Summary of Contents

Contents

Chapter 1: California and U.S. Federal Privacy Overview

Chapter 2: California and U.S. Federal Privacy Laws from A to Z

Chapter 3: Compliance Guide

Chapter 4: Drafting a Privacy Policy

Chapter 5: Drafting Other Privacy Documentation

Chapter 6: Enforcement

Chapter 7: Risk Mitigation

Table of Cases

Index
# Contents

*Summary of Contents* ...................................................... iii  
*Foreword* ........................................................................ xxv  
*About This Book* ........................................................... xxxiii  
*About the Author* ........................................................... xxxv  
*Acknowledgments* ............................................................ xxxvii  
*Readers’ Feedback Regarding Prior Editions of This Book* ...................................................... xxxix

## Chapter 1: California and U.S. Federal Privacy Law Overview

1.1 Chapter Overview .......................................................... 1  
1.2 California ....................................................................... 1  
1.2.1 Laws Made by California vs. Federal Laws .................. 3  
1.2.2 Scope and Applicability of California Law ................. 4  
  1.2.2.1 Limitations on California Jurisdiction Under International Law ........................................... 5  
  1.2.2.2 Limitations on California Jurisdiction Under Federal Law ............................................... 10  
  1.2.2.3 California Conflict of Law Rules ....................... 13  
  1.2.2.4 Enforceability of California Laws Outside California ......................................................... 18  
1.3 Privacy ............................................................................ 20  
  1.3.1 Rights to Privacy and Data Privacy ......................... 20  
  1.3.2 Data Protection, Data Privacy and Data Security. .... 24  
  1.3.3 Property .................................................................. 27  
  1.3.4 Freedom of Speech and Information ................. 29  
1.4 Law .............................................................................. 33  
1.5 California and U.S. Federal Privacy Law Summary .............. 34  
  1.5.1 Scope. .................................................................... 34  
  1.5.2 Terminology ................................................................ 35
1.5.3 Key Features .................................................. 37
1.5.4 California and U.S. Privacy Law—What It Is Not .................. 37

Chapter 2: California and U.S. Federal Privacy Laws from A to Z

2.1 Chapter Overview .................................................. 43
2.2 Autonomy Privacy and Article 1 of the California Constitution .... 44
   2.2.1 Who and What Data Is Protected? .......................... 48
   2.2.2 Who Must Comply? ........................................... 48
   2.2.3 How To Comply? .............................................. 49
   2.2.4 Sanctions and Remedies .................................... 53
2.3 Brokers ............................................................... 54
   2.3.1 Who and What Data Is Protected? ......................... 55
   2.3.2 Who Must Comply? ............................................ 55
       2.3.2.1 Business ................................................ 56
       2.3.2.2 Personal Information Selling .......................... 56
       2.3.2.3 Direct Relationship .................................... 56
       2.3.2.4 Exemptions .............................................. 58
   2.3.3 How To Comply? .............................................. 59
   2.3.4 Sanctions and Remedies .................................... 59
2.4 California Consumer Privacy Act ................................ 59
   2.4.1 Who and What Data Is Protected? .......................... 64
       2.4.1.1 California Residents .................................... 64
       2.4.1.2 Personal Information - Broad Definition .............. 65
       2.4.1.3 Personal Information - Narrower Definition in the Security Breach Context ........................................ 68
       2.4.1.4 Sensitive Personal Information ......................... 69
   2.4.2 Who Must Comply? ............................................ 71
       2.4.2.1 Doing Business in California ......................... 71
       2.4.2.2 Operating For Profit or Financial Benefit of Owners .... 73
       2.4.2.3 Determining Means and Purposes of Processing ..... 73
       2.4.2.4 Thresholds .............................................. 74
       2.4.2.5 Affiliates ................................................. 76
       2.4.2.6 Exempted Businesses .................................... 78
2.4.3 How to Comply? ............................................................. 78
  2.4.3.1 Identifying and Avoiding Personal Information
          Selling and Sharing ............................................. 80
  2.4.3.2 Extra Obligations for Businesses that Sell or Share ....... 84
  2.4.3.3 Limit the Use of Sensitive Personal Information ............ 88
  2.4.3.4 Data Subject Rights .......................................... 90
  2.4.3.4 Privacy Notices and Policies .................................. 94
  2.4.3.5 Training and Record Keeping Requirements .................. 95
  2.4.3.6 Exceptions and Exemptions .................................... 96
  2.4.3.7 Data Minimization ........................................... 96
  2.4.3.9 Additional Requirements and Prohibitions under CCPA
          Regulations regarding Dark Patterns and other Topics .......... 97
  2.4.4 Sanctions and Remedies ......................................... 98
    2.4.4.1 Civil and Administrative Penalties ......................... 98
    2.4.4.2 Statutory Damages ......................................... 100
    2.4.4.3 Unfair Competition Claims ................................. 103
  2.5 Data Security Requirements ....................................... 104
    2.5.1 General Requirements for the Security of
          Personal Information ........................................... 105
      2.5.1.1 Who and What Data Is Protected? ......................... 105
      2.5.1.2 Who Must Comply? ....................................... 106
      2.5.1.3 How To Comply? ......................................... 107
      2.5.1.4 Sanctions and Remedies ................................. 107
    2.5.2 Disposal of Customer Records ................................ 107
      2.5.2.1 Who and What Data Is Protected? ......................... 107
      2.5.2.2 Who Must Comply? ....................................... 108
      2.5.2.3 How To Comply? ......................................... 108
      2.5.2.4 Sanctions and Remedies ................................. 109
    2.5.3 Wireless Network Security ................................... 109
      2.5.3.1 Who and What Data Is Protected? ......................... 109
      2.5.3.2 Who Must Comply? ....................................... 109
      2.5.3.3 How To Comply? ......................................... 110
      2.5.3.4 Sanctions and Remedies ................................. 110
2.5.4 Social Security Numbers .................................................. 110
  2.5.4.1 General Restrictions ............................................. 111
  2.5.4.2 Social Security Number Truncation on Pay Stubs .......... 113
2.5.5 Automated License Plate Recognition Systems ................. 113
  2.5.5.1 Who and What Data Is Protected? .............................. 114
  2.5.5.2 Who Must Comply? .............................................. 114
  2.5.5.3 How To Comply? ................................................. 114
  2.5.5.4 Sanctions and Remedies ........................................ 116
2.5.6 Student Online Personal Information .............................. 116
2.5.7 Payment Card Industry Security Standards ..................... 117
2.5.8 Cybersecurity ............................................................. 117
2.5.9 Data Security by Design—Requirements for Product Manufacturers ........................................ 118
2.5.10 Computer Interference Laws ........................................ 120
  2.5.10.1 Computer Fraud and Abuse Act (CFAA) .................... 122
  2.5.10.2 California Comprehensive Computer Data Access and Fraud Act (CCDAFA) .................... 125
2.6 Employee Privacy .............................................................. 134
  2.6.1 Overview—Workplace Privacy in General ....................... 135
  2.6.2 California Labor Code Section 226 ............................... 138
    2.6.2.1 Who and What Data Is Protected? ......................... 139
    2.6.2.2 Who Must Comply? ........................................... 139
    2.6.2.3 How To Comply? ............................................. 140
    2.6.2.4 Sanctions and Remedies ................................... 140
  2.6.3 California Labor Code Section 435 ............................... 141
    2.6.3.1 Who and What Data Is Protected? ......................... 141
    2.6.3.2 Who Must Comply? ........................................... 141
    2.6.3.3 How To Comply? ............................................. 141
    2.6.3.4 Sanction and Remedies ................................... 141
  2.6.4 California Labor Code Section 980 ............................... 142
    2.6.4.1 Who and What Data Is Protected? ......................... 142
    2.6.4.2 Who Must Comply? ........................................... 143
Contents

2.6.4.3 How To Comply? .................................................143
2.6.4.4 Sanctions and Remedies .......................................143
2.6.5 Other Laws Specifically Addressing Employers ...............143
2.6.5.1 California Labor Code Section 1026 ................................143
2.6.5.2 ID Device Implants—California Civil Code Section 52.7 ....144
2.6.5.3 Background Checks—Fair Credit Reporting Act ...............144
2.6.5.4 Health Information ..............................................144
2.6.5.5 Polygraphs .....................................................144
2.6.5.6 Subpoenas .....................................................144
2.6.5.7 Anti-Discrimination Laws .....................................144
2.6.5.8 California Consumer Privacy Act (CCPA) .....................146

2.7 Financial Information ..................................................147
2.7.1 Gramm-Leach-Bliley Act ...........................................148
  2.7.1.1 Who and What Data Is Protected? ..................149
  2.7.1.2 Who Must Comply? ..................................150
  2.7.1.3 How To Comply? ..................................150
  2.7.1.4 Sanctions and Remedies ...............................151
2.7.2 California Financial Information Privacy Act .................152
  2.7.2.1 Who and What Data Is Protected? ..................153
  2.7.2.2 Who Must Comply? ..................................154
  2.7.2.3 How To Comply? ..................................154
  2.7.2.4 Sanctions and Remedies ...............................156
2.7.3 Consumer Reports, Background Checks—
  Federal Fair Credit Reporting Act ...............................156
  2.7.3.1 Who and What Data Is Protected? ..................157
  2.7.3.2 Who Must Comply? ..................................157
  2.7.3.3 How To Comply? ..................................158
  2.7.3.4 Sanctions and Remedies ...............................160
2.7.4 Consumer Reports, Background Checks—
  California Consumer Credit Reporting Agencies Act ............162
  2.7.4.1 Who and What Data Is Protected? ..................163
  2.7.4.2 Who Must Comply? ..................................163
Contents

2.7.14 Payment Card Industry Standards ........................................... 193

2.8 Government ................................................................................. 193

2.8.1 Federal Statutes ......................................................................... 194

2.8.2 California Statutes ..................................................................... 198

2.9 Health and Medical Information .................................................. 201

2.9.1 Health Insurance Portability and Accountability Act ................. 201

2.9.1.1 Who and What Data Is Protected? ........................................ 202

2.9.1.2 Who Must Comply? .............................................................. 203

2.9.1.3 How To Comply? ................................................................. 203

2.9.1.4 Sanctions and Remedies ....................................................... 208

2.9.2 California Confidentiality of Medical Information Act .............. 211

2.9.2.1 Who and What Data Is Protected? ........................................ 211

2.9.2.2 Who Must Comply? .............................................................. 212

2.9.2.3 How To Comply? ................................................................. 214

2.9.2.4 Sanctions and Remedies ....................................................... 215

2.9.3 Genetic Information Nondiscrimination Act ............................... 218

2.9.3.1 Who and What Data Is Protected? ........................................ 218

2.9.3.2 Who Must Comply? .............................................................. 218

2.9.3.3 How To Comply? ................................................................. 219

2.9.3.4 Sanctions and Remedies ....................................................... 220

2.9.4 California Genetic Information Privacy Act ............................... 221

2.9.4.1 Who and What Data Is Protected? ........................................ 222

2.9.4.2 Who Must Comply? .............................................................. 222

2.9.4.3 How To Comply? ................................................................. 223

2.9.4.4 Sanctions and Remedies ....................................................... 224

2.9.5 Other Health Information Privacy Laws .................................... 225

2.9.5.1 Collection of Medical Information for Direct Marketing Purposes ........................................................................... 225

2.9.5.2 California Shine the Light Law .............................................. 225

2.9.5.3 California Health and Safety Code ...................................... 225

2.9.5.4 Records Maintained by State Agencies ................................. 226

2.9.5.5 Welfare and Institutions Code .............................................. 226
# Contents

2.13.3.3 How To Comply? ........................................ 254  
2.13.3.4 Sanctions and Remedies ............................. 254  
2.13.4 Rental Car Surveillance ................................. 255  
  2.13.4.1 Who and What Data Is Protected? ................. 255  
  2.13.4.2 Who Must Comply? ................................ 255  
  2.13.4.3 How To Comply? ................................... 255  
  2.13.4.4 Sanctions and Remedies ............................ 256  
2.14 Mail .......................................................... 256  
2.15 Notification of Data Security Breaches .................. 258  
  2.15.1 General California Data Security Breach  
     Notification Requirement .................................. 258  
     2.15.1.1 Who and What Data Is Protected? ............... 258  
     2.15.1.2 Who Must Comply? ................................ 259  
     2.15.1.3 How To Comply? ................................... 260  
     2.15.1.4 Sanctions and Remedies ............................ 266  
  2.15.2 Data Breach Notification Requirements Under Other Laws  
     .............................................................. 268  
2.16 Online Privacy ............................................. 271  
  2.16.1 Telecommunications Carriers ....................... 271  
     2.16.1.1 Who and What Data Is Protected? ............... 272  
     2.16.1.2 Who Must Comply? ................................ 272  
     2.16.1.3 How To Comply? ................................... 272  
     2.16.1.4 Sanctions and Remedies ............................ 273  
  2.16.2 Children’s Online Privacy Protection Act ........ 273  
     2.16.2.1 Who and What Data Is Protected? ............... 273  
     2.16.2.2 Who Must Comply? ................................ 274  
     2.16.2.3 How To Comply? ................................... 276  
     2.16.2.4 Sanctions and Remedies ............................ 278  
  2.16.3 California Online Privacy Protection Act .......... 279  
     2.16.3.1 Who and What Data Is Protected? ............... 279  
     2.16.3.2 Who Must Comply? ................................ 280  
     2.16.3.3 How To Comply? ................................... 282  
     2.16.3.4 Sanctions and Remedies ............................ 284
2.19.6.9 California Law on Collection of License Plate Information ...........................................315
2.19.6.10 Guest and Passenger Records .................................................................316

2.20 Supermarket Club Cards .................................................................316
2.20.1 Who and What Data Is Protected? ............................................................316
2.20.2 Who Must Comply? ........................................................................316
2.20.3 How To Comply? ...........................................................................317
2.20.4 Sanctions and Remedies .................................................................317

2.21 Torts ...............................................................................................317
2.21.1 Who and What Data Is Protected? ............................................................318
2.21.1.1 Intrusion Upon Seclusion .................................................................318
2.21.1.2 Public Disclosure of Private Facts ........................................319
2.21.1.3 False Light ................................................................................319
2.21.1.4 Right to Publicity ..................................................................320
2.21.1.5 Stalking and Other Invasions of Privacy .............................................322
2.21.2 Who Must Comply? .................................................................322
2.21.3 How To Comply? .................................................................323
2.21.4 Sanctions and Remedies .................................................................323

2.22 Unsolicited Marketing Communications .................................................................324
2.22.1 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 .................................................................326
2.22.1.1 Who and What Data Is Protected? ............................................................326
2.22.1.2 Who Must Comply? ........................................................................327
2.22.1.3 How To Comply? ...........................................................................327
2.22.1.4 Sanctions and Remedies .................................................................330
2.22.2 California Anti-Spam Law .................................................................332
2.22.2.1 Who and What Data Is Protected? ............................................................334
2.22.2.2 Who Must Comply? ........................................................................334
2.22.2.3 How To Comply? ...........................................................................335
2.22.2.4 Sanctions and Remedies .................................................................336
2.22.3 Telephone Consumer Protection Act .................................................................337
2.22.3.1 Who and What Data Is Protected? ............................................................340
2.23.2 Reader Privacy Act.............................................358
  2.23.2.1 Who and What Data Is Protected? ....................359
  2.23.2.2 Who Must Comply? ....................................359
  2.23.2.3 How To Comply? .......................................359
  2.23.2.4 Sanctions and Remedies ...............................360

