Privacy and Data Protection in Business: Laws and Practices

LexisNexis Law School Publishing Advisory Board

Privacy and Data Protection in Business: Laws and Practices

Jonathan I. Ezor

LexisNexis®

ISBN: 9781422490969

Library of Congress Cataloging-in-Publication Data

Ezor, Jonathan
Privacy and data protection in business : laws and practices / Jonathan I. Ezor.
p. cm.
Includes index.
Looseleaf ISBN 978-1-4224-9096-9
1. Business records--Law and legislation--United States. 2. Data protection--Law and legislation--United States. 3. Privacy, Right of--United States. 4. Computer networks--Access control--United States. 5. Digital communications--United States. I. Title.
KF1357.5.E96 2012
346.73'065--dc23

2012028733

NOTE TO USERS
To ensure that you are using the latest materials available in this area, please be sure to periodically check the LexisNexis Law School web site for downloadable updates and supplements at www.lexisnexis.com/lawschool.

Editorial Offices
121 Chanlon Rd., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2012–Pub.3329)

Acknowledgments

This book would not have been possible without a number of people to whom I express my deep appreciation. First and foremost, I wish to thank my wife Stacy and our children Avi, Eitan and Elisheva, for their support, encouragement, and feedback.

Next, my friends and Touro College Jacob D. Fuchsberg Law Center colleagues Gary Shaw and Linda Howard Weissman, who co-founded and remain active in building the Institute for Business, Law and Technology at Touro which I have headed since 2003. Touro Law Dean Emeritus Howard A. Glickstein and Dean Lawrence Raful have provided valued leadership, both institutional and personal, and the Touro Law faculty has always supported me and the Institute's programs. My Touro students have learned from and with me about privacy and many other business technology law subjects, and teaching law students remains one of my sweetest pleasures. This work in particular would not have been possible without the enthusiastic and capable research assistance of Touro Law students Stephanie Rapp and Scott Richman, for which I am grateful.

I also want to acknowledge the attorneys and other professionals of the IBLT Advisory Board, on whose sage guidance I have relied for many years; Andrew Lustigman and Adam Solomon and their Olshan colleagues; and Andrew Lupu, Jules Polonetsky, and the other business privacy thought leaders and practitioners from whom I have learned so much in my career.

Finally, this book is dedicated to my mother Rita Ezor, "star of stage, screen and language arts." She has always been my best example of how writing and teaching are most effective when done with an appreciation of audience and purpose, and a desire to engage, not just inform, one's students.

TABLE OF CONTENTS

Chapter 1 INTRODUCTION: THE MEANING OF PRIVACY AND THE VALUE OF INFORMATION 1

I. STARTING POINT: WHAT IS "PRIVACY"? 1
II. THE BUSINESS VALUE OF INFORMATION 6
III. COMPUTERS AND DIGITAL MEDIA: THEIR IMPACT ON PRIVACY . . . 7
IV. THE ROLE (AND RULE) OF LAW 8
V. CHALLENGES FOR THE RISK MANAGER 9
From "A Face is Exposed for AOL Searcher No. 4417749" 10
VI. THE APPROACH OF THIS BOOK: PRACTICAL UNDERSTANDING AND A PATH TO BEST PRACTICES 11

