
</tr>
<tr>
<td>VII. Conclusion</td>
<td>326</td>
</tr>
</tbody>
</table>
Chapter 11
State Attorneys General Protect Consumers in the IoT Era

Ellen Rosenblum
Cheryl Hiemstra
Katherine Campbell

I. Role of State Attorneys General
II. Collaboration with the Federal Trade Commission
III. Data Breaches
IV. Privacy, Big Data, and Consumer Protection
V. Innovations in State Privacy Laws and Regulations
VI. Consumer Protection in Communication, Information, and Media Technology Networks
VII. Consumer Welfare Implications Associated with Data Mining

Chapter 12
ICT in the States: The Challenges of Public Policy Making in the IoT Era

Michael Aisenberg

I. Federalism: An Obstacle or Opportunity for IoT?
II. The ICT Public Policy Context: Congressional Policy Gridlock
III. What Is at Stake in ICT Policy in the IoT Era?
IV. Issues of SCMTL ICT Policy Interest in the IoT Era
   A. Modernize Contracting for Information and Communications Technology Devices, Software, Services
   B. Privacy
   C. Institution of State/Local Inspector General (IG) Functions
   D. Reverse Existing Federal Preemption of State Civil Jurisdiction for Cyber-Based IoT Injuries
   E. Fusion Centers for IoT Flaw Information Sharing
V. Future Paths
Chapter 13

IoT Licensing Issues and Interoperability 359

Christopher A. Suarez

I. Introduction 359
II. The Trend toward Standardization and Interoperability in the IoT 360
   A. The Medical IoT 361
   B. Smart Home IoT Devices 362
   C. Connected Cars 364
III. Licensing in an Interoperable IoT 366
   A. Standards Essential Patents and Licensing 367
   B. FRAND Obligations and Standard Setting Organizations 372
   C. Royalty Stacking and Patent Hold-Up 376
   D. Licensing Principles and Strategies 379

Chapter 14

Liability and Connected Products: Litigation and the IoT 385

Richard M. Martinez

I. Introduction 385
   A. When the Internet Meets Things: Potential Injuries and Damages from the IoT 386
   B. The Harms from IoT Attacks Can Be Substantial 388
   C. The Growing Threat: From Stuxnet to Hackable Cars 389
   D. Risks to Privacy: Harms without Data Breaches 392
   E. Consumers in a Market of Complex Goods 394
   F. Liability and the IoT 395
II. Claims of Deceptive and Unfair Trade Practices 395
   A. ASUSTek Computer Inc. 396
   B. D-Link Systems, Inc. 397
   C. Lenovo Group Ltd. 398
   D. Vizio Inc. 399
   E. VTech Holdings Ltd. 399
   F. Standard Innovation Corp. 400
   G. ADT LLC 401
III. Liability for Diminished Value 402
IV. Possible New Statutory Bases of Liability 403
Contents

V. The California Consumer Privacy Act of 2018 404
   A. California’s First Step to Regulate Security of IoT Devices 405
VI. The Big Question: Product Liability in the IoT 406
VII. Yet Unknown Question: Global and International Liability 410
VIII. Conclusion 410

Chapter 15
Challenges for Electronic Discovery in the IoT Era 413
Christopher A. Suarez
Lucy L. Thomson

I. e-Discovery of IoT Data Is Complex 415
   A. Types of IoT Data 416
   B. Collection and Preservation of IoT Data 417
   C. Chain of Custody 420
   D. Privacy Issues 420
   E. IoT Forensics 421
   F. Scope of IoT Data Collection and Proportionality 421
   G. Analysis, Predictive Coding, and Artificial Intelligence 422
   H. Authentication of IoT Data 422
II. Information Governance for Executives and Corporate Counsel 425
III. ABA Ethics Rules: A Deeper Understanding of New Technologies Is Needed 427

Chapter 16
The IoT and Intellectual Property 429
Robert Maier

I. Introduction 429
II. Patent Law 430
   A. Software Patents Outside the United States 436
   B. Enforcement of IoT Patents 437
III. Trade Secret Law 438
   A. Uniform Trade Secrets Act (UTSA) 439
   B. Defend Trade Secrets Act (DTSA) 440
   C. Differences between Patent and Trade Secret Protection 442
IV. Copyright Law 444
   A. Derivative Works and Fair Use 445
Chapter 17
When Things Get Hacked: Insurance Coverage for IoT-Related Risks

John Buchanan
Dustin Cho

I. Introduction 457
II. Commercial General Liability Insurance Coverage for Bodily Injury or Property Damage Caused by Cyber Attacks through the IoT
   A. Cyber Exclusions in the CGL Form 461
   C. Exclusion p, ¶ (2): “Loss of . . . Electronic Data” 469
III. First-Party Property Coverage 470
IV. Emerging Coverage Solutions 472
V. Conclusions and Recommendations for Entities with IoT Risk Exposures 475

Chapter 18
Corporate Counsel and the Internet of Things

Joe Whitley
Melissa Goldman

I. Impact of IoT on Corporate Governance 478
   A. Role of General Counsel 478
   B. Role of Information Security Officer (ISO) 481
   C. Role of Compliance Officer 483
   D. Role of Board of Directors 485
II. Strategies for General Counsel during a Security Incident 488
   A. Internal Investigations 489
   B. Working with Law Enforcement and Other Governmental Entities 493
   C. Special Considerations for Public Companies 495
III. Future Outlook 498
Chapter 19
What Employers Need to Know about the Internet of Things 499
Peter Gillespie

I. Employers Have a Significant Role to Play as the Internet of Things Expands 499
II. Legal Requirements for Employers 501
   A. IoT-Related Privacy Risks for Employers 501
   B. State Data Protection Statutes 505
   C. National Labor Relations Act 507
   D. Wage and Hour Laws 509
   E. Litigation: Data Retention Requirements 510
III. Steps Employers Should Take to Stay Ahead of IoT Risks 511
IV. Conclusion 514

Chapter 20
Get SMART on Training: Make Privacy and Security a Part of the Organization’s Culture 517
Ruth Hill Bro
Jill D. Rhodes

I. Data Protection Training Basics and Core Principles 517
   A. Why Train on Data Protection? 519
   B. What Does SMART Training Look Like? 522
II. SMART Training in Action 527
   A. Understanding the Basics of Employees: Role and Generational Differences 528
   B. Building an Effective and Diverse Program 530
   C. Measuring Success (through Phishing Campaigns and Other Means) 533
III. Ten Key Points 534

Chapter 21
Back to the Future: Anticipating Regulatory Hurdles within IoT Pelotons 537
Brian Subirana

I. IoT Is Funneling Increasing Policy Complexity 537
II. IoT Peloton Road Mapping 539
### Contents

III. Anticipating IoT Long-term Peloton Business Benefits 543
   A. Information: Security of IoT 545
   B. Life: Wake Neutrality of Artificial Intelligence IoT Devices 547
   C. Matter: Legal Programming with High-Resolution Management, Blockchain, and a Packetized IoT Supply Chain 550
IV. A Very Long-Term IoT Business Benefit Scenario 551
V. Establishing Policy Options for IoT Pelotons 553

Index 557