2.23.3 Connected Television .....................................360
  2.23.3.1 Who and What Data Is Protected? ....................361
  2.23.3.2 Who Must Comply? ....................................361
  2.23.3.3 How To Comply? .......................................361
  2.23.3.4 Sanctions and Remedies ...............................362

2.23.4 Other Laws ..................................................362

2.24 Wiretapping, Eavesdropping and Communications Privacy ..........363
  2.24.1 The Federal Electronic Communications Privacy Act ..........364
    2.24.1.1 Who and What Data Is Protected? ....................364
    2.24.1.2 Who Must Comply? ....................................365
    2.24.1.3 How To Comply? .......................................365
    2.24.1.4 Sanctions and Remedies ...............................370
  2.24.2 The California Invasion of Privacy Act ....................371
    2.24.2.1 Who and What Data Is Protected? ....................373
    2.24.2.2 Who Must Comply? ....................................373
    2.24.2.3 How To Comply? .......................................373
    2.24.2.4 Sanctions and Remedies ...............................374
  2.24.3 California Telecommunications Customer Privacy .............375
    2.24.3.1 Who and What Data Is Protected? ....................375
    2.24.3.2 Who Must Comply? ....................................376
    2.24.3.3 How To Comply? .......................................376
    2.24.3.4 Sanctions and Remedies ...............................376
  2.24.4 Skimming Radio-Frequency Identification ....................376
  2.24.5 Electronic Eavesdropping by State Law Enforcement Officials ..377
  2.24.6 The California Electronic Communications Privacy Act ..........377
  2.24.7 Information on Lawful Abortions ...........................378
Contents

2.25 XXX — Revenge Porn ............................................ 378
  2.25.1 Who and What Data Is Protected? .......................... 379
  2.25.2 Who Must Comply? .......................................... 380
  2.25.3 How To Comply? ............................................ 380
  2.25.4 Sanctions and Remedies .................................... 380
2.26 Your Privacy Rights—Shine the Light ............................ 383
  2.26.1 Who and What Data Is Protected? .......................... 384
  2.26.2 Who Must Comply? .......................................... 384
  2.26.3 How To Comply? ............................................ 384
  2.26.4 Sanctions and Remedies .................................... 385
2.27 Paparazzi Laws .................................................... 386
  2.27.1 Intrusion into Seclusion by Paparazzi ...................... 387
    2.27.1.1 Who and What Data Is Protected? .................... 387
    2.27.1.2 Who Must Comply? .................................... 388
    2.27.1.3 How To Comply? ....................................... 388
    2.27.1.4 Sanctions and Remedies .............................. 389
  2.27.2 California Criminal Paparazzi Law ......................... 389
    2.27.2.1 Who and What Data Is Protected? .................... 389
    2.27.2.2 Who Must Comply? .................................... 389
    2.27.2.3 How To Comply? ....................................... 390
    2.27.2.4 Sanctions and Remedies .............................. 390

Chapter 3: Compliance Guide
3.1 Chapter Overview .................................................. 391
3.2 Starting a Compliance Program .................................. 391
3.3 Taking Charge .................................................... 391
3.4 Mobilizing Resources ............................................. 393
3.5 Appointing a Privacy Officer .................................... 396
3.6 Preparing a Task List ............................................ 397
3.7 Taking Inventory of Data ......................................... 399
3.8 Defining Objectives and Priorities ............................... 400
3.9 Finding the Best Approach for a Particular Organization .... 400
3.10 Identifying Legal and Other Requirements ..............................................402
3.11 Executing Tasks ..................................................................................402
3.12 Automation ........................................................................................403
3.13 Maintenance .....................................................................................404

Chapter 4: Drafting a Privacy Policy
4.1 Chapter Overview ....................................................................................407
4.2 Drafting Considerations In General .......................................................407
   4.2.1 Why Are You Creating the Document? .........................................408
   4.2.2 Who Is Your Audience? .................................................................410
   4.2.3 Policies Versus Other Documentation ........................................412
4.3 Privacy Notices and Policies in General ..............................................419
   4.3.1 Who Should Issue Notices: Service Provider or Customer? ........419
6.3.2 Which Topics Do Companies Typically Have to Address? ............420
      4.3.2.1 Who Is Issuing the Notice? ......................................................421
      4.3.2.2 What Is the Scope of the Notice and to Whom Is the Notice Addressed? 421
      4.3.2.3 What Categories of Data Does the Company Collect? ..........422
      4.3.2.4 For What Purposes Does the Company Collect Data and What Does the Company Do With It? 422
      4.3.2.5 To Whom Does the Company Disclose Data? .......................423
   4.3.3 Which Topics Should a Company Not Address? ..........................423
   4.3.4 Form and Delivery Requirements ................................................425
4.4 Privacy Policies for Websites, Apps and Other Online Services ........426
   4.4.1 Applicable Laws ........................................................................426
   4.4.2 Combined or Multiple Notices to Satisfy Different Laws. ............430
   4.4.3 Personal Data Transferred From Business to Business ..........432
   4.4.4 Notice Contents ........................................................................433
      4.4.4.1 Data Categories ................................................................434
      4.4.4.2 Third Party Data Sharing ......................................................436
      4.4.4.3 Data Access and Update Process ......................................443
      4.4.4.4 Changes ........................................................................443
      4.4.4.5 Effective Date ................................................................445
4.4.4.6 Response to Do Not Track Signals ................................. 446
4.4.4.7 Cookies and Tracking Pixels ........................................ 448
4.4.4.8 Data Security .......................................................... 449
4.4.5 Style and Organization ................................................... 453
4.4.6 Notice Placement .......................................................... 456
4.5 Privacy Notices for Callers .................................................. 459
4.6 Privacy Notices for Employees ............................................. 460
4.7 Opt-out Notices for Direct Marketing Communications ............... 464
4.8 Privacy Notices under the California Consumer Privacy Act ......... 465
  4.8.1 Updates, Supplements or Separate Stand-Alone Notices? ....... 465
  4.8.2 Disclosure Requirements under the California Consumer Privacy Act (CCPA) ........................................ 466
  4.8.3 Disclosures Required for Companies That Sell or Share Personal Information ........................................... 468
  4.8.4 Disclosures Regarding Sensitive Personal Information .......... 469
4.9 Other Privacy Policies and Notices ........................................ 469

Chapter 5: Drafting Other Privacy Documentation

5.1 Chapter Overview ............................................................ 471
5.2 Consent ........................................................................ 471
  5.2.1 When To Seek and Not To Seek Consent ......................... 471
  5.2.2 How To Obtain Valid Consent ....................................... 475
  5.2.3 Opt-In, -Out, and In-Between ..................................... 478
    5.2.3.1 Examples of Consent Mechanisms .......................... 478
    5.2.3.2 Minimum Requirements ...................................... 481
    5.2.3.3 Selecting Implementation Options ......................... 481
    5.2.3.4 Silence As Consent ........................................... 481
    5.2.3.5 Affirmative, Express Consent .............................. 482
  5.2.4 Above and Beyond Opt-In Consent ................................ 483
  5.2.5 Other Considerations for Consent Drafting ....................... 485
    5.2.5.1 Incorporation of Notices into Consent Declarations ...... 485
    5.2.5.2 Expressing Focused Consent ................................ 486
    5.2.5.3 Placement of Consent Mechanism and Declaration ...... 487
5.2.5.4 Who Should Obtain Consent—
Data Controller or Processor? ............................... 487
5.3 Agreements ........................................................ 488
  5.3.1 Agreements With Data Subjects Versus Consent
      From Data Subjects ............................................. 489
  5.3.2 Asking for an Express Acceptance of Website
      Privacy Statements or General Privacy Notices ........... 489
  5.3.3 Agreements Instead of Consent ........................... 491
  5.3.4 Commercial Agreements Between Companies .............. 492
  5.3.5 Terms for Data Processing Services Agreements .......... 494
  5.3.6 Terms for Data Subprocessing Agreements ............... 495
  5.3.7 Terms for Agreements Between Data Controllers ........ 496
  5.3.8 Terms Dictated by Laws and Compliance Agendas ....... 496
5.4 Protocols .......................................................... 497
  5.4.1 Direct Communications Protocol ......................... 499
  5.4.2 Data Protection Protocol for Internet-of-Things
      Product Development ............................................ 502
5.5 Questionnaires and Data Submission Forms ...................... 503
5.6 Documenting Decisions and Compliance Efforts ................ 505
5.7 Assessments ........................................................ 506

Chapter 6: Enforcement

6.1 Chapter Overview ................................................ 507
6.2 Enforcement of Privacy Laws through Private Civil Litigation ........ 507
  6.2.1 Causes of Action ........................................... 507
    6.2.1.1 Common Law ........................................... 508
    6.2.1.2 Privacy Statutes ........................................ 515
    6.2.1.3 Unfair Competition Law ............................... 518
    6.2.1.4 Unjust Enrichment, Restitution, Other Causes of
            Action and Remedies ...................................... 527
  6.2.2 Special Issues in Privacy Litigation ....................... 527
    6.2.2.1 Article III Standing ................................... 528
    6.2.2.2 California Standing Requirements ..................... 538
6.2.2.3 Class Action Litigation ........................................... 539
6.2.2.4 Litigation Privilege Issues .................................... 549
6.2.3 Jurisdiction in Privacy Litigation ............................. 550
   6.2.3.1 Subject Matter Jurisdiction .............................. 550
   6.2.3.2 Personal Jurisdiction .......................... 551
6.3 Enforcement of Privacy Laws by Government Agencies ...... 556
   6.3.1 Federal Trade Commission Enforcement Actions ....... 556
   6.3.2 California Attorney General Enforcement Actions ....... 563
6.4 Enforcement of Privacy Laws in Criminal Proceedings ....... 571
   6.4.1 Criminal Prosecution ....................................... 572
   6.4.2 Privacy for Criminal Defendants .......................... 573
      6.4.2.1 Suppression Remedy .................................. 574
      6.4.2.2 Statutory Remedy ..................................... 575
6.5 Enforcement Against Online Service Providers ............... 575
   6.5.1 Contributory Liability and Immunities of
   Online Services Providers ......................................... 576
   6.5.2 Demands for Identity Information ......................... 580

Chapter 7: Risk Mitigation

7.1 Chapter Overview .................................................. 583
7.2 Compliance Program .............................................. 583
   7.2.1 Formal Program ............................................. 583
   7.2.2 Compliance Checklist ........................................ 584
      7.2.2.1 Who Is in Charge of Data Privacy and
      Security Compliance in the Organization? ................. 584
      7.2.2.2 Are All Stakeholders Instructed and
      Trained Regarding Their Responsibilities? ................. 585
      7.2.2.3 Are You Doing Enough To Keep Data Secure? ....... 585
      7.2.2.4 Have All Data Subjects Received Appropriate Notices and
      Granted Consent Where Required? Are All Notice and
      Consent Forms Accurate and Up-to-Date? .................... 586
      7.2.2.5 Are Your Marketing Activities in Compliance with
      Applicable Law? .................................................. 586
7.2.2.6 Do You Design Products, Processes and Standard Contracts to Allow or Facilitate Compliance with Data Privacy and Security Requirements by Your Employees, Customers and Product Users? .................587

7.2.2.7 Are You Collecting or Retaining More Data than You Need? ..587

7.2.2.8 Are You “Selling” or “Sharing” Personal Information, or “Using Sensitive Personal Information” under the CCPA? . . . .588

7.2.3 Maintenance .........................................................588

7.3 Due Diligence and Audits ...............................................588

7.3.1 Due Diligence in Mergers and Acquisitions (M&A) Scenarios ..............................................589

7.3.2 Due Diligence Questions to Ask ..................................591

7.3.3 Due Diligence Regarding Service Providers and Vendors ..................................................592

7.4 Risk Mitigation via Contracts ........................................592

7.5 Insurance ................................................................593

Table of Cases ..................................................................595

Index ............................................................................625
Foreword

by Paul M. Schwartz

We are all California privacy lawyers or soon will be. California is the state with the largest economy in the United States. Were it an independent country, it would rank as the fourth-largest economy in the world. For companies within the United States and participants in the global digital economy, commercial transactions with California residents are a “must.” As a consequence, all privacy lawyers must be aware of the complex web of privacy and security regulations in the Golden State. Their advice to clients must be based on solid knowledge of California privacy law.

Beyond the economic significance of this state, there is a further and more subtle reason why California privacy law is important. It is due to the role of the “California Effect,” which is a concept that refers to the role of California in setting a national privacy policy agenda.

Data breach notification legislation provides an initial example of the California Effect. Since California enacted the first data breach statute in 2002, all other states have now passed such legislation. In the HITECH Act of 2009, moreover, federal lawmakers required notification for leaks of health care information that falls under the jurisdiction of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Data breach notification is an idea from California that has swept the nation.

California privacy policy innovations have also had a global impact. In the European Union, the European Commission adopted a regulation in June 2013 establishing a data breach notification obligation for telecommunication companies and internet service
providers.1 More broadly, the General Data Protection Regulation of 2016, which took effect in May 2018, requires data controllers to notify supervisory authorities of data breaches and, in some instances, to inform the parties whose data is leaked.2 As for the rest of the world, according to one estimate, one-third of nations in the Asia-Pacific region have adopted a data breach notification requirement.3

More recently, California has enacted and amended the California Consumer Privacy Act (CCPA). In the words of Lothar Determann, this law “broke with the U.S. tradition of narrowly crafted, harm-based, sector- and situation-specific privacy laws and moved in the direction of omnibus regulation of data processing.” California has taken a decisive step in changing the national conversation around information privacy regulation. As Anupam Chander and co-authors have noted, this law has served as a decisive catalyst for other states.5 In their view, California privacy law represents the efforts of individual norm entrepreneurs who have harnessed the state legislative process to produce the CCPA, which, in turn, has exercised a strong influence of this model on other states.6

During the current era of gridlock in Washington, the role of California is more important than ever. Until recently, the California Effect served as the first part of a regulatory cycle. Typically, after legislative action in this state and perhaps other ones, regulated entities would seek relief through a “flight to Washington.”7 Congress would respond to developments at the state level with laws that, at their best, consolidated, corrected, and improved the initial state efforts at regulation.

