CYBERSECURITY LAW

JEFF KOSSEFF

WILEY

Cybersecurity Law

Cybersecurity Law

Jeff Kosseff

WILEY

Registered Offices
John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA

Editorial Office
111 River Street, Hoboken, NJ 07030, USA

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Library of Congress Cataloging-in-Publication Data:

Names: Kosseff, Jeff, 1978- author.
Title: Cybersecurity law / Jeff Kosseff.
Description: Hoboken, New Jersey : John Wiley & Sons, [2017] | Includes bibliographical references and index.
Identifiers: LCCN 2016038242| ISBN 9781119231509 (cloth) | ISBN 9781119232025 (epub)
Subjects: LCSH: Computer security – Law and legislation – United States. | Data protection – Law and legislation – United States. | Hacking – United States – Prevention. | Cyberterrorism – Prevention. | Privacy, Right of – United States. | Computer networks – Security measures. | Computer security – Law and legislation.
Classification: LCC KF1263.C65 K67 2017 | DDC 343.7309/99 – dc23
LC record available at https://lccn.loc.gov/2016038242

Cover image: Westend61/Gettyimages
Cover design by Wiley

Set in 10/12pt Warnock by SPi Global, Chennai, India

Printed in the United States of America

V10007636_011519

This book is dedicated to my two biggest supporters, my wife, Crystal Zeh, and my daughter, Julia Kosseff.

Contents

About the Author *xv*
Acknowledgment *xvii*
About the Companion Website *xix*
Introduction *xxi*

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? *5*
1.1.3 LabMD: What Constitutes "Unfair" or "Deceptive" Data Security? *9*
1.1.4 FTC June 2015 Guidance on Data Security *11*
1.1.5 FTC Protecting Personal Information Guide *14*
1.1.6 Lessons from FTC Cybersecurity Complaints *15*
1.1.6.1 Failure to Secure Highly Sensitive Information *16*
1.1.6.1.1 Use Industry-Standard Encryption for Sensitive Data *16*
1.1.6.1.2 Routine Audits and Penetration Testing are Expected *17*
1.1.6.1.3 Health-Related Data Requires Especially Strong Safeguards *18*
1.1.6.1.4 Data Security Protection Extends to Paper Documents *19*
1.1.6.1.5 Business-to-Business Providers also are Accountable to the FTC For Security of Sensitive Data *20*
1.1.6.1.6 Companies are Responsible for the Data Security Practices of Their Contractors *22*
1.1.6.1.7 Make Sure that Every Employee Receives Regular Data Security Training for Processing Sensitive Data *23*
1.1.6.1.8 Privacy Matters, Even in Data Security *23*
1.1.6.1.9 Limit the Sensitive Information Provided to Third Parties *24*
1.1.6.2 Failure to Secure Payment Card Information *24*
1.1.6.2.1 Adhere to Security Claims about Payment Card Data *24*
1.1.6.2.2 Always Encrypt Payment Card Data *25*
1.1.6.2.3 Payment Card Data Should be Encrypted Both in Storage and at Rest *26*

1.1.6.2.4 In-Store Purchases Pose Significant Cybersecurity Risks *26*
1.1.6.2.5 Minimize Duration of Storage of Payment Card Data *28*
1.1.6.2.6 Monitor Systems and Networks for Unauthorized Software *29*
1.1.6.2.7 Apps Should Never Override Default App Store Security Settings *29*
1.1.6.3 Failure to Adhere to Security Claims *30*
1.1.6.3.1 Companies Must Address Commonly Known Security Vulnerabilities *30*
1.1.6.3.2 Ensure that Security Controls are Sufficient to Abide by Promises about Security and Privacy *31*
1.1.6.3.3 Omissions about Key Security Flaws can also be Misleading *33*
1.1.6.3.4 Companies Must Abide by Promises for Security-Related Consent Choices *33*
1.1.6.3.5 Companies that Promise Security Must Ensure Adequate Authentication Procedures *34*
1.1.6.3.6 Adhere to Promises about Encryption *35*
1.2 State Data Breach Notification Laws *36*
1.2.1 When Consumer Notifications are Required *37*
1.2.1.1 Definition of Personal Information *37*
1.2.1.2 Encrypted Data *38*
1.2.1.3 Risk of Harm *39*
1.2.1.4 Safe Harbors and Exceptions to Notice Requirement *39*
1.2.2 Notice to Individuals *40*
1.2.2.1 Timing of Notice *40*
1.2.2.2 Form of Notice *40*
1.2.2.3 Content of Notice *41*
1.2.3 Notice to Regulators and Consumer Reporting Agencies *41*
1.2.4 Penalties for Violating State Breach Notification Laws *42*
1.3 State Data Security Laws *42*
1.3.1 Oregon *43*
1.3.2 Rhode Island *45*
1.3.3 Nevada *45*
1.3.4 Massachusetts *46*
1.4 State Data Disposal Laws *49*