Chapter 2 CONSUMER PRIVACY: BALANCING VALUE TO CONSUMERS WITH VALUE OF CONSUMERS 13

I. WHY CONSUMER PRIVACY MATTERS: A LESS THAN CHEERY SCENARIO 13
II. CONSUMER INFORMATION COLLECTION AND THE RISE OF E-COMMERCE 14
A Redefinition of the Concept of Personal Privacy 14
III. CONSUMER PRIVACY AND CONSUMER PROTECTION: THE FTC . . . 18
Unfair methods of competition unlawful; prevention by Commission 18
Fair Information Practice Principles Generally 19
IV. ANATOMY OF A PRIVACY POLICY: THE FAIR INFORMATION PRACTICE PRINCIPLES IN ACTION 26
a. Notice/Awareness: Spreading the (Accurate) Word 26
b. Choice/Consent: Getting Informed Permission 29
May 24, 2001 Letter from FTC Bureau of Consumer Protection to Junkbusters Corp and Electronic Privacy Information Center 29
c. Integrity/Security: Keeping Data Safe and Unaltered 31
BJ's Wholesale Club Settles FTC Charges Agency Says Lax Security Compromised Thousands of Credit and Debit Cards 31
ValueClick to Pay $2.9 Million to Settle FTC Charges 33
d. Enforcement/Redress: Remedies for Wrongs 34
V. OTHER FEDERAL LAWS INVOLVING CONSUMER PRIVACY 34
VI. STATE CONSUMER PRIVACY LAWS: LOCAL LEGISLATION, WIDE-RANGING IMPACT 39
Cal. Bus. & Prof. Code § 22575. Commercial Web site operators; posting of privacy policy; violation of subdivision for failure to post policy; policy requirements 40

TABLE OF CONTENTS

Excerpt from Cal. Civ. Code § 1798.83: Personal Information; Disclosure to Direct Marketers 41
VII. CONCLUSION: BEST PRACTICES START WITH ACCURATE DISCLOSURE 44

Chapter 3 SOCIAL MEDIA PRIVACY: NOT (NECESSARILY) AN OXYMORON 47

I. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT: THE KEY FEDERAL STATUTE 48
II. SOCIAL MEDIA SHARING: THE FOUR WS 49
a. Who: Identity, Anonymity and Pseudonymity Online 49
Excerpt from "A Rape in Cyberspace" by Julian Dibbell 50
Excerpt from "Afghanistan War Logs: Story Behind Biggest Leak in Intelligence History" 52
Excerpted From The Cutting Edge: The Helsinki Incident and the Right to Anonymity By Daniel Akst 54
b. What: Content as Disclosure 55
From "A Twitter Code of Conduct" by Douglas MacMillan 57
c. When: Time as a Key Element of Identity 57
From "Faulty IP address data leads to Shaq attack on innocent family" 59
d. Where: Location-Based Information 59
From "Virtual Community Standards" 61
From "Geo-Location Technologies and Other Means of Placing Borders on the 'Borderless' Internet" 61
From "Please Rob Me: The Risks of Online Oversharing" 63
From "Facebook 'Friend' Suspected in Burglary" 64
III. CONCLUSION: SOCIAL MEDIA PRIVACY: SIGNIFICANT CHALLENGES AND BEST PRACTICES 64

Chapter 4 THE SPECIAL CASE OF CHILDREN 67

I. LAW AND SELF-REGULATION TO PROTECT CHILDREN'S PRIVACY 69
a. Self-Regulation: The CARU Guidelines 69
b. The Origins of COPPA 74
II. REQUIREMENTS OF COPPA 83
April 22, 2002 News Release: FTC Protecting Children's Privacy Online . 85
Iconix Brand Group Settles Charges Its Apparel Web Sites Violated Children's Online Privacy Protection Act Company Will Pay $250,000 Civil Penalty . 86
III. COPPA, THE FTC, AND THE EVOLUTION OF NEW TECHNOLOGIES . 87

An Examination of Children's Privacy: New Technology and the Children's Online Privacy Protection Act 88
July 12, 2010 Comments by Facebook, Inc. on COPPA Review 89
European NGO Alliance for Child Safety Online Submission to the FTC Review of the COPPA Rule 90
IV. CONCLUSION: CHILDREN'S PRIVACY: SIGNIFICANT CHALLENGES AND BEST PRACTICES 97
[Consumer Reports] Survey: 7.5 Million Facebook Users are Under the Age of 13, Violating the Site's Terms 97
Kids Today: How the Class of 2011 Engages with Media 98
A-Gs to probe kids' privacy on Facebook 99