5 Anupam Chander et al., Catalyzing Privacy Law, 105 Minn. L. Rev. 1733 (2021).
6 Anupam Chander et al., Catalyzing Privacy Law, 105 Minn. L. Rev. 1733, 1781 (2021).
7 For the classic description of this process, see E. Donald Elliott, Bruce A. Ackerman & John C. Millian, Toward a Theory of Statutory Evolution: The Federalization of Environmental Law, 1. J.L. Econ. & Org. 313 (1985).
Today, however, there is entrenched gridlock in Washington for privacy and other policy areas. Congress is setting new records for its lack of productivity and struggling to carry out the most basic tasks, including, at times, the task of enacting a federal budget. Congress has also been largely silent on the privacy front. Thus, the traditional federal-state cycle for privacy legislation is missing a necessary component due to the general lack of federal inputs into the legislative process. In face of this lack of activity in D.C., state privacy law, in general, and the California Effect, in particular, are more important than ever. In turn, the California legislature has proven eager and able to enact new legislation. As Determann’s *California Privacy Law* demonstrates, the resulting legal approach in the Golden State is both highly complex and notably different from European Union law, which has established the template for most of the rest of the world outside of the United States.

In California and elsewhere in the United States, information privacy law traditionally consisted of a patchwork of sectoral privacy laws. A sectoral law, whether state or federal, typically regulates only a narrow area of the use of personal data processing. The game changer in this regard has been the CCPA, which took effect in 2020. This new California law represents a significant movement towards a European-style “omnibus” privacy statute – at least in certain regards. And, as noted above, this statute already is playing a strong role in catalyzing and influencing other state privacy laws.8

The CCPA broadens the typical approach of federal and state privacy law. It extends the classic sectoral orientation of the United States by reaching more entities than the typical sectoral law and by expanding the set of required fair information practices. It regulates personal information use by for-profit businesses that satisfy one or more of an enumerated threshold list. Its jurisdictional triggers look to whether a company has gross revenues over $25 million; buys, sells, or shares the information of 100,000 or more consumers; or derives 50 percent

---

8 Anupam Chander et al., Catalyzing Privacy Law, 105 Minn. L. Rev. 1733 (2021).
or more of annual revenues through the sale or sharing of personal information.

The CCPA also guarantees an expanded range of consumer rights compared to a typical U.S. privacy law or the preceding regulations in California or other states. Under the CCPA, a consumer has legal rights to access and correct her information; to “port” personal information from one company to another; and to opt-out from processing and from the sale of her personal information. The CCPA also guarantees a right to deletion, subject to certain exceptions, of the personal information that a business stores on a consumer. Further, it prohibits a business from discriminating against a consumer who exercises her rights under the law. The CCPA provides protection for children’s information by prohibiting the selling of personal information of a consumer who is under 16 years of age without consent. Finally, the definition of “personal information” in the CCPA is quite broad—indeed, it reaches more data than even the GDPR.

One of the most important aspects of the CCPA is how it navigates the complicated terrain between anti-discrimination provisions and the permissibility of data sale. The CCPA generally prohibits discrimination against California residents who exercise their interests under the statute, including their rights of access, data erasure and data portability. But regulated companies may provide a different price, rate or quality in their services to a consumer when the difference is reasonably related to the value of a consumer’s data.9 Regulations are currently being formulated to provide guidelines as to when such data trades meet this test. In this area, California is in advance of the GDPR and European law in structuring a privacy-promotive framework for data trade.

As for private rights of action, the CCPA permits this kind of enforcement only as regards its data breach provisions. The CCPA gives the essential role for enforcement to both the California Attorney General and a new entity, the California Privacy Protection Agency. As Determann explains, the California Attorney General has the power to bring civil enforcement actions in court, and the CPPA to bring administrative enforcement actions.10 The law permits significant

---

9 Lothar Determann, California Privacy Law, Chapter 2 §2-4.2.5 (4th ed. 2023).
civil enforcement penalties of up to $2,500 for each violation and up to $7,500 “for each intentional violation.” The CCPA also permits regulated entities to request an attorney general opinion on CCPA compliance.

In Determann’s view, this law places considerable new burdens on businesses. He observes that in its aftermath businesses face a California law that combines the worst aspects of EU and U.S. regulatory approaches; he points to “extremely broad regulation of data processing in the CCPA plus myriad sector-, situation- and harm-specific privacy laws, which overlap with the CCPA.”11 Adding to the high stakes, regulations for the CCPA are still being finalized.

III

A further compliance risk in the United States is that the sheer complexity and volume of different statutes, federal and state, will overwhelm even the most determined privacy lawyer. Determann’s California Privacy Law proves indispensable in navigating this difficult landscape through the depth and clarity of its coverage. Determann carefully reviews California’s requirements for data security, location tracking, online privacy, and, of course, data breach notification. He explains the state’s anti-paparazzi laws and its “Shine the Light” law, which requires mandatory disclosures to consumers when businesses transfer consumer information to third parties for direct marketing purposes.

As a further matter, understanding California law requires setting it in the context of federal law. One of the strongest aspects of Determann’s California Privacy Law is its seamless integration of federal and California privacy law. In myriad areas, it proves impossible to understand one without the other. Health care and financial privacy law alike demonstrate why such an integrated analysis is indispensable. HIPAA, the federal regulation for health care privacy, places numerous obligations on “covered entities,” which include health plan operators, health care providers, employers who operate health insurance plans, and many other parties who have access to electronic health care insurance. HIPAA does not preempt stricter state laws, however, and

California’s Confidentiality of Medical Information Act (CMIA), which predates HIPAA by over a decade, is one such statute. CMIA also extends far more broadly than HIPAA; it covers “[a]ny business that offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information” as a “provider of health care.”12 This state health care privacy statute contains specific requirements for employee health information, as well as detailed obligations for valid authorization for disclosure of health information, including typeface-size requirements.

A similar interplay occurs between federal and state law for financial privacy. At the federal level, the Gramm-Leach-Bliley Act (GLBA) regulates the use by “financial institutions” of the “nonpublic personal information” of consumers. It does not generally preempt state laws that provide greater privacy protection, and California’s Financial Privacy Act (FIPA) does have stricter requirements in certain areas. Unlike the federal law, for example, FIPA requires opt-out notices before information sharing with affiliated institutions. As in California’s CMIA, FIPA also contains highly specific requirements for the mandated forms in which information is to be provided to consumers.

Determann’s California Privacy Law also provides a host of practical suggestions regarding privacy compliance; the drafting of policy policies and other privacy documentation; and achieving risk mitigation. One of the most interesting aspects of the compliance section of this book is the author’s perceptive analysis of consent issues. Pursuant to both Californian and federal statutes, the consent of affected parties is needed before certain specific kinds of personal data use. Under other laws, consent is optional but can release a company from extensive disclosure requirements. Determann points out both the benefits of obtaining consent and the possible risks of such a seemingly risk-averse policy.13 As he notes, consent, once obtained, must be documented and may require authentication steps regarding the identity of the party from whom consent is sought.14 But there can be considerable costs to obtaining consent where it is not strictly required by law. An existing business relationship may be disrupted

12 Cal. Civ. Code § 56.06(b).
if consent is sought. Seeking consent may require development of a process to seek new or additional consent should the terms of processing change.

IV

Privacy lawyers are well advised to keep an eye on developments in Sacramento, the California state capital. Determann’s *California Privacy Law* provides peerless assistance in doing so; it is a tour-de-force guide to the most important state privacy law in the world. It also provides a host of practical advice through dos and don’ts regarding a broad range of compliance issues. Privacy lawyers and practitioners are fortunate to have this up-to-date treasure of insight and advice.

Paul M. Schwartz
*Jefferson E. Peyser Professor of Law*
*Berkeley Law School*
About This Book

In late 2013, I embarked on a new book project, based on suggestions from the publishers of The Recorder (www.therecorder.com), who liked my previously published Field Guide to International Data Privacy Law and asked me to write “a California version.” I was immediately enthusiastic about. The plan and received much encouragement from colleagues, including Chris Hoofnagle at the Berkeley School of Law. As a practitioner, I had been looking for such a book myself and knew how increasingly difficult companies and their counsel have found it to get by without good comprehensive coverage of California and U.S. federal privacy laws. I vaguely knew then that I was in for a lot of work, given the proliferation of privacy-related legislation in California. But, it was not until a few months later, after I had taken inventory of all the relevant laws, that I realized what I was in for. And I knew I needed help.

Luckily, I found enthusiastic and talented volunteers to support my efforts in my current and former privacy law classes. It paid off that I have been teaching privacy law courses since 2003 at four law schools in the San Francisco Bay Area (and was the first to add a course on privacy law to the curriculum of three of these great law schools): University of California, Berkeley School of Law; University of California College of the Law, San Francisco (formally known as Hastings College of the Law); Stanford Law School; and the University of San Francisco School of Law. My research assistants have helped me gather statutes, legislative history, cases, and analyses. Many thanks to all of you! I could not have done this without you. As promised, you receive attribution in the “Acknowledgments” section of this book.

My thanks also go to the readers of the first four editions of this book. Thank you for your interest and feedback - and some of you, for contributing to this materially revised and updated 5th edition. Its original template - Determann’s Field Guide to Data Privacy Law - is
also available in its 5th edition in English, and twelve other language versions have been released by publishers in Argentina, Belgium, Brazil, China, Egypt, Germany, Hungary, Italy, Japan, Korea, Russia and Turkey.

As I was working on the new editions, I was amazed how much has changed in the privacy field in the last few years. For a compressed summary and a little fun, please check out Privacy Please at www.youtube.com/watch?v=7u0XNVHXzus.

If you have any comments, criticism, supplements, corrections, or other thoughts, please send them to me at lothar@gmail.com. I hope that practitioners will find this book helpful, that scholars or policymakers will find it interesting, and that other legal commentators can build on the materials in this book. I hope that there will be handbooks for other states’ privacy laws soon—let me know, please, if you would like to write one and if I can help.

Lothar Determann
October 12, 2022
About the Author

Lothar Determann practices and teaches international data privacy, commercial, and intellectual property law. He is admitted to the Bar in California and Germany and has practiced law at Baker & McKenzie LLP in San Francisco and Palo Alto, California since 1998. He teaches Computer Law, Data Privacy Law, and Electronic Commerce Law at the Freie Universität Berlin since 1994 and at the University of California, Berkeley School of Law since 2004. He has taught privacy law and other courses also at the University of California College of the Law, San Francisco (formally known as Hastings College of the Law - from 2010 to 2021), the University of San Francisco Law School (2000 to 2005) and at Stanford Law School (2011). He has authored more than 150 articles and five books, including Determann’s Field Guide to Data Privacy Law, 5th Edition, 2022, also available in Arabic, Chinese, French, German, Hungarian, Italian, Japanese, Korean, Portuguese, Russian, Spanish and Turkish.
Acknowledgments

The author is deeply grateful for valuable contributions from students and fellow scholars and practitioners. Specifically, the author thanks Dean Susan Freiwald, University of San Francisco (USF) School of Law, for her invaluable ongoing academic mentorship, as well as suggestions and edits for the first edition of this book; Natalie Nicol, J.D. 2014, UC Hastings College of the Law (UC Hastings), for research assistance and editing of the first edition; and Jessica Vapnek, Lecturer at UC Hastings College, for thoughtful suggestions and comprehensive editing of the fourth and fifth edition.

For contribution to the first edition, the author thanks Tod Gamlen, partner at Baker & McKenzie LLP, for input and suggestions regarding Chapter 6; Arianne Vanessa Josephine T. Jimenez, LL.M. 2014, J.S.D. Candidate 2016, Berkeley Law, for research assistance and editing; and Sean Hanley, PrivacyVille co-creator and UC Hastings Class of 2016, for input regarding Chapter 4; and the author also thanks a number of students from Bay Area law schools who volunteered as research assistants for the first edition, namely Rosalind Jane Schonwald, Ismael Andani Abdulai (Barrister-at-law and Solicitor of the Supreme Court of Ghana), Violaine Brunet, François Joli-Coeur, Togzhan Ibrayeva, Jonathan Unikowski, and Austin Whitney at Berkeley Law; Timothy Yim (Director of Data & Privacy, Startup Policy Lab), Hannah M. Strain, Gabriel Nevin, Jasmine A. Braxton, Melis Atalay, Eric Whitehead, Tylor S. Dominguez, Jennifer Hardin, and Paige Pembrook at UC Hastings; and Jana Juricova, Michael Martinez, Noah S. Johnson, Winston Hu, Jin Ho, Rahul Devnani, Karl Uhlig, and Kacee Taylor at the USF School of Law.

For contributions to the second edition, the author thanks Bethany Lewis, CIPP/US, CIPP/E, Privacy Project Manager, The Nielsen Company, for comprehensive review and edits; Matt Tonner, Attorney, Turn Inc.; Grace Cheong, UC Hastings; Ary Jaramillo, Berkeley Law; and Winston Hu and Rahul Devnani, USF School of Law.
For contributions to the third edition, the author thanks Hank Dempsey, Chief Consultant, Assembly Privacy and Consumer Protection Committee; Julia R. Weisner, JD, Health Center Counsel and Compliance Director, LifeLong Medical Care; Amiee Lee, JD Candidate, USF School of Law; Jon Neiditz, Kilpatrick Townsend & Stockton, Atlanta; and the 2017 California Privacy Law class at UC Hastings, particularly Huong Chu-Nguyen (also for the portrait on the book’s back cover); Sam Micon; Felipe Pereira; Daniel Stefanic; Sarah Glendon; and Camille Savary.

For contributions to the fourth edition, the author thanks Jessica Vapnek, Lecturer at UC Hastings; Ed Totino and Jonathan Tam, Baker McKenzie; Lauren Kitces, Squire Patton Boggs; Hank Dempsey, Head of Public Policy - California at Snap Inc.; Dominique Shelton Leipzig and Amanda Mobrand, Perkins Coie; Prof. Linsey Krolik, Santa Clara University School of Law and Senior Director, Privacy Counsel at Bill.com; Ardi Kolah; Alex D’Amico, Morrison Mahoney LLP; Jose Antonio Sesin, Sr. Counsel, Corporate, Privacy and Security at Agero, Inc.; Irene Jan, Attorney, CIPP/US, CIPM, CIPT; Christopher O’Connor; Deepali V. Lugani, Attorney, CIPP/US; and the author’s students in the 2020 California Privacy Law Workshop at UC Hastings, in particular Katrina Eckert, Caroline Sir, Alexis M. Lazzeri, Dantam Le, Amy Lucas, David Watson, Katarina Sivakova, Jose Vega Ruiz, Fred Feyzi, Taylor Galusha, Andrew Klair, Ciara Clement and Michael Winton.

For contributions to the fifth edition, the author thanks Jessica Vapnek, Lecturer at the University of California College of the Law, San Francisco; Hank Dempsey, Head of Public Policy - US States at Snap Inc. and Environmental Planning Commissioner, City of Mountain View; Jonathan Tam, Partner at Baker McKenzie; Tom Tysowsky, Associate at Baker McKenzie; Lauren Kitces, Senior Managing Associate at Sidley Austin LLP; Grayson Myers, Summer Associate at Baker McKenzie; Julian Schneider, Data Protection and Privacy Analyst, HewardMills; and my students at the University of California, Berkeley School of Law, including Maxime Perez, Gary Lee, Suriti Chowdhary, Kiana Harkema, Vasundhara Majithia, Debora Fiore de Barros, Ryota Asakura, Yuki Kondo, Yue Lu, Elias Garcia, Julia Bront, Sho Ito, Justin Fan and Vartika Goyal.