2 Cybersecurity Litigation *51*
2.1 Article III Standing *52*
2.1.1 Applicable Supreme Court Rulings on Standing *53*
2.1.2 Lower Court Rulings on Standing in Data Breach Cases *57*
2.1.2.1 Injury-in-Fact *57*
2.1.2.1.1 Broad View of Injury-in-Fact *57*
2.1.2.1.2 Narrow View of Injury-in-Fact *60*
2.1.2.2 Fairly Traceable *62*
2.1.2.3 Redressability *63*

2.2 Common Causes of Action Arising from Data Breaches *64*
2.2.1 Negligence *64*
2.2.1.1 Legal Duty and Breach of Duty *65*
2.2.1.2 Cognizable Injury *67*
2.2.1.3 Causation *69*
2.2.2 Negligent Misrepresentation or Omission *70*
2.2.3 Breach of Contract *72*
2.2.4 Breach of Implied Warranty *76*
2.2.5 Invasion of Privacy by Publication of Private Facts *80*
2.2.6 Unjust Enrichment *81*
2.2.7 State Consumer Protection Laws *82*
2.3 Class Action Certification in Data Breach Litigation *84*
2.4 Insurance Coverage for Cybersecurity Incidents *90*
2.5 Protecting Cybersecurity Work Product and Communications from Discovery *94*
2.5.1 Attorney–Client Privilege *96*
2.5.2 Work Product Doctrine *98*
2.5.3 Non-Testifying Expert Privilege *101*
2.5.4 Applying the Three Privileges to Cybersecurity: *Genesco v. Visa* *102*

3 Cybersecurity Requirements for Specific Industries *105*
3.1 Financial Institutions: Gramm-Leach-Bliley Act Safeguards Rule *106*
3.1.1 Interagency Guidelines *106*
3.1.2 Securities and Exchange Commission Regulation S-P *109*
3.1.3 FTC Safeguards Rule *110*
3.2 Financial Institutions and Creditors: Red Flag Rule *112*
3.2.1 Financial Institutions or Creditors *116*
3.2.2 Covered Accounts *116*
3.2.3 Requirements for a Red Flag Identity Theft Prevention Program *117*
3.3 Companies that use Payment and Debit Cards: Payment Card Industry Data Security Standard (PCI DSS) *118*
3.4 Health Providers: Health Insurance Portability and Accountability Act (HIPAA) Security Rule *121*
3.5 Electric Utilities: Federal Energy Regulatory Commission Critical Infrastructure Protection Reliability Standards *127*
3.5.1 CIP-003-6: Cybersecurity – Security Management Controls *127*
3.5.2 CIP-004-6: Personnel and Training *128*
3.5.3 CIP-006-6: Physical Security of Cyber Systems *128*
3.5.4 CIP-007-6: Systems Security Management *128*
3.5.5 CIP-009-6: Recovery Plans for Cyber Systems *129*
3.5.6 CIP-010-2: Configuration Change Management and Vulnerability Assessments *129*

3.5.7 CIP-011-2: Information Protection *130*
3.6 Nuclear Regulatory Commission Cybersecurity Regulations *130*

4 Cybersecurity and Corporate Governance *133*
4.1 Securities and Exchange Commission Cybersecurity Expectations for Publicly Traded Companies *134*
4.1.1 10-K Disclosures: Risk Factors *135*
4.1.2 10-K Disclosures: Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A) *137*
4.1.3 10-K Disclosures: Description of Business *137*
4.1.4 10-K Disclosures: Legal Proceedings *138*
4.1.5 10-K Disclosures: Examples *138*
4.1.5.1 Wal-Mart *138*
4.1.5.2 Berkshire Hathaway *143*
4.1.5.3 Target Corp *144*
4.1.6 Disclosing Data Breaches to Investors *147*
4.2 Fiduciary Duty to Shareholders and Derivative Lawsuits Arising from Data Breaches *150*
4.3 Committee on Foreign Investment in the United States and Cybersecurity *152*
4.4 Export Controls and the Wassenaar Arrangement *154*