Chapter 5 HEALTH AND MEDICAL PRIVACY: (UN)CONDITIONAL PROTECTION 101

I. HEALTH CONDITIONS AND GENETIC CODE: PREVENTING DISCRIMINATION AND DISCLOSURE 102
Cases of Genetic Discrimination National Human Genome Research Institute, National Institutes of Health, Cases of Genetic Discrimination, http://www.genome.gov/12513976 (last visited May 8, 2012). 102
§ 2000ff-1: Employer Practices42 U.S.C. § 2000ff-1. 103
Confidentiality of Genetic Information42 U.S.C. § 2000ff-5. 105
Doe v. Borough of Barrington 107
II. OBLIGATIONS TO DISCLOSE: CASES AND STATUTES 121
Tarasoff v. Regents of University of California 122
Leonard v. Latrobe Area Hosp. 134
Persons and officials required to report cases of suspected child abuse or maltreatment 139
III. THE CHALLENGES OF DIGITAL PERSONAL HEALTH INFORMATION 140
IV. FEDERAL STATUTORY DIRECTIVES REGARDING ELECTRONIC MEDICAL RECORDS: HIPAA AND HITECH 141
a. Electronic Storage: The HIPAA Statutory Framework 142
Recommendations With Respect to Privacy of Certain Health Information. 142
Sec. 1173: Standards to Enable Electronic Exchange 143
b. HIPAA Regulations: The Privacy and Security Rules 145
§ 160.103 Definitions.45 CFR § 160.103. 146
Business Associates Business Associates, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html (last visited May 8, 2012). 153
c. The HITECH Act and Revisions to HIPAA 157

Notification in the case of breach 42 U.S.C. § 17932. 157
d. HHS Enforcement of the HIPAA Privacy and Security Rules 161
How OCR Enforces the HIPAA Privacy RuleHow OCR Enforces the HIPAA Privacy Rule, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/howocrenforces.html (last visited May 8, 2012). 161
University of California settles HIPAA Privacy and Security case involving UCLA Health System facilities UCLAHS to improve policies and procedures to better safeguard patient information 163
Rite Aid Agrees to Pay $1 Million to Settle HIPAA Privacy Case Company agrees to substantial corrective action to safeguard consumer information 164
V. STATE HEALTH PRIVACY LAWS 165
VI. PRIVATE ENFORCEMENT OF PHI AND RELATED PRIVACY RIGHTS 167
Sorrell v. Ims Health Inc. 167

Chapter 6 FINANCIAL PRIVACY: INFORMATION AND VALUE . . 183

I. VERIFIABLE IDENTITY FOR FINANCIAL TRANSACTIONS 183
II. THE RIGHT TO FINANCIAL PRIVACY ACT 184
III. THE FAIR CREDIT REPORTING ACT 187
From "40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations" 209
IV. THE GRAMM-LEACH BLILEY ACT 210
From: The Gramm-Leach-Bliley Act: Privacy of Consumer Financial Information the Gramm-Leach-Bliley Act: Privacy of Consumer Financial Information, http://ftc.gov/privacy/glbact/glboutline.htm (last visited May 8, 2012). 211
Credit Report Resellers Settle FTC Charges; Security Failures Allowed Hackers to Access Consumers' Personal Information 214
V. OTHER RELEVANT LAWS 216
VI. PURCHASE PRIVACY: SELF-REGULATION AND INDUSTRY GUIDANCE ON LEGISLATION 216

Chapter 7 WORKPLACE PRIVACY: DIFFERENT NEEDS, DIFFERENT EXPECTATIONS, DIFFERENT RULES 219

I. MONITORING WORKERS: PHYSICALLY AND ELECTRONICALLY . 219
a. Reasonable Expectations of Workplace Data Privacy 219
§ 31–48d. Employers engaged in electronic monitoring required to give prior notice to employees. Exceptions. Civil penalty 223
b. Electronic Monitoring by Private Versus Public Employers: Case Law