The author takes sole responsibility for any errors and omissions.
Readers’ Feedback Regarding Prior Editions of This Book

This handbook is essential for any company doing business in California. From simple-to-read summaries on the law to tips on setting up a data privacy compliance program, Lothar Determann’s *California Privacy Law* has everything you need to know as in-house counsel to comply with the privacy laws in California. A must-have reference book for any legal department.

**Patricia Timm**  
*General Counsel, SugarCRM*

Determann’s new guide to privacy law in California is a most useful tool that covers an important topic in a comprehensive way. It is written in understandable language, can be digested without prior knowledge of the subject, and includes practical suggestions for selecting sensible privacy policies that are consistent with the circumstances of individual businesses. This is a book to have within an arm’s reach of anybody in California who is responsible for administering privacy policies.

**Charles H. Dick Jr.**  
*General Counsel of the San Diego County Bar Association*

California drives the law of privacy in the United States. Lothar Determann, an eminent practitioner and professor of privacy, computer, and software law, has written the definitive account of California policymakers’ weighty contribution to privacy law. Determann has assembled exactly what a lawyer needs to triage California privacy law topics. Each law’s rationale, scope, compliance requirements, and sanctions are covered. Each law is also annotated with the most important cases and with tradecraft for implementing the laws.
Comprehensive and detailed, this volume is more than just a hornbook of California privacy law. The work’s broad scope and approachable style makes it a great volume for anyone who is entering privacy practice and who wants more historical and international context for the law of privacy. The reader can learn from Determann’s substantial experience on how to draft a privacy policy, how to conceive of a privacy program, how to manage “consent,” and how to address privacy risk.

**Chris Jay Hoofnagle**  
*UC Berkeley Law*

I have been looking for a comprehensive book for a while now, and it looks like I found it! Thanks for saving us headache down the road.

**Mark Griffin**  
*J.D. Associate Director of Legal Projects, Robert Half Legal*

Congrats on the republication of this excellent work, which I’m certainly going to recommend to my colleagues and clients. I am deeply impressed with its comprehensiveness and practical advice.

**Jon Neiditz**  
*Kilpatrick Townsend & Stockton, Atlanta*
CHAPTER 1

California and U.S. Federal Privacy Law Overview

1.1 Chapter Overview
This book is intended to give businesses, attorneys, privacy officers and other professionals practical guidance on compliance requirements, rights and remedies under California and U.S. federal privacy law.

Companies that have to comply with California privacy law also have to comply with applicable U.S. federal privacy laws, because U.S. federal laws apply in California. The reverse statement (companies subject to U.S. federal law also have to comply with California law) would not be entirely accurate, but it would almost be so, given that most companies are doing or trying to do business in California or with California-based businesses or consumers, given the economic significance of the Golden State. As a result, most major U.S. and foreign companies are trying to comply with California privacy laws and use them as a benchmark, proxy or starting point for compliance with other U.S. laws for reasons further explained in this chapter.

This chapter also addresses the threshold questions of what California privacy law is, when California privacy law applies, who has to comply with California privacy law and how California privacy law relates to other privacy laws.

1.2 California
California is the largest of the 50 U.S. states by population (39.2 million people in 2022)¹ and the third largest by area (after Alaska and Texas). Its economy, the largest in the United States, is so vast that it is comparable to that of many countries. In 2021, the gross state

product (GSP) was about $3.4 trillion, larger than that of all but four countries—the United States, China, Japan and Germany—and ahead of the United Kingdom, France, India, Italy, Brazil, Canada, Korea, Russia, Australia, Spain and Mexico.2

California is diverse and extreme. It has the largest non-white population in the United States, making up 60 percent of the state population. More than 200 languages are spoken and read in California, including more than 100 indigenous languages, making California one of the most linguistically diverse areas in the world.3 California has the highest mountain and the lowest point in the contiguous United States.4 California has the oldest trees on the planet and the latest technologies. The San Francisco Bay Area and Silicon Valley in Northern California are home to many of the world’s largest high-tech corporations, as well as thousands of tech startup companies, many of which work on technologies and business models focused on personal data. Southern California, particularly Hollywood and Los Angeles, are centers of gravity for the film and music industries, as well as the media and paparazzi. The struggle between privacy and data commercialization is front and center in California; it is one of the state’s key dynamics. No surprise then that California is often first in the United States—and sometimes in the world—to adjudicate and legislate on privacy topics.5

The term “California Privacy Law” in the title of this book could have a number of different meanings. It could refer to laws enacted by the California state legislature. It could mean laws made in California (by California or federal government institutions, including regulatory agencies and courts situated on California territory). It could also mean laws applicable or enforceable in California—regardless of where or

by whom the laws are made. Before diving into the topic further, it is worth taking a closer look at these different meanings and angles, to better define the geographical focus of this book.

1.2.1 Laws Made by California vs. Federal Laws

The California government makes laws in its bicameral legislative body (called the “California state legislature” or “California legislature,” consisting of the State Assembly and State Senate), in its courts and in its regulatory agencies (such as the California Public Utilities Commission, which regulates privately owned telecommunications companies). Companies and individuals in California and elsewhere are subject to laws made by the California legislature. For example, companies in other U.S. states and in foreign countries participating in phone calls with persons in California have to comply with laws made in California that require all parties to a phone call to consent to recording.7

A company or consumer in California who wants to know what applicable law requires or what rights it provides cannot look only at laws made in California. This is because California companies and residents are also subject to U.S. federal laws made by the United States Congress in Washington, D.C., and interpreted by courts and agencies situated in California (as in other U.S. states and territories). Companies and consumers in California are also subject to the laws of other U.S. states and of other countries. For example, California companies that place web cookies on computers of Europeans who access websites hosted in California are subject to European laws that require prior consent to cookie placement.8

6 See www.legislature.ca.gov and www.senate.ca.gov.
7 See Kearney v. Salomon Smith Barney, Inc., 39 Cal. 4th 95, 119-21 (2006) (interpreting California statute prohibiting recording of telephone conversation without the consent of all parties to apply to a conversation between one party in California and another in Georgia).
8 See the applicable Directive (Directive on privacy and electronic communications) at 2002 O.J. (L 201) 37, available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN, and an opinion on the applicability of EU data protection laws by the Article 29 Working Group, which is comprised of representatives of the national data protection authorities in the European Union, the European Data Protection Supervisor and a representative of the European Commission (Opinion 8/2010 on applicable law
If one were to define the term “California law” to mean laws that apply to organizations and individuals in California, then “California law” would encompass many laws that are made outside of California. This book is focused on a narrower subset of “California law,” namely, laws made by the California legislature and California courts and agencies. That is how this text uses the term “California law.” Where it is necessary to refer to federal laws or decisions by federal courts in other U.S. states in order to understand laws made by California, this book will mention or summarize these. Even with this narrower focus, the number and scope of laws is too vast to cover in just one handbook, and so this book selects and uses key examples.

1.2.2 Scope and Applicability of California Law

California law applies to persons, companies, activities, things and places in California. Persons and companies in California have rights and obligations under California law with respect to activities and transactions taking place within the State of California. If and to what extent California law applies in cases involving more than one state or country, however, is not always clear. In particular, controversies regarding online privacy often concern multiple jurisdictions. Any company anywhere in the world that collects data from website visitors or mobile app users inevitably connects with some users in California, and needs to determine whether California law applies to its activities and what California law requires. To make this determination, one must identify what activities the California legislature intended to cover (by referring to general principles of statutory interpretation and conflict of law rules in each statute) and what the California legislature has jurisdiction to cover (by referring to jurisdictional limitations imposed by international and U.S. federal law). The following discussion looks first at limitations under international law and then U.S. federal law.

1.2.2.1 Limitations on California Jurisdiction
Under International Law

International law does not address or limit the applicability of California privacy law. As a matter of public international law, California privacy law may apply to companies and persons in other countries, and some California laws do, in fact, apply abroad.

The world is composed of territorial states or countries having separate and unique systems of laws. Historically, the exercise of jurisdiction by a country was limited to people, property and acts within its territory, and to relatively exceptional situations in which a country’s nationals traveled beyond its borders. The power of a country to make and enforce laws ended at its borders, and countries were thought to enjoy exclusive authority to regulate within their borders. As countries and societies opened up and engaged in more global commerce and communications, countries saw an increasing need to regulate activities originating in another country’s territory.

Today, most countries assume authority to regulate activities outside their borders. For example, the United Kingdom enacted the Bribery Act of 2010, which criminalizes the failure of commercial organizations to prevent bribery, in response to cross-border bribery by businesses in the United Kingdom. In order to curb unethical transactions that affect the United Kingdom, the Bribery Act governs companies outside the United Kingdom and applies to activities even if they are performed wholly in another country. Similarly, Russian anti-monopoly law applies to agreements and actions by companies

---

10 See American Banana Co. v. United Fruit Co., 213 U.S. 347, 356 (1909) (“[T]he general and almost universal rule is that the character of an act as lawful or unlawful must be determined wholly by the law of the country where the act is done.”).
12 Bribery Act, 2010, c. 23 (U.K.).
14 Bribery Act, 2010 c. 23, § 3(6)(b) (U.K.).
operating outside the territory of the Russian Federation when such agreements or actions affect competition within its territory. In 2015, Russia enacted a law requiring companies anywhere in the world to store personal data concerning Russians on Russian territory. Similarly, according to data protection authorities in the European Union (EU), any company anywhere in the world has to comply with EU data protection laws if it places a web cookie on a computer of an EU resident. Data protection authorities in Europe have regulatory pursued U.S. companies for alleged non-compliance with the EU General Data Protection Regulation (GDPR). In 2021, plaintiffs in Europe brought a class-action lawsuit in a court in California against a California company for alleged violations of the GDPR, but the California court dismissed the case based on forum non conveniens and international comity grounds.

The United States frequently regulates the activities of overseas corporations through extraterritorial federal laws. The Foreign Corrupt Practices Act, which criminalizes the bribery of foreign officials, applies to foreign corporations whose shares trade in the United States securities market. Title I of the Americans with Disabilities Act, which prohibits employers from discriminating against individuals with disabilities, applies to foreign corporations that employ United States citizens working abroad. The Sarbanes-Oxley Act, which imposes standards for corporate responsibility, provides for United States jurisdiction over foreign accounting firms if they play “a

substantial role in the preparation and furnishing” of accounting statements within the purview of the US Securities and Exchange Commission.24 The United States Bankruptcy Code includes in its definition of the bankruptcy estate all assets of a debtor regardless of whether the assets are located within the United States,25 giving the United States bankruptcy courts jurisdiction over a company’s assets located abroad.

In the arena of U.S. privacy laws, the Federal Trade Commission has clarified that the federal U.S. federal Children’s Online Privacy Protection Act (COPPA) applies to any company anywhere in the world if it collects personal data from children in the United States, and COPPA applies to U.S. companies that collect personal data from children outside the United States.26 Also, under the U.S. federal anti-spam law, persons within and outside the United States are prohibited from sending marketing emails to U.S. email accounts and from harvesting U.S. users’ email addresses from websites contrary to the applicable terms of use.27

Occasionally, governments criticize other governments for overbroad extraterritorial legislation. For example, in 1996, the European Community (EC) retaliated against perceived overbroad U.S. legislation imposing sanctions on Cuba, Iran and Libya by introducing a regulation “protecting against the effects of the extraterritorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom” because the EC

26 See Question B.7, Complying with COPPA: Frequently Asked Questions, Fed. Trade Comm’n, www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (“The Internet is a global medium. Do websites and online services developed and run abroad have to comply with the Rule? Foreign-based websites and online services must comply with COPPA if they are directed to children in the United States, or if they knowingly collect personal information from children in the U.S. The law’s definition of ‘operator’ includes foreign-based websites and online services that are involved in commerce in the United States or its territories. As a related matter, U.S.-based sites and services that collect information from foreign children also are subject to COPPA”). See id.
Council believed that “by their extra-territorial application such laws, regulations and other legislative instruments violate international law.”

Based on that European regulation, companies and individuals in Europe could recover damages and invoke sanctions in European courts against companies and individuals residing abroad if the Europeans were held liable outside Europe based on extraterritorial legislation of the United States or other countries. More recently, the EU enacted a regulation to protect European companies doing business with Iran from the impact of US extraterritorial sanctions. Paradoxically, the EU regulation itself applies extraterritorially and demonstrates that the EU countries do not accept limitations on their own ability to enact extra-territorial legislation.

Public international law—the law of nations—governs rights and obligations between countries. Generally, sovereign nations retain the powers of self-governance and do not submit to supranational authorities that can impose laws on them, although there are several prominent exceptions to this general rule. Instead, public international law is created through contracts between countries (also

---


31 Many nations submit jurisdiction over specific trade matters to the World Trade Organization. Similarly, many countries cede jurisdiction to the International Court of Justice over international human rights matters. Finally, the most striking example of an existing supranational legislative body is the European Union; its 27 member states have ceded jurisdiction in a variety of broadly defined areas. See Treaty on the Functioning of the European Union, (EN) No. 26 of Oct. 2012, art. 1, 2012 O.J. (C 326) 47. See also The Council of Europe Cybercrime Convention, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm; Ian Walden, Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent, Queen Mary School of Law Legal Studies Research Paper No.
known as “treaties”) and customary international law. Countries create customary international law through consistent practice in recognition of a legal obligation to follow the practice.

Countries tend to acknowledge that their jurisdiction to execute and adjudicate is generally limited to their own territory, which means a country must not send police, marshals or bailiffs to enforce its laws in another country without that country’s consent (e.g., via judicial assistance programs). But countries have not accepted any meaningful geographical limitations on their own jurisdiction to prescribe laws. For example, jurisdiction under antitrust law is often independent from territorial boundaries, as are violations of criminal law. Also, many European countries retain jurisdiction over criminal matters if an element of the offense is committed within the state’s borders. Moreover, many countries have enacted expansive embargoes and extraterritorial trade sanctions laws.


See S.S. “Lotus” (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7) (The Permanent Court of International Justice stated, “[T]he first and foremost restriction imposed by international law upon a State is that—failing the existence of a permissive rule to the contrary—it may not exercise its power in any form in the territory of another State.”).

James Crawford, Brownlie’s Principles of Public International Law, 456–57 (8th ed., 2012) (discussing the move away from the territorial theory of jurisdiction in international law); ch. 21 (discussing prescriptive, enforcement and adjudicative jurisdiction).

See, e.g., Hartford Fire Ins. Co. v. California, 509 U.S. 764, 796 (1993) (“[I]t is well established . . . that the Sherman Act applies to foreign conduct that was meant to produce and did in fact produce some substantial effect in the United States.”).