5 Anti-Hacking Laws *159*
5.1 Computer Fraud and Abuse Act *160*
5.1.1 Origins of the CFAA *160*
5.1.2 Access without Authorization and Exceeding Authorized Access *161*
5.1.2.1 Narrow View of "Exceeds Authorized Access" and "Without Authorization" *163*
5.1.2.2 Broader View of "Exceeds Authorized Access" and "Without Authorization" *167*
5.1.2.3 Attempts to Find a Middle Ground *169*
5.1.3 The Seven Sections of the CFAA *170*
5.1.3.1 CFAA Section (a)(1): Hacking to Commit Espionage *172*
5.1.3.2 CFAA Section (a)(2): Hacking to Obtain Information *172*
5.1.3.3 CFAA Section (a)(3): Hacking a Federal Government Computer *176*
5.1.3.4 CFAA Section (a)(4): Hacking to Commit Fraud *178*
5.1.3.5 CFAA Section (a)(5): Hacking to Damage a Computer *181*
5.1.3.5.1 CFAA Section (a)(5)(A): Knowing Transmission that Intentionally Damages a Computer Without Authorization *181*
5.1.3.5.2 CFAA Section (a)(5)(B): Intentional Access Without Authorization that Recklessly Causes Damage *184*
5.1.3.5.3 CFAA Section (a)(5)(C): Intentional Access Without Authorization that Causes Damage and Loss *185*

5.1.3.5.4 CFAA Section (a)(5): Requirements for Felony and Misdemeanor Cases *186*
5.1.3.6 CFAA Section (a)(6): Trafficking in Passwords *188*
5.1.3.7 CFAA Section (a)(7): Threatening to Damage or Obtain Information from a Computer *190*
5.1.4 Civil Actions under the CFAA *193*
5.1.5 Criticisms of the CFAA *195*
5.2 State Computer Hacking Laws *198*
5.3 Section 1201 of the Digital Millennium Copyright Act *201*
5.3.1 Origins of Section 1201 of the DMCA *202*
5.3.2 Three Key Provisions of Section 1201 of the DMCA *203*
5.3.2.1 DMCA Section 1201(a)(1) *203*
5.3.2.2 DMCA Section 1201(a)(2) *208*
5.3.2.2.1 Narrow Interpretation of Section (a)(2): Chamberlain Group v. Skylink Technologies *209*
5.3.2.2.2 Broad Interpretation of Section (a)(2): MDY Industries, LLC v. Blizzard Entertainment, Inc. *211*
5.3.2.3 DMCA Section 1201(b)(1) *215*
5.3.3 Section 1201 Penalties *217*
5.3.4 Section 1201 Exemptions *218*
5.3.5 The First Amendment and DMCA Section 1201 *224*
5.4 Economic Espionage Act *227*
5.4.1 Origins of the Economic Espionage Act *228*
5.4.2 Criminal Prohibitions on Economic Espionage and Theft of Trade Secrets *229*
5.4.2.1 Definition of "Trade Secret" *230*
5.4.2.2 "Knowing" Violations of the Economic Espionage Act *234*
5.4.2.3 Purpose and Intent Required under Section 1831: Economic Espionage *234*
5.4.2.4 Purpose and Intent Required under Section 1832: Theft of Trade Secrets *236*
5.4.3 Civil Actions for Trade Secret Misappropriation: The Defend Trade Secrets Act of 2016 *238*
5.4.3.1 Definition of "Misappropriation" *239*
5.4.3.2 Civil Seizures *240*
5.4.3.3 Injunctions *241*
5.4.3.4 Damages *241*
5.4.3.5 Statute of Limitations *242*

6 Public–Private Cybersecurity Partnerships *243*
6.1 U.S. Government's Civilian Cybersecurity Organization *244*
6.2 Department of Homeland Security Information Sharing under the Cybersecurity Act of 2015 *245*
6.3 Energy Department's Cyber-Threat Information Sharing *249*

6.4 Critical Infrastructure Executive Order and the National Institute of Standards and Technology's Cybersecurity Framework *250*
6.5 U.S. Military Involvement in Cybersecurity and the Posse Comitatus Act *256*

7 Surveillance and Cyber *259*
7.1 Fourth Amendment *260*
7.1.1 Was the Search or Seizure Conducted by a Government Entity or Government Agent? *261*
7.1.2 Did the Search or Seizure Intrude Upon an Individual's Privacy Interests? *265*
7.1.3 Did the Government have a Warrant? *269*
7.1.4 If the Government Did Not Have a Warrant, Did an Exception to the Warrant Requirement Apply? *271*
7.1.5 Was the Search or Seizure Reasonable under the Totality of the Circumstances? *273*
7.2 Electronic Communications Privacy Act *275*
7.2.1 Stored Communications Act *276*
7.2.1.1 Section 2701: Third-Party Hacking of Stored Communications *278*
7.2.1.2 Section 2702: Restrictions on Service Providers' Ability to Disclose Stored Communications and Records to the Government and Private Parties *279*
7.2.1.2.1 The Cybersecurity Act of 2015: Allowing Service Providers to Disclose Cybersecurity Threats to the Government *282*
7.2.1.3 Section 2703: Government's Ability to Force Service Providers to Turn Over Stored Communications and Customer Records *284*
7.2.2 Wiretap Act *286*
7.2.3 Pen Register Act *290*
7.2.4 National Security Letters *291*
7.3 Communications Assistance for Law Enforcement Act (CALEA) *293*
7.4 Encryption and the All Writs Act *294*