TABLE OF CONTENTS

Counterpoints 224
Michael A. Smyth v. The Pillsbury Company 224
City of Ontario v. Quon 229
c. An Outside View: Monitoring Employees' Personal Activities 239
Konop v. Hawaiian Airlines 242
February 8, 2011 NLRB Press Release: Settlement reached in case involving discharge for Facebook comments 256
II. EMPLOYEE PERSONAL INFORMATION: A NON-CONSUMER CONTEXT 257

Chapter 8 DATA BREACH: PREVENTION, DETECTION, AND NOTIFICATION 259

I. THE CAUSES AND SCOPE OF DATA BREACHES 260
United States v. Ivanov 262
II. LEGAL OBLIGATIONS TO PREVENT DATA BREACH 270
a. Self-Imposed Obligations: Contracts, Disclosure and Internal Policies . . . 270
b. Spotting Potential Data Breach Vulnerability: The FTC's Red Flags Rule . 279
III. POST-BREACH: DISCLOSURE AND LIABILITY 282
a. Breach Notification Laws: State and Potential Federal Requirements 283
§ 1798.81.5. Security procedures and practices with respect to personal information about California residents 283
§ 1798.82. Civil actions; violation of title 284
b. Litigation Arising out of Data Breach 288
Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data 288
In Re Hannaford Bros. Co. Customer Data Security Breach Litigation4 A.3d 492 (supreme Judical Ct. Maine 2010) (notes Omitted). 291
In Re: Heartland Payment Systems, Inc. Customer Data Security Breach Litigation 295

Chapter 9 INTERNATIONAL PRIVACY LAW: A WORLD OF DIFFERENT APPROACHES 329

I. JURISDICTION: WHAT LAWS APPLY? 329
II. TWO MAJOR RELEVANT REGIMES: THE EU DATA PROTECTION DIRECTIVE AND PIPEDA 331
a. The EU Data Protection Directive and the U.S. Safe Harbor 331
i. The EU Data Protection Directive 331
SECTION IX: NOTIFICATION 332
Chapter IV: Transfer of Personal Data to Third Countries 334

TABLE OF CONTENTS

ii. The U.S. Safe Harbor 336
iii. Safe Harbor Enforcement 341
Court Halts U.S. Internet Seller Deceptively Posing as U.K. Home Electronics Site 341
iv. Proposed Updates to the EU Data Protection Directive 342
Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses . 342
b. PIPEDA 344
c. Other International Privacy Regimes: The APEC Framework, Pathfinder and Cross-Border Enforcement Arrangement. 345
Acting U.S. Commerce Secretary Rebecca Blank Announces U.S. Participation in APEC's Cross Border Privacy Rules System 345
FTC Becomes First Enforcement Authority in APEC Cross-Border Privacy Rules System 346

Chapter 10 PRIVACY AND CYBERCRIME INVESTIGATIONS: THE FOURTH AMENDMENT AND ECPA 349

I. THE FOURTH AMENDMENT AND DATA SEARCHES 350
Guest v. Leis 352
United States v. Adjani 364
U.S. v. Horowitz 375
II. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT AND LAW ENFORCEMENT 379
People v. Harris 379
III. EYES IN THE GROUND AND SKY: THE USE OF GPS TRACKING AND DRONES IN LAW ENFORCEMENT 385
U.S. v. Jones 386
From "Did a Surveillance Drone Help in the Arrest of a North Dakota Farmer?" 395

Chapter 11 ATTORNEYS: CLIENT PRIVACY AND ETHICS 397

I. APPLICABILITY OF PRIVACY LAWS AND REGULATIONS TO ATTORNEYS 397
American Bar Ass'n v. F.T.C. 398
Lawyer for preeminent firms pleads guilty in $37 million insider trading scheme using information stolen from employers 414
II. CLIENT CONFIDENTIAL INFORMATION: UNINTENTIONAL DISCLOSURE BY LAWYERS 416

TABLE OF CONTENTS

Table of Cases **TC-1**

Index **I-1**