See, e.g., United States v. Leiia-Sanchez, 602 F.3d 797 (7th Cir. 2010) (applying racketeering statute to extraterritorial conduct); United States v. Aguilar, 756 F.2d 1418 (9th Cir. 1985) (applying statute prohibiting impersonation of government official to extraterritorial conduct); United States v. Nippon Paper Indus. Co., 109 F.3d 1 (1st Cir. 1997) (applying price-fixing statute to extraterritorial conduct).

Thus, it is difficult to argue or demonstrate that international law imposes meaningful limits on the legislative jurisdiction of the United States over the activities of foreign individuals or companies. As a matter of comity and respect for other countries’ sovereignty, courts, scholars and commentators tend to phrase this less drastically and write, for example, that a country may enact laws that apply extraterritorially concerning “conduct outside its territory that has or is intended to have substantial effect within its territory.” But the concept of “substantial effect” does not draw a clear line or invoke any material limitation in practice.

Public international law does not concern itself with how individual countries—such as the U.S.—allocate jurisdiction between federal, state and local government levels. Therefore, since public international law does not constrain the United States’ jurisdiction to prescribe extraterritorially and also does not address the allocation of jurisdiction within its national system, by extension it does not place any meaningful limits on California’s jurisdiction to prescribe.

1.2.2.2 Limitations on California Jurisdiction Under Federal Law

Unlike international law, U.S. federal law does limit California’s jurisdiction to legislate. In principle, California and other states are free to legislate on any topic, whereas the U.S. Congress may only legislate based on enumerated powers set forth in the United States Constitution. Privacy is not one of the enumerated powers. In practice, however, the U.S. Constitution (through the Supremacy Clause and the Commerce Clause) significantly constrains California privacy law by limiting California’s ability to regulate out-of-state and foreign corporations and persons. The Supremacy Clause provides that the federal Constitution—and federal laws, generally—take precedence over state laws. Where state and federal law conflict, federal law

41 U.S. Const. art. VI, cl. 2.
preempts or displaces state law.\textsuperscript{42} Congress may indicate its intent to preemt state law in two ways: through a statute’s express language (typically in the form of a preemption clause) or through the statute’s structure and purpose.\textsuperscript{43} Where the scope of a statute indicates that Congress intended federal law to occupy the legislative field or where there is an actual conflict between state and federal law, the state law will be invalidated.\textsuperscript{44}

Moreover, where a state law presents an “obstacle to the accomplishment and execution of the full purposes and objectives” of a federal act, it violates the Supremacy Clause.\textsuperscript{45} A state law that interferes with federal policy may be invalidated under the Supremacy Clause. Federal laws have preempted state laws concerning a broad range of issues, including drug labeling;\textsuperscript{46} trade restrictions with foreign countries;\textsuperscript{47} training, testing and licensing of hazardous waste site workers;\textsuperscript{48} and the labeling by weight of packaged foods.\textsuperscript{39} In a privacy enforcement action initiated by the California attorney general against Delta Air Lines, federal law—specifically, the Airline Deregulation Act—was found to preempt application of the California Online Privacy Protection Act (CalOPPA) to commercial airlines.\textsuperscript{50} The Commerce Clause imposes additional constraints on state attempts to regulate out-of-state corporations. The Commerce Clause grants Congress the authority to regulate interstate commerce, as well as commerce with foreign nations.\textsuperscript{51} It also prohibits states from

\textsuperscript{43} See Altria Grp., Inc. v. Good, 555 U.S. 70, 76 (2008).
\textsuperscript{44} See Altria Grp., Inc. v. Good, 555 U.S. 70, 76-77 (2008).
\textsuperscript{46} See PLIVA Inc. v. Mensing, 564 U.S. 604 (2011).
\textsuperscript{51} U.S. Const. art. I, § 8, cl. 3.
passing legislation that improperly discriminates against or unduly burdens out-of-state commerce.52 This principle is often referred to as the implications of the “dormant” Commerce Clause or “negative” Commerce Clause, and a number of rules follow from it. When a state law effectively imposes a tax only on out-of-state products, it violates the dormant Commerce Clause.53 Where a state law provides for different treatment of in-state and out-of-state economic actors, it will be upheld only if it serves a legitimate local purpose and the purpose cannot be achieved through available nondiscriminatory means.54 Even if a state law does not discriminate against out-of-state businesses and attempts to advance a legitimate local public interest, it may be struck down when a court finds that the burden on interstate commerce outweighs the local benefits.55

The Supreme Court has invalidated state legislation under the dormant Commerce Clause on the ground that it regulates extraterritorial corporate conduct. Healy v. The Beer Institute involved a Connecticut law requiring beer companies to post their prices and affirm that these prices were no higher than those in four neighboring states.56 After noting that the “critical inquiry” under the Commerce Clause is whether a state regulation has the practical effect of regulating conduct beyond its boundaries, the court invalidated the statute, reasoning that the Connecticut law had the effect of preventing brewers from engaging in competitive pricing in Massachusetts and elsewhere based on prevailing market conditions.57 The Supreme Court has invalidated state laws on similar grounds concerning a liquor price affirmation scheme58 and communications between out-of-state acquiring corporations and out-of-state shareholders.59

When states attempt to regulate the internet, courts have to consider the dormant Commerce Clause. In one early case, American Library Association v. Pataki, a federal district court reasoned that due to the

internet’s amorphous geography, state laws seeking to regulate internet communications present a high likelihood that an individual will be subject to inconsistent laws by states regulating conduct beyond their borders, which offends the dormant Commerce Clause. Though many courts have followed Pataki, there is no bright-line rule that makes state attempts to regulate the internet per se invalid. As such, there is continuing uncertainty over the appropriate role for states in internet governance. In 2002, a California appellate court upheld a narrow California anti-spam statute after applying the balancing test set forth by the U.S. Supreme Court in Pike v. Bruce Church. A year later, in 2003, the Second Circuit stated that it is “likely that the Internet will soon be seen as falling within the class of subjects that are protected from State regulation because they ‘imperatively demand … a single uniform rule.’” Given that companies collect vast amounts of personal data from residents in many states via the internet, the dormant Commerce Clause may well place limitations on California’s ability to pass data privacy laws that conflict with other states’ laws.

Thus, unlike international law, U.S. federal law does have the potential to impose enforceable and meaningful limitations on California’s ability to apply California privacy law outside California’s border. Privacy advocates, businesses and politicians discuss preemption in the privacy field with great interest.

1.2.2.3 California Conflict of Law Rules

Besides being limited by U.S. federal law, the territorial scope of California laws is also limited by California laws themselves. Some statutes explicitly specify whether they apply only to data or persons in California or to anyone, anywhere. For example, the California wiretap statute, California Penal Code Section 631(a), applies to communications “while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state;” this statute applies to persons acting outside California but only with respect to communications within California;

63 American Booksellers Found. v. Dean, 342 F.3d 96, 104 (2d Cir. 2003).
California Penal Code § 637.7(a), which limits the use of radio-frequency identification devices (i.e., tracking devices), applies only to a “person or entity in this state”); and California Corporations Code Section 25400 provides that it is “unlawful for any person, directly or indirectly, in this state” to commit securities fraud (as defined by the statute). These laws apply only to companies or persons in California.

On the other hand, CalOPPA applies to companies anywhere because it specifies a residency limitation only with respect to data subjects. CalOPPA provides that “any operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service shall conspicuously post its privacy policy on its Web site.”65

Similarly, the California Consumer Privacy Act of 2018 (“CCPA”) protects only California residents but requires businesses around the world to comply,66 subject to a convoluted and narrow exception: “if every aspect of the commercial conduct takes place wholly outside of California.” The statute defines that to mean where “the business collected that information while the consumer was outside of California, no part of the sale of the consumer’s personal information occurred in California, and no personal information collected while the consumer was in California is sold.”67

It is not always clear whether a state statute applies to a specific situation. Legal issues often arise that significantly affect more than one state, and courts must determine which jurisdiction’s laws govern a particular dispute. When the laws of two or more jurisdictions conflict, a body of rules dictates their ordering and resolution. These rules are generally referred to as “conflict of laws” rules. Where a statute is silent on its applicability to companies outside the state of California, courts look to legislative intent to determine whether the law applies to foreign corporations,68 as well as general conflict of law rules.

66 See Chapter 2.4.2 of this book.
68 See, e.g., Greb v. Diamond Int’l Corp., 56 Cal. 4th 243 (2013) (California statute allowing dissolved corporations to be sued irrespective of the date of dissolution does not apply to out-of-state corporations); Kearney v. Salomon Smith Barney, Inc., 39 Cal. 4th 95 (2006) (California eavesdropping statute applies to out-of-
Subject to constitutional restrictions, a court will follow a statutory directive of its own state as to choice of law.\(^{69}\) Where there is no such directive, courts may consider a number of factors, including the needs of the interstate and international systems, the relevant policies of the forum, the protection of justified expectations and the basic policies underlying the particular field of law.\(^{70}\)

There is a long-standing presumption in American law that a law does not apply extraterritorially absent legislative intent.\(^{71}\) Historically, the default position was that the statutes of a state have no force beyond the state’s borders.\(^{72}\) Although a state has the power to “legislate concerning the rights and obligations of its citizens with regard to transactions occurring beyond its boundaries, the presumption is that it did not intend to give its statutes any extraterritorial effect.”\(^{73}\) The presumption against extraterritoriality will not be overcome absent a showing of legislative intent clearly expressed or reasonably inferred from the language of the act or from its purpose, subject matter or history.

In the privacy arena, the default is probably the other way around, given the legislative intent to protect Californians from threats to privacy, regardless of where such threats emanate.\(^{74}\) If a California privacy statute is silent on the scope of applicability, California courts are likely to apply the statute to companies outside of the state when the complained-of activity took place or affected persons while they

---

\(^{69}\) Restatement (Second) of Conflict of Laws, § 6 (1971; revised 1986, 1988).
\(^{70}\) Restatement (Second) of Conflict of Laws, § 6 (1971; revised 1986, 1988).
\(^{73}\) North Alaska Salmon Co. v. Pillsbury, 174 Cal. 1, 4 (1916).
\(^{74}\) Cal. Civ. Code, § 1798.81.5(a)(1) states: “It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information.” The term “business” is defined in Cal. Civ. Code § 1798.80 broadly to mean any “sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution.”
were within the State of California. But, California privacy laws would probably not be presumed to protect residents of California whose privacy is intruded upon by non-Californian companies while the California resident is physically in another U.S. state or country.\textsuperscript{75}

The California Supreme Court adopted the “governmental interest” approach to conflict of laws issues in 1967, and it remains the chosen method for resolving conflict of law disputes in tort and contracts cases.\textsuperscript{76} The objective of this analysis is “to determine the law that most appropriately applies to the issue involved.”\textsuperscript{77} The governmental interest analysis generally involves three steps.\textsuperscript{78} First, the court must identify the specific state laws that govern the disputed legal issue and determine whether they are the same or different. If there is a difference, the court then examines each jurisdiction’s interest in applying its own laws under the circumstances of the case to determine whether a true conflict exists. If the court finds that there is a true conflict, it must carefully evaluate and compare the nature and strength of the interest of each jurisdiction in applying its own law, thereby determining “‘which state’s interest would be more impaired if its policy were subordinated to the policy of the other state.’”\textsuperscript{79} The court will then apply “the law of the state whose interest would be the more impaired if its law were not applied.”\textsuperscript{80}

In Kearney v. Salomon Smith Barney, Inc., the California Supreme Court resolved a conflict of laws issue pertaining to California’s Invasion of Privacy Act (CIPA).\textsuperscript{81} Clients of Salomon Smith Barney, a nationwide brokerage firm based in Georgia, alleged that employees of the firm had recorded their telephone conversations without their knowledge or consent in violation of California’s eavesdropping

\textsuperscript{75} See Speyer v. Avis Rent a Car Sys., Inc., 415 F. Supp. 2d 1090, 1095-97 (S.D. Cal. 2005) (finding that California’s unfair competition law did not apply to rental car transactions conducted by California residents while they were out of the state).


\textsuperscript{77} Reich v. Purcell, 67 Cal 2d. 551, 554 (1967).


statute.\textsuperscript{82} They filed a class action against Salomon Smith Barney seeking injunctive relief and damages.\textsuperscript{83} The court determined there was a true conflict between the California eavesdropping statute, which prohibits monitoring and recording a telephone conversation without the consent of all parties, and the relevant Georgia statute, which provides that telephone conversations may be recorded with the consent of only one party to a conversation.\textsuperscript{84} Applying the next phase of the governmental interest analysis, the court found that the failure to apply California law in this context would result in a more significant impairment of California’s interest in protecting the privacy of its residents than Georgia’s interest in having its law applied.\textsuperscript{85} Therefore, the California invasion of privacy statute would apply in determining whether the Georgia corporation’s actions constituted an unlawful invasion of privacy.\textsuperscript{86} The court also made clear that out-of-state companies that do business in California are required, as a general matter, to comply with the laws of the state.\textsuperscript{87}

The Kearney precedent is a strong indication that California courts are willing to apply state privacy laws to out-of-state corporations that engage with California residents, particularly where the legislature has made clear its intent to protect and promote their privacy. Although courts resolve conflict of laws issues on a case-by-case basis, companies that operate in California should pay careful attention to California privacy regulations and comply whenever possible. Privacy is a top priority for the California legislature, which processes and passes many privacy-related bills every year.\textsuperscript{88} Where California privacy laws do not have explicit territorial limitations, out-of-state and overseas corporations should assume that they have to comply.

\textsuperscript{88} Cal. Civ. Code § 1798.81.5(a)(1) states: “It is the intent of the Legislature to ensure that personal information about California residents is protected.” See also Chapter 2.3 of this book and Lothar Determann, Diana Francis and Oliver Zee, \textit{New California Privacy Laws}, BNA Privacy & Security Law Report, 10/28/2013, 12 PVLIR 1820.
Courts apply the same conflicts of law tests when addressing cases involving companies outside the United States operating in or affecting California. For example, in Arno v. Club Med, Inc., 89 the 9th Circuit applied California’s three-part governmental interest analysis (as the California Supreme Court did in Kearney) in deciding whether California or French law governed a California resident’s civil claims against a French resort where she was employed.

In summary, companies outside California are subject to California privacy laws if such laws are not preempted by federal law and do not violate the dormant Commerce Clause of the U.S. Constitution, and if the particular California privacy law specifically provides that it shall apply extraterritorially (e.g., because it expressly refers to all companies anywhere or because it specifies territorial limitations only with respect to the location of data subjects). Out-of-state companies are also subject to particular California privacy laws when those laws are silent on the question of applicability and a court finds that California’s interests prevail over other jurisdictions’ potential interests.