8 Cybersecurity and Federal Government Contractors *299*
8.1 Federal Information Security Management Act *300*
8.2 NIST Information Security Controls for Government Agencies and Contractors *301*
8.3 Classified Information Cybersecurity *306*
8.4 Covered Defense Information and Controlled Unclassified Information *309*

9 Privacy Laws *317*
9.1 Section 5 of the FTC Act and Privacy *318*
9.2 Health Insurance Portability and Accountability Act *324*
9.3 Gramm-Leach-Bliley Act and California Financial Information Privacy Act *326*
9.4 CAN-SPAM Act *327*
9.5 Video Privacy Protection Act *328*
9.6 Children's Online Privacy Protection Act *330*
9.7 California Online Privacy Laws *332*
9.7.1 California Online Privacy Protection Act (CalOPPA) *332*
9.7.2 California Shine the Light Law *333*
9.7.3 California Minor "Eraser Law" *335*
9.8 Illinois Biometric Information Privacy Act *337*

10 International Cybersecurity Law *339*
10.1 European Union *340*
10.2 Canada *346*
10.3 China *350*
10.4 Mexico *353*
10.5 Japan *356*

Appendix A: Text of Section 5 of the FTC Act *361*

Appendix B: Summary of State Data Breach Notification Laws *369*

Appendix C: Text of Section 1201 of the Digital Millennium Copyright Act *413*

Appendix D: Text of the Computer Fraud and Abuse Act *425*

Appendix E: Text of the Electronic Communications Privacy Act *433*

Index *485*

A definitiv

Expanding on the author's e
Cybersecurity Law is the defi
of U.S. and international la
information safeguarding, lav
and many other cybersecurity
real-world examples and case studies to help readers understand the presented material
of the presented material. The book begins by outlining the le
security, which synthesizes the Federal Trade Commission's cy
to provide the background of the FTC's views on data securit
data security requirements imposed by a growing number of st
litigation arising from data breaches. Anti-hacking laws, suc
Fraud and Abuse Act, Economic Espionage Act, and the Digital Millennium Copyright Act, and how companies are able to fight cybercriminals while ensuring compliance with the U.S. Constitution and statutes are discussed thoroughly. Featuring an overview of the laws that allow coordination between the public and private sectors as well as the tools that regulators have developed to allow a limited amount of collaboration, this book also:

- Addresses current U.S. and international laws, regulations, and court opinions that define the field of cybersecurity including the security of sensitive information, such as financial data and health information
- Discusses the cybersecurity requirements of the largest U.S. trading partners in Europe, Asia, and Latin America, and specifically addresses how these requirements are similar to (and differ from) those in the U.S.
- Provides a compilation of many of the most important cybersecurity statutes and regulations
- Emphasizes the compliance obligations of companies with in-depth analysis of crucial U.S. and international laws that apply to cybersecurity issues
- Examines government surveillance laws and privacy laws that affect cybersecurity as well as each of the data breach notification laws in 47 states and the District of Columbia
- Includes numerous case studies and examples throughout to aid in classroom use and to help readers better understand the presented material
- Supplemented with a companion website that features in-class discussion questions and timely and recent updates on recent legislative developments as well as information on interesting cases on relevant and significant topics

Cybersecurity Law is appropriate as a textbook for undergraduate and graduate-level courses in cybersecurity, cybersecurity law, cyber operations, management-oriented information technology (IT), and computer science. This book is also an ideal reference for lawyers, IT professionals, government personnel, business managers, IT management personnel, auditors, and cybersecurity insurance providers.

JEFF KOSSEFF is Assistant Professor of Cybersecurity Law at the United States Naval Academy in Annapolis, Maryland. He frequently speaks and writes about cybersecurity and was a journalist covering technology and politics at *The Oregonian,* a finalist for the Pulitzer Prize, and a recipient of the George Polk Award for national reporting.

Cover design: Wiley
Cover image: ©Westend61/ Gettyimages

www.wiley.com/go/kosseff/cybersecurity

ISBN 978-1-119-23150-9

WILEY

Also available as an e-book

9 781119 231509