1.2.2.4 Enforceability of California Laws Outside California

Even though international law does not place meaningful limitations on a state’s power to prescribe, it does place relatively clear limitations on a country’s or state’s power to adjudicate and enforce. California cannot send its police, judges or other government officials to other countries to enforce California law there. But, other countries may choose to recognize and enforce judgments issued by California courts in the interest of reciprocity and comity, 90 because California also recognizes and enforces foreign money awards (but not injunctions) under the California Uniform Foreign-Country Money Judgments Recognition Act. 91 Some foreign companies are vulnerable to actions

---

89 Arno v. Club Med, Inc., 22 F.3d 1464 (9th Cir. 1994).
91 There are currently no treaties between the United States and other countries guaranteeing the recognition or enforcement of judgments, see Denis Rice, Global Jurisdiction over Privacy, Breach of Security, and Internet Activity, in: Privacy Compliance and Litigation in California § 11.70-1 (looseleaf); Yahoo! Inc. v. La Ligue contre Le Racisme et L’Antisemitisme, 433 F.3d 1199, 1213 (9th Cir.)
by the California government against assets and business interests that these companies have in California. Other companies may feel relatively safe with respect to laws and enforcement actions originating in California because they do not have strong ties to California, and thus enforcement of California laws against them seems unlikely.

Within the United States, courts and agencies of other states in principle must enforce California laws and judgments. The United States Constitution provides that each state in the United States must give full faith and credit to the public acts, records and judicial proceedings of every other state. The Full Faith and Credit Clause is implemented by a federal statute, which provides that authenticated acts of the legislature, records and judicial proceedings of any state are entitled to the same full faith and credit in every court within the United States as they have by law or usage in the courts where they originate. Full faith and credit must be extended to a judgment rendered by a California court or agency even if the action or proceeding that resulted in the judgment could not have been brought under the law or policy of the state applying the California decision.

When a plaintiff seeks to enforce a California or federal privacy law in a California court against an out-of-state defendant, jurisdictional limitations under the Due Process Clause of the Fourteenth Amendment to the United States Constitution come into play. Many California privacy laws apply to companies in other states and


92 U.S. Const. art. IV, § 1.


94 Baker by Thomas v. Gen. Motors Corp., 522 U.S. 222, 232 (1998) (“In numerous cases this Court has held that credit must be given to the judgment of another state although the forum would not be required to entertain the suit on which the judgment was founded.”) (quoting Milwaukee Cnty. v. M.E. White Co., 296 U.S. 268, 277 (1935))).
countries, but a company that is subject to a California privacy law is not also automatically subject to jurisdiction of California courts.95

1.3 Privacy

Privacy is a sweeping, evolving concept.96 Among other values, privacy encompasses freedom of thought, bodily integrity and self-determination, solitude in certain physical spaces (especially the home), control over personal information and reputation and freedom from surveillance, searches and interrogation by the government.97

1.3.1 Rights to Privacy and Data Privacy

For Samuel Warren and Louis Brandeis, the right to privacy is the individual’s “right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others.”98 In their groundbreaking article from 130 years ago, “The Right to Privacy,”99 Warren and Brandeis explained that individuals cannot be compelled to express their own thoughts and sentiments (except when upon the witness stand), and even if individuals choose to express their thoughts, they “generally retains the power to fix the limits of the publicity which shall be given them.”

Alan Westin’s Privacy and Freedom100 defined privacy as “the claim of individuals, groups, or institutions to determine for themselves when,
how, and to what extent information about them is communicated to others." Westin distinguishes four states of privacy, specifically: (1) solitude, (2) intimacy, (3) anonymity, and (4) reserve. The first is characterized by separation from the group and freedom from the observation of other persons and is the most complete state of privacy. In the second state, the individual is acting as a “part of a small unit that claims and is allowed to exercise corporate seclusion so that it may achieve a close, relaxed, and frank relationship between two or more individuals.” The third state of privacy occurs “when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance.” It also encompasses the situation of publishing ideas anonymously. The last state of privacy for Westin is “the creation of a psychological barrier against unwarranted intrusion; this occurs when the individual’s need to limit communication about himself is protected by the willing discretion of those surrounding him.”

For Charles Fried, privacy is the “control over knowledge about oneself,” not simply “an absence of information about what is in the minds of others.” For Ruth Gavison, privacy pertains to “accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others’ attention.” Helen Nissenbaum emphasizes the context of privacy and technology for the integrity of social life.

Julie Inness argues that “‘intimacy’ is the common denominator in all the matters that people claim to be private.” Privacy is “the state of the agent having control over decisions concerning matters that draw their meaning and value from the agent’s love, caring, or liking. These

decisions cover choices on the agent’s part about access to herself, the dissemination of information about herself, and her actions.”111 Anita L. Allen defines privacy as the “inaccessibility of persons, their mental states, or information about them to the senses and surveillance devices of others.”112

Paul Schwartz understands information privacy to result from legal restrictions and other conditions, such as social norms, that govern the use, transfer, and processing of personal data.”113

Susan Freiwald notes that trends to undermine or negate the privacy of electronic communications are “destructive of society’s ability to communicate. . . . If courts do not establish constitutional protections for the electronic communications that are now central to our lives and work, then we will have accorded law enforcement surveillance powers of Orwellian magnitude.”114

In Conceptualizing Privacy,115 Daniel Solove presents general headings that capture recurrent ideas in the field of privacy:

(1) the right to be let alone—Samuel Warren and Louis Brandeis’s famous formulation for the right to privacy;
(2) limited access to the self—the ability to shield oneself from unwanted access by others;
(3) secrecy—the concealment of certain matters from others;
(4) control over personal information—the ability to exercise control over information about oneself;
(5) personhood—the protection of one’s personality, individuality, and dignity; and
(6) intimacy—control over, or limited access to, one’s intimate relationships or aspects of life.

114 Susan Freiwald, First Principles of Communications Privacy, 2007 Stan. Tech. L. Rev. 3. at #30 and #34.
The Supreme Court has stated that it is up to the states to protect a person’s general right to privacy—the right to be let alone by other people.116 Other federal jurisprudence describes privacy as the right of an individual “to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person….”117 The Fourth Amendment protects “privacy against certain kinds of government intrusions,”118 namely, those that intrude on reasonable expectations of privacy.119 In his famous Olmstead dissent,120 which has been cited or referred to repeatedly in various cases121 tackling privacy and the Fourth Amendment, Justice Brandeis declared that the makers of the Constitution:

[...]

The privacy right involves at least two different kinds of interests: “[O]ne is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions.”122

Paul Schwartz notes that “[i]nformation privacy can . . . be distinguished from ‘decisional privacy,’ which, for example, was at stake in the Supreme Court’s decision in Roe v. Wade. The focus of decisional privacy is on freedom from interference when one makes certain fundamental decisions, including those concerning reproduction and child-rearing. In contrast, information privacy is concerned with the use, transfer, and processing of the personal data generated in daily life. Decisional and information privacy are not unrelated; the use,
transfer, or processing of personal data by public and private sector organizations will affect the choices that we make.”

California case law similarly recognized these two distinct classes of privacy interests: (1) the “interest in precluding the dissemination or misuse of sensitive and confidential information (‘informational privacy’);” and (2) the “interest in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference (‘autonomy privacy’).”

1.3.2 Data Protection, Data Privacy and Data Security

The terms “data privacy” and “data protection” are often used interchangeably, in particular in the context of comparisons of Anglo-Saxon data privacy laws and continental European data protection laws. Actually, the two terms and legislative concepts have quite different origins and purposes. Data protection is about protecting individuals (the data subjects) from the effects of automated data processing. Data privacy, by contrast, is about protecting individuals’ communications from intrusion.

Under European data protection laws, the default rule is “verboten” (German for “forbidden”). Companies are generally prohibited from processing personal data, unless they obtain consent from the data subjects or they find an applicable statutory exemption. European data protection laws are first and foremost intended to restrict and

126 Governments are also subject to restrictions on data processing under national European data protection laws, but details vary from country to country. In 2014, people in Europe reacted with outrage to revelations about large-scale surveillance regarding electronic communications by the United States National Security Agency (NSA) and European intelligence services. Yet, the EU Data Protection Regulation continues largely to exempt data processing for national security purposes, due to different views in the 28 EU member states on this topic. See Lothar Determann and Karl-Theodor zu Guttenberg, On War and Peace in Cyberspace: Security, Privacy, Jurisdiction, 41 Hastings Const. L.Q., 1, 13 (2014).
reduce the automated processing of personal data—even if such data is publicly available.

One key feature of European-style data protection laws is a data minimization requirement: Companies are prohibited from collecting, using and retaining data, unless they obtain consent or have another compelling reason to process the data. And, companies are required to minimize the amount of data they collect, the instances of processing, the people who have access and the time periods in which they retain data. In practice, many companies in Europe collect and process personal data as much as their competitors in other parts of the world. European data protection laws provide for exemptions, and data subjects grant consent to allow this. But, a general hostility to personal data processing and databases in European data protection laws is important to keep in mind for purposes of understanding and applying European data protection laws. That posture may help explain why European companies do not lead in information-driven economy sectors, such as electronic commerce, cloud computing, software-as-a-service and social networking, where much of the innovation and market leaders come from the United States and, increasingly, Asia.

California, the United States and many countries outside of Europe, by contrast, generally allow data processing. Instead, their focus is on data privacy. Data privacy laws are primarily intended to protect individuals from intrusion into seclusion and interception of confidential communications. Given this focus, individuals are usually not protected, unless they have a reasonable expectation of privacy in a particular situation or unless some other policy justifies protection.127 Companies can—and frequently do—vitiate such expectations of privacy by notifying individuals of the companies’ data collection and processing activities (e.g., in employee handbooks, website

privacy statements and in-store warnings about security cameras). Individuals receive some protection in the sanctity of their homes, for example, but communications and activities outside receive little or no protection (e.g., information in public records, records shared with third parties, photos taken in public, audible phone conversations in public, postings on the internet or via social networking platforms, etc.). Instead of enacting one comprehensive data protection law, Congress and state legislatures have enacted numerous sector- and threat-specific laws on the federal and state level to address specific concerns about data privacy narrowly and without too much collateral damage to freedom of information and technological progress.

More recently, legislatures around the world have started to supplement data privacy laws with sectoral data security laws. These laws aim to protect individuals from specific harms resulting from unauthorized access to personal information, in particular, identity theft (e.g., criminals using someone’s personal data to acquire or charge credit cards). Examples include data security breach notification laws (California passed the first law in 2002, with most U.S. states and many countries following suit thereafter), detailed prescriptions regarding technical and organizational measures to protect health information in the Health Insurance Portability and Accountability Act (HIPAA) and U.S. state laws in California, Massachusetts, Nevada and New York requiring the encryption of certain data in certain circumstances.

In line with common language usage and in the interest of simplicity, this book will use the term “data privacy” collectively for data

128 See, e.g., In re Yahoo Mail Litig., 7 F. Supp. 3d 1016, 1028-32 (N.D. Cal. 2014) (holding that by agreeing to terms of service, email service provider’s users had explicitly consented to provider’s practice of scanning and analyzing emails, therefore barring their claim under the federal Wiretap Act).

129 See, e.g., Evens v. Superior Court, 77 Cal. App. 4th 320, 324 (1999) (holding that teacher had no reasonable expectation of privacy in her communications made in the classroom); United States v. Standefer, No. 06-CR-2674-H, 2007 WL 2301760, at *3 (S.D. Cal. Aug. 8, 2007) (“There is no reasonable expectation of privacy in financial records such as checks, deposit slips, and financial statements maintained by third party institutions such as banks, because a depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.” (internal quotations omitted)).

protection, data privacy and data security, except where differentiation matters.

1.3.3 Property

Data privacy laws are not concerned with property rights. Under property laws, persons can own real estate, chattels, intangibles or other items and be entitled to exclude others from use of or access to such items. Property rights are intended to incentivize farmers to invest in land and authors to invest in the creation of original works. Owners may or must obtain deeds and register their property rights with land registries, the Patent & Trademark Office, the Copyright Office or other agencies. Property owners can grant exclusive or non-exclusive licenses or transfer their property rights.

Data privacy laws are not intended to give incentives to data subjects to make investments or derive profits from personal data. Data privacy laws also do not contemplate that rights can be registered, licensed or transferred. Data subjects can grant consent to allow use of their personal data, but they cannot assign or transfer ownership to new owners. Data subjects can prohibit companies from collecting or using personal data under certain circumstances, but not with the objective of granting exclusive exploitation rights. The remedies and effects of privacy laws can resemble property laws under some circumstances. But, privacy laws are not only enforced by data subjects, but also by regulators (which would not normally concern themselves with the enforcement of individual property rights). For example, the Federal Trade Commission or state attorneys general may sanction companies that violate consumer privacy laws with fines, due to the public interest in preserving privacy and human dignity.

Talk about informational self-determination and proposals for property law regimes to protect privacy sometimes give people


the idea that they own personal data about themselves. But, it is a fact is that no one owns facts. Factual information is largely excluded from intellectual property law protection. Copyright law protects only creative expression, not factual information. Trade secret law protects information that companies keep secret if such information derives an economic value from being secret. Personal information about individuals can be kept secret and protected under trade secret laws if it has an independent economic value due to being secret. When social media companies and other online service operators aggregate information about usage and user preferences, it is the companies that can claim trade secret ownership rights in such aggregate information, not the individuals (the data subjects) to whom the information pertains. Also, databases with content and personal information can be protected under European database laws and U.S. state laws on appropriation.


134 See, e.g., 17 U.S.C., § 102(b) (“In no case does copyright protection . . . extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery . . . .”); Publications, Inc. v. Rural Tel. Serv. Co., Inc., 499 U.S. 340, 347-48 (1991) (holding that “all facts—scientific, historical, biographical, and news of the day” are part of the public domain and are not copyrightable because they do not owe their origin to an act of authorship as required by Article I, § 8, cl. 8 of the U.S. Constitution for protection) (citations omitted).

135 See, e.g., Cal. Civ. Code, § 3426.11.


137 See, e.g., National Basketball Ass’n v. Motorola, Inc., 105 F.3d 841, 852-54 (2d Cir. 1997) (discussing the merits of a “hot news” misappropriation claim in the context of the unauthorized electronic delivery of near-real-time professional basketball statistics) (citations omitted); United States Golf Ass’n v. Arroyo Software Corp., 69 Cal. App. 4th 607, 611-12, 618 (1999) (discussing California’s common law misappropriation as applicable to the unauthorized use of golf handicap formulas that were developed through intensive data collection and analysis); Board of Trade City of Chicago v. Dow Jones and Co., 439 N.E.2d 526, 537 (Ill. App. Ct. 1982) (applying Illinois’ common law misappropriation to the unauthorized use of the Dow Jones Index and Averages as a trading vehicle); Restatement (Third) of Unfair Competition, § 38 (1995); Jane C. Ginsburg, Copyright, Common Law, and Sui Generis Protection of Databases in the United States and Abroad, 66 U. Cin. L. Rev. 151, 157 et seq. (1997).
1.3.4 Freedom of Speech and Information

Privacy rights can complement the rights to free speech and information. For example, people can speak more freely when they can remain anonymous or at least hide or obscure their identities. But privacy rights can also directly conflict with rights to free speech and information, for example, in the context of defamation claims or “rights to be forgotten,” which are aimed at restricting dissemination and access to information. Both rights have to be balanced. In balancing conflicts between freedom of speech and privacy, California—and the United States, more generally—tend to give greater weight to freedom of speech and information than any other jurisdiction in the world.

While technology innovators in the United States are working hard to be remembered, European politicians are obsessed with a “right to be forgotten.” This makes for quite a symbolic illustration of the transatlantic divide with respect to innovation in the information age.

In 2014, the Court of Justice of the European Union (CJEU) issued a ruling granting EU citizens a limited “right to be forgotten.” The case, which concerned a Spanish lawyer, Mario Costeja González, requires search engines to consider requests from EU citizens to remove links to web pages resulting from a search for their name where search results

138 See EU Proposes ‘Right To Be Forgotten’ By Internet Firms, BBC News (Jan. 23, 2012), http://www.bbc.co.uk/news/technology-16677370 (discussing the EU’s proposed regulation requiring firms to delete data about users upon request if there are no “legitimate grounds” for the data to be kept); Bruno Waterfield, ‘Right To Be Forgotten’ Proposed By European Commission, The Telegraph (Nov. 5, 2010), http://www.telegraph.co.uk/technology/news/8111866/Right-to-be-forgotten-proposed-by-European-Commission.html (quoting Viviane Reding, the European Commissioner for Justice, Fundamental Rights and Citizenship at that time: “Internet users must have effective control of what they put online and be able to correct, withdraw or delete it at will . . . . [T]he right to be forgotten is essential in today’s digital world.”); Joseph Turow, et al., Americans Reject Tailored Advertising and Three Activities That Enable It, SSRN Electronic Journal (Sept. 2009), available at https://www.researchgate.net/publication/228204611_Americans_Reject_Tailored_Advertising_and_Three_Activities_That_Enable_It (reporting that in a random survey of 1,000 American adults, 92 percent believed that there should be a law requiring websites and advertising companies to delete all stored information about an individual, if requested to do so).

“appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed.” In just the first five months following the ruling, Google alone processed more than 140,000 removal requests related to 491,000 links.140

The 2014 CJEU judgment as well as the subsequent codification of the “right to be forgotten” in Article 17 of the European Union’s General Data Protection Regulation (GDPR)141 stands in stark contrast to decisions by U.S. federal courts with respect to search engine results. U.S. federal courts have uniformly held that search results are protected by the First Amendment and that individuals do not have a cause of action against search engine operators based on the inclusion or removal of search results pertaining to them.142 Therefore, search engine operators cannot be compelled under U.S. federal or California privacy laws to modify, include or delete search results. In 2019, the CJEU clarified that a search engine provider may limit the removal of search results to pages visible from the territory of the European Economic Area and does not have to censor search results visible to users in the United States or other countries.143

In his dark vision of Nineteen Eighty-Four, which has influenced the development of privacy law and policy, George Orwell described

a government obsessed with constantly rewriting history, causing facts to be forgotten and controlling citizens’ memories.\textsuperscript{144} In most constitutions around the world, the right to free speech and information is protected against government interference.\textsuperscript{145} According to Article 17 of the GDPR,\textsuperscript{146} effective May 25, 2018, politicians and other data subjects can demand that information about themselves be deleted from internet search results, websites or others’ social media accounts on the grounds that the information is no longer relevant or needed.\textsuperscript{147} In the aforementioned case concerning Mario Costeja González, the CJEU had already created such a “right to be forgotten” before the legislative process was completed. Under the GDPR, various government authorities in the EU are now empowered to censor free speech and curb rights to information.\textsuperscript{148}

\footnotesize
\begin{itemize}
\item \textsuperscript{144} See George Orwell, \textit{Nineteen Eighty-Four} (1949).
\item \textsuperscript{145} E.g., Constitution of the Republic of South Africa, 1996, Ch. 2, § 16(1)(b) (granting freedom of expression and freedom to receive or impart information or ideas); Bundesverfassung [BV] [Constitution] Apr. 18, 1999, SR 101, art. 16 (Switzerland) (granting the right to free expression and the right to receive, gather and disseminate information from generally accessible sources); Saligang Batas ng Pilipinas [Constitution] 1987, art. III, §§ 4, 7 (Philippines) (granting the right to freedom of speech and expression, and the right to information on matters of public concern). See generally Lothar Determann, \textit{Kommunikationsfreiheit im Internet: Freiheitsrechte und gesetzliche Beschränkungen} [Freedom of Communications on the Internet] (1999).
\item \textsuperscript{146} Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, May 4, 2016, L119/1.
\item \textsuperscript{148} During the 2012 Symposium of the Stanford Technology Law Journal on “First Amendment Challenges in the Digital Age,” (see \textit{Symposium 2012: First Amendment Challenges in the Digital Age}, Stan. Tech. L. Rev., https://law.stanford.edu/stanford-technology-law-review-stlr/stlr-past-symposia/#slsnav-2013), Professor Franz Werro argued for a right to be forgotten in reference to an incident that had recently occurred in Switzerland: a bank robber served a long prison sentence, then started a new career and became a successful businessman. Many years later, a journalist tracked him down and reported on his past, putting his new existence in jeopardy. Professor Werro argued that the ex-convict-turned-successful-businessman had a right to have his past forgotten. I argued against such a right by pointing to the right of the public to remain informed, and the value of this particular story for
\end{itemize}
California enacted a much narrower law requiring operators of online platforms to enable minors to remove their own social media posts, which most operators already allow, for minors and adults alike.\textsuperscript{149} It is not yet settled whether today’s children will want or need a right to be forgotten as they grow up. Former Google CEO Eric Schmidt has suggested that today’s children may have to change their names when they turn 30, to have their pasts forgotten and to dissociate themselves from all the sensitive, potentially embarrassing information that they and their friends published on social media sites.\textsuperscript{150} But perhaps, instead, social media will foster tolerance, and soon there will be so much embarrassing information about everyone online that society will learn to accept the fact that youngsters may be wild and take extreme views. Maybe once our children turn 30, society will have become less hypocritical and accept that young people have a right to change their views. Then, hopefully, no one has to wish to be forgotten, hide their past or change their name.


1.4 Law

The United States Congress enacts U.S. federal laws, as contemplated by the U.S. Constitution, which allocates specific subject matter areas to federal legislative jurisdiction. To the extent the U.S. Constitution does not provide for federal legislative jurisdiction, California and other states are generally empowered to make laws.151

In California, as in other states in the United States, the state legislature, as well as courts and administrative agencies make law. Statutory laws are rules enacted by legislatures, addressing situations generally and in the abstract. They differ from judgments of courts and adjudicatory rulings by administrative agencies, which address a defined set of facts relating to specific cases, controversies, parties, individuals or companies.152 The California legislature makes new law in statutes and also codifies court-made law, including, for example, the privacy torts.153 In the California Civil Code, the California legislature clarifies that it does not mean to ossify the common law through codification, and California courts shall remain in charge of further developing common law.154

As companies develop and apply their policies and practices regarding personal data, they need to take account of more than general, statutory laws. Companies also must take into account practices of competitors, court cases involving other companies, general guidance from executive agencies, regulatory enforcement

151 U.S. Const. art. I, § 8 and Amendment X.
152 See U.S. Const. art. III, § 2; Arizonans for Official English v. Arizona, 520 U.S. 43 (1997); Renne v. Geary, 501 U.S. 312 (1991). See Samuel W. Cooper, Considering “Power” in Separation of Powers, 46 Stan. L. Rev. 361, 387 (1994) (“Legislative power is the power to decree a result but not to implement it. It is the power to create a new policy, either general or specific, and present that policy to those charged with its implementation.”); 16A Am. Jur. 2d Constitutional Law § 261 (“Resolving specific controversies between parties, declaring the law, and ensuring the orderly and effective administration of justice are core judicial functions protected by the separation of powers doctrine.”).
actions, self-regulatory industry initiatives, public opinion and customer expectations.

If enough companies follow a certain practice, then this course of dealing can become legally relevant. Courts or regulators may look to industry practices to determine what exactly the term “reasonable” in a privacy statement or statute means. Customers may also adjust their demands and refer to “standard practice” or “best practices” in procurement terms and requests for proposals. Individuals may develop privacy expectations that companies may have either to honor under various laws or negate via privacy notices. Also, smaller companies tend to find comfort in the fact that larger companies follow a certain practice, hoping that this will keep the smaller company relatively safe from challenges by regulators and class-action plaintiffs’ firms, which tend to target bigger players or deeper pockets first.

Given the relatively recent advent of privacy laws and rapid changes in this area, attorneys and other professionals often find it difficult to determine what the law is on a particular point and frequently refer to “best practices” as a surrogate to justify decisions on privacy topics. This can cause companies to do more or less than they are required to do by applicable laws. Following recommendations that someone calls “best practices” can easily result in missed business opportunities or exposure to liability. Different companies have different interests and operate in different circumstances. Each has to determine for itself which practices are best in a particular scenario.

For these reasons, although it is generally advisable to monitor and consider industry standards and “best practices,” it is also important for every company to recognize that practices are not laws and that the “best practices” are what works best for you and your company.

1.5 California and U.S. Federal Privacy Law Summary

1.5.1 Scope
As discussed earlier, this book focuses on California and U.S. federal laws that are intended to protect individual data privacy. California

155 See Chapters 1.2 and 1.4.
privacy laws can also apply to companies in other U.S. states and
countries, and companies in California have to comply with foreign and
U.S. federal privacy laws, subject to conflict of law and jurisdictional
rules that are summarized in this chapter.

**1.5.2 Terminology**

Terminology and definitions in California and U.S. federal privacy
laws are varied and disparate. For example, a number of California
statutes use the term “personally identifiable information” but define
it differently. In the California Civil Code, one can find different
definitions of similar-sounding terms like “personal identification
information,” “personal information” and “personally identifiable
information.” Within the California Consumer Privacy Act

---

157 Cal. Civ. Code § 1747.08 (the Song-Beverly Credit Card Act uses the term
“personal identification information,” which courts have interpreted to cover
any information relating to a person, even a zip code, see Pineda v. Williams-
Sonoma Stores, Inc., 51 Cal. 4th 524, 530 (2001)). The statutory definition in
Cal. Civ. Code § 1747.08(3)(b) states: “For purposes of this section ‘personal
identification information,’ means information concerning the cardholder,
other than information set forth on the credit card, and including, but not
limited to, the cardholder’s address and telephone number.”
the term “personal information” with an enumerative list of data categories.
Cal. Civ. Code § 1798.80 (e) contains a much broader definition: “‘Personal
information’ means any information that identifies, relates to, describes, or
is capable of being associated with, a particular individual, including, but
not limited to, his or her name, signature, social security number, physical
characteristics or description, address, telephone number, passport number,
driver’s license or state identification card number, insurance policy number,
education, employment, employment history, bank account number, credit
card number, debit card number, or any other financial information, medical
information, or health insurance information. ‘Personal information’ does not
include publicly available information that is lawfully made available to the
general public from federal, state, or local government records.” Only a couple
of sections further, in Cal. Civ. Code § 1798.81.5(d)(1), on data security breach
notifications, the term “personal information” is defined with an enumerated
list of data categories.
159 Cal. Civ. Code § 1798.81.5[d][1] uses and defines the term “personal
information” but also uses “personally identifiable information” in subsection
[f], without separate definition: “Any person or business that is required to
issue a security breach notification pursuant to this section to more than 500
California residents as a result of a single breach of the security system shall
 (“CCPA”), the term “personal information” is defined in two subsections very differently for distinct parts of the statute.\textsuperscript{160}

This book will use the specific terms in a statute when discussing that statute, but will otherwise use terms that are more common in U.S. and international data privacy law literature, including the following:

“Personal data” means information that relates to an individual person who can be identified, including identifying information (e.g., name, passport number, etc.) and any other data (e.g., photos, phone numbers, etc.). Whether personal data is protected by a particular California privacy law depends on the statute’s or law’s definitions, which may refer to “personal information,” “personally identifiable information,” “personal identification information,” “medical information,” “personally identifiable health information,” etc.

“Data subject” means the individual person to whom personal data relates. California torts and some statutes protect any person. Other statutes protect more limited groups, for example, consumers, children or patients. Companies and other legal entities do not typically enjoy protections under privacy laws.\textsuperscript{161}

“Data controller” means a company that collects, uses and processes personal data for its own purposes (e.g., an employer with respect to employee data and a retailer with respect to customer data). California torts and some statutes apply to anyone. Other statutes regulate more limited groups, for example, operators of online services or medical care providers. Thus, it is important to determine for each statute its scope of applicability, both in terms of territorial range and subject matter (see details on these statutes in Chapter 2).

“Data processor” or “service provider” means a company that processes personal data on behalf of a data controller (e.g., an accountant or payroll service provider that assists an employer). Data processors act as service providers for data controllers and can generally satisfy only a few limited obligations, namely, follow the data controller’s instructions, keep data secure and notify the controller in

\textsuperscript{160}See the extremely broad definition in Cal. Civ. Code § 1798.140(v) and Cal. Civ. Code § 1798.150(a)(1), which refers to a much narrower definition in § 1798.81.5(d)(1).

\textsuperscript{161}FCC v. AT&T Inc., 562 U.S. 397 (2011).
case of a breach. Companies have to clearly position themselves and their business partners as data controllers or data processors to ensure that they can identify and meet their respective obligations.

“Processing” means any handling of personal data, including collection, storage, alteration, disclosure and use, by data controllers or data processors.

### 1.5.3 Key Features

California and U.S. federal privacy laws impose numerous obligations and prohibitions to protect reasonable data privacy expectations of Californians. Companies can satisfy most obligations and overcome most prohibitions by providing notice or seeking consent from data subjects. Without a reasonable expectation of privacy, data subjects do not tend to have many rights under California or U.S. federal privacy laws.\(^{162}\) Companies can set, qualify and negate privacy expectations by way of notice. Very few statutes fail to recognize notice or consent as an exception to prohibitions.\(^{163}\) Therefore, privacy notices play a key role under California and U.S. federal privacy laws and will be addressed in detail in Chapter 4 of this book.

Data subjects can enforce most laws by way of individual or class-action lawsuits. The Federal Trade Commission, the California attorney general and other regulators can also bring lawsuits or impose fines and other sanctions, but private lawsuits are more prevalent.\(^{164}\)

### 1.5.4 California and U.S. Privacy Law—What It Is Not

No one omnibus statute: Unlike many European, Latin American and Asian countries, neither the United States nor California has enacted one comprehensive data privacy statute. The U.S. Congress decided

---


163 Exceptions include the Song-Beverly Credit Card Act (Cal. Civ. Code § 1747 et seq.), see Chapter 2.7.9.3.1 of this book and Cal. Lab. Code § 435.

164 See Chapter 6 for more detail.
against European-style omnibus data protection legislation in the 1970s. Until a ballot initiative prompted the passage of the CCPA in 2018, California had taken a similar approach and only enacted privacy legislation regarding specific threats, industries or groups of data subjects. Some attribute the successful development of Silicon Valley as the world’s preeminent information technology and online services hub to the lack of an omnibus data protection law. Whether the more selective and sectoral regulatory approach in the United States and in California has resulted in more or less privacy protections is debatable. History shows that the more specific U.S. laws have been rigorously enforced whereas the broader and theoretically more protective European laws have been mostly honored in the breach. Since the CCPA took effect in 2018, businesses face the worst of both worlds in California: extremely broad regulation of data processing in the CCPA plus myriad sector-, situation- and harm-specific privacy laws, which overlap with the CCPA. Additionally, businesses are confronted with constant and rapid change: The California Legislature has amended the CCPA several times in 2018, 2019 and 2020 while the California attorney general enacted and amended regulations under the CCPA several times as well. At the general election in 2020, California voters adopted another ballot initiative to significantly alter and expand the CCPA and cancel the 2020 legislation. Meanwhile, the California Legislature has enacted other specific privacy laws imposing additional and different requirements on companies, including the California Age-Appropriate Design Code Act.

No default prohibition of data processing: In the United States, companies are generally allowed to process personal data unless...

---

169 The law was signed by California’s Governor in September 2022. See also Chapters 2.4 and 2.16 of this book.
particular restriction or prohibition applies. This is in contrast to Europe where data processing is prohibited by default, and companies have to find specific justifications and permissions.\footnote{See Article 7 of the EU Data Protection Directive, Article 6(1) of the General Data Protection Regulation, and Lothar Determann, \textit{International Data Transfers from Europe and Beyond}, 25 Rev. Bank Financ. Serv. (2009).}

\textit{Data minimization}: Unlike in Europe, California and the United States have traditionally not required that companies avoid or minimize the processing of personal data. Companies have been permitted to collect and process as much data as they want, so long as they comply with applicable consent, notice and security requirements.\footnote{See Cal. Civ. Code §§ 1798.199.10 and Chapter 2.4 of this book.} “Big data” has generally been allowed in the United States. Yet, effective January 1, 2023 under the CCPA, a “business’ collection, use, retention, and sharing of a consumer’s personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.”\footnote{Cal. Civ. Code §1798.100(c).}

\textit{Data protection authorities}: Neither the United States federal government nor any states had established European-style data protection authorities until the California Privacy Rights Act required the creation of a new California Privacy Protection Agency in 2020 based on a ballot initiative adopted at the 2020 general election.\footnote{See Chapter 2.4 of this book.} Previously, the California attorney general had created a Privacy Enforcement and Protection Unit in 2012,\footnote{See California Attorney General, \textit{Attorney General Kamala D. Harris Announces Privacy Enforcement and Protection Unit} (July 9, 2012), http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-privacy-enforcement-and-protection.} which will continue to enforce the CCPA and other California privacy laws, while the new California Privacy Protection Agency is only tasked with enforcing the CCPA. At the federal level, the Federal Trade Commission has protected consumer privacy quite effectively based on its powers to enforce general unfair competition laws and some specific privacy
laws, including the CAN-SPAM Act and the Children’s Online Privacy Protection Act (COPPA).  

No data protection registries or filings: The United States has not established any database registries or filing requirements under privacy laws. Companies do not generally have to submit filings to the California or federal government relating to data processing activities or seek any government approval before processing.

Data protection officers: Unlike in Europe, California privacy laws do not require companies to appoint general data protection officers. Under HIPAA, however a U.S. federal health federal law, covered entities have to appoint a data privacy official and a data security official.

No specific restrictions on international data transfers: California and the United States have traditionally stood for free trade and free information flows. International data transfers are not specifically restricted, unlike under the laws in Europe and an increasing number of other countries.

Translation requirements: English is the official language of California. Under California and federal privacy laws, companies are not explicitly required to provide translations of privacy notices, privacy policies or other privacy-related documentation. But, the attorney general requires in regulations under the CCPA that businesses make privacy notices “available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.”

Also, companies in California have to provide translations of certain
types of consumer contracts if they negotiate such contracts primarily in Spanish, Chinese, Tagalog, Vietnamese or Korean; this requirement could also extend to privacy-related documentation if it were part of such a contract.\textsuperscript{179} Moreover, government agencies and employers can be required to provide translations under certain circumstances.\textsuperscript{180}


\textsuperscript{180} For example, long-term health care facilities must provide translations of the Patients’ Bill of Rights (which could include privacy policies) into any language that is used by at least one percent of the facility’s population, Cal. Health & Saf. Code § 1599.61. State and local authorities are required to provide written materials in languages other than English, for example, under Cal. Gov. Code § 7290 et seq. (state agencies in general); Cal. Lab. Code, § 105 (Dept. of Labor Stds. Enforcement); Cal. Unemp. Ins. Code § 316 (unemployment compensation); Cal. Welf. & Inst. Code § 19013.5 (Dept. of Rehabilitation) and § 10607 (Dept. of Social Services). In Samaniego v. Empire Today LLC, 205 Cal. App. 4th 1138 (2012), the California Court of Appeal found an employment contract to be unconscionable where an employer did not provide a Spanish translation of a contract that contained a number of one-sided provisions.
Table of Cases

Absher v. AutoZone, Inc.,
(164 Cal. App. 4th 332 2008) 2.7.9.3.4

ACLU v. Superior Court,
S227106, Ct. App. 2/3 B259392 (Cal. Sup. Ct. August 31, 2017) 2.5.5, 2.8.2

Acosta v. Byrum,
180 N.C. App. 562 (N.C. Ct. App. 2006) 2.9.1.4

Acosta v. Scott Labor LLC,
377 F. Supp. 2d 647 (N.D. Ill. 2005) 2.6.1

Acosta v. Trans Union, LLC,
243 F.R.D. 377 (C.D. Cal. 2007) 2.7.3.4

Agnew v. Parks,
172 Cal. App. 2d 756 (Cal. Ct. App. 1959) 2.17.3

Allstar Mktg. Grp., LLC v. Your Store Online, LLC,
666 F. Supp. 2d 1109 (C.D. Cal. 2009) 6.2.3.2

Altia Grp., Inc. v. Good,
555 U.S. 70 (2008) 1.2.2.2

Alvarez v. Brookstone Co., Inc.,

Alvarez v. Kmart Holding Corp.

Amalgamated Transit Union, Local 1756, AFL-CIO v. Superior Court
46 Cal. 4th 993, 1005 (2009) 6.2.1.3

Ambers v. BUY.COM, Inc.,
No. SACV 13-0196 AG (JPRx), 2013 U.S. Dist. LEXIS 69219 (C. D. Cal. Apr. 30, 2013) 2.7.9.2

American Acad. of Pediatrics v. Lungren,
(1997) 16 Cal. 4th 307 2.2, 2.2.3,

American Banana Co. v. United Fruit Co.,
213 U.S. 347 (1909) 1.2.2.1

American Bankers Ass’n. v. Gould,
412 F.3d 1081 (9th Cir. 2005) 2.7.2.3.2
American Booksellers Found. v. Dean,
342 F. 3d 96 (2d Cir. 2003) 1.2.2.2
American Library Ass’n v. Pataki,
969 F. Supp. 160 (S.D.N.Y. 1997) 1.2.2.2
Local 443, N.L.R.B.,
No. 34-CA-12576 (2010) 4.6
Ameri-Medical Corp. v. Workers’ Comp. Appeals Bd.,
42 Cal. App. 4th 1260 (Cal. Ct. App. 1996) 2.2.1
Anti-Defamation League of B’nai B’rith v. Superior Court,
Antonelli v. Meyer,
No. 5:11-CV-03874 EJD, 2014 WL 4949796
(N.D. Cal. Sept. 30, 2014) 2.6.3.2, 2.27.1.4
Apple Inc. v. Superior Court,
56 Cal. 4th 128 (2013) 2.7.9.2, 4.4.1, 6.2.1.3
Archer v. United Rentals, Inc.,
195 Cal. App. 4th 807 (Cal. Ct. App. 2011) 2.7.9.1
Arizonans for Official English v. Arizona,
520 U.S. 43 (1997) 1.4
Arno v. Club Med, Inc.,
22 F.3d 1464 (9th Cir. 1994) 1.2.2.3
Asis Internet Servs. v. Active Response Grp.,
2008 U.S. Dist. LEXIS 109818 (N.D. Cal. 2008) 2.16.2.2
Baird v. Sabre Inc.,
995 F. Supp. 2d 1100 (C.D. Cal. 2014) 2.22.6.4
Baker by Thomas v. Gen. Motors Corp.,
522 U.S. 222 (1998) 1.2.2.4
Balsam v. Trancos, Inc.,
as modified on denial of reh’g (Mar. 21, 2012) 2.22.2
Bancroft & Masters, Inc. v. Augusta Nat. Inc.,
223 F.3d 1082 (9th Cir. 2000) 6.2.3.2
Banks v. DMV,
419 F. Supp. 2d 1186 (C.D. Cal. 2006) 2.19.4.4
Barber v. Time, Inc.,
159 S.W.2d 291 (Mo. 1942) 6.2.1.1
Batzel v. Smith,
333 F.3d. 1119 (9th Cir. 2003) 6.5.1
<table>
<thead>
<tr>
<th>Case</th>
<th>Citation</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bernhard v. Harrah's Club</td>
<td>16 Cal. 3d 313 (1976)</td>
<td>1.2.2.3</td>
</tr>
<tr>
<td>Bevan v. Smartt</td>
<td>316 F. Supp. 2d 1153 (D. Utah 2004)</td>
<td>2.6.1</td>
</tr>
<tr>
<td>Beyond Sys., Inc. v. Kraft Foods, Inc.</td>
<td>No. 13-2137, 2015 WL 451944 (4th Cir. Feb. 4, 2015)</td>
<td>2.22.1, 2.22.1, 2.22.1.4.4</td>
</tr>
<tr>
<td>Big S Sporting Goods Corp. v. Zurich Am. Ins. Co.</td>
<td>957 F. Supp. 2d 1135 (C.D. Cal. 2013)</td>
<td>2.7.9.4</td>
</tr>
<tr>
<td>Board of Trade City of Chicago v. Dow Jones and Co.</td>
<td>439 N.E.2d 526 (Ill. App. Ct. 1982)</td>
<td>1.3.3</td>
</tr>
<tr>
<td>Brickman v. Facebook</td>
<td>No. 16-cv-00751-TEH (N.D. Cal. 2017)</td>
<td>2.22.3.4</td>
</tr>
<tr>
<td>Bridges v. Wixon</td>
<td>326 U.S. 135 (1945)</td>
<td>2.11.1</td>
</tr>
<tr>
<td>Briggs v. American Air Filter Co., Inc.</td>
<td>630 F.2d 414 (5th Cir. 1980)</td>
<td>4.6</td>
</tr>
<tr>
<td>Brown v. Mortensen</td>
<td>51 Cal. 4th 1052 (2011)</td>
<td>2.9.2</td>
</tr>
<tr>
<td>Brown v. Mortensen</td>
<td>30 Cal. App. 5th 931, 242 Cal. Rptr. 3d 67 (2019)</td>
<td>2.9.2.4</td>
</tr>
<tr>
<td>Brown-Forman Distillers Corp. v. New York State Liquor Auth.</td>
<td>476 U.S. 573 (1986)</td>
<td>1.2.2.2</td>
</tr>
</tbody>
</table>
Buraye v. Equifax,
625 F. Supp. 2d 894 (C.D. Cal. 2008) 2.7.4.3.3

Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C.,
314 Conn. 433 (2014) 2.9.1.4

Cahen v. Toyota Motor Corp.,
147 F. Supp. 3d 955 (N.D. Ca. 2015) 2.2.3

Calder v. Jones,

142 Cal. App. 4th 21 (Cal. Ct. App. 2006) 2.9.2.4

Californians For Disability Rights v. Mervyn’s, LLC,
39 Cal.4th 223 (2006) 6.2.1.3

Camacho v. Bridgeport Financial, Inc.,
523 F.3d 973 (9th Cir. 2008) 2.7.5.4

Capp v. Nordstrom, Inc.,

Carvalho v. Equifax Info. Servs., LLC,
629 F.3d 876 (9th Cir. 2010) 2.7.4.3.3

Catsouras v. Dep’t of California Highway Patrol,
181 Cal. App. 4th 856 (Cal. Ct. App. 2010) 6.2.1.1

CDF Firefighters v. Maldonado,
158 Cal. App. 4th 1226 (Cal. Ct. App. 2008), as modified on denial of reh’g (Feb. 5, 2008) 6.2.1.1

Cel-Tech Comm’ns, Inc. v. Los Angeles Cellular Tel. Co.
20 Cal. 4th 163 (1999) 6.2.1.3

Chabner v. United of Omaha Life Ins. Co.,
225 F.3d 1042 (9th Cir. 2000) 6.2.1.3

Chamber of Commerce of U.S. v. Lockyer,

Chang v. Lederman,

467 U.S. 837 (1984) 6.3.1

Cisneros v. U.D. Registry, Inc.,
39 Cal. App. 4th 548 (Cal. Ct. App. 1995) 2.7.4.1

City of Ontario, Calif. v. Quon,
560 U.S. 746 (2010) 2.6, 2.6.1
Table of Cases

City of San Jose v. Superior Court,
No. S218066, ___ P.3d ___, 2017 WL 818506
(Cal. Supreme Ct., March 2, 2017) 2.8.2

City of San Jose v. Superior Court,
12 Cal. 3d 447 (1974) 6.2.2.3

Clapper v. Amnesty Int’l USA,
133 S. Ct. 1138 (2013) 6.2.2.1

Collegenet, Inc. v. XAP Corp.,
483 F. Supp. 2d 1058 (2007) 4.2.1, 4.4.4.4, 5.2.5.2, 6.2.1.3

Conservatorship of Wendland,
26 Cal. 4th 519, 531 (2001) 2.2,

Corales v. Bennett,
S67 F.3d 554 (9th Cir. 2009) 6.2.1.1

Corley v. Google,
N.D. Cal., No. 16-473, brief filed, 4/26/16 2.24.1.3

Craigslist Inc. v. 3Taps Inc.,
942 F. Supp. 2d 962 (N.D. Cal. 2013) 2.5.10, 2.5.10.2.3

Crosby v. Nat’l Foreign Trade Council,
530 U.S. 363 (2000) 1.2.2.2

Cubby, Inc. v. CompuServe Inc.,
776 F. Supp. 135 (S.D.N.Y. 1991) 6.5.1

Curto v. Medical World Comme’ns, Inc.,
No. 03CV6327, 2006 U.S. Dist. LEXIS 29387
(E.D.N.Y. May 15, 2006) 2.6.1

Cybersell, Inc. v. Cybersell, Inc.,
130 F.3d 414 (9th Cir. 1997) 6.2.3.2

D’Amico v. Bd. of Med. Examiners,
11 Cal. 3d 1 (1974) 6.3.2

Dardarian v. OfficeMax N. Am., Inc.,
No. 11-cv-00947-YGR, 2014 U.S. Dist. LEXIS 178463
(N.D. Cal. Dec. 30, 2014) 2.7.9.3

Davis v. Devanlay Retail Group, Inc.,
LEXIS 178252 (E.D. Cal. Dec. 14, 2012) 2.7.9.3, 2.7.9.3.1, 2.7.9.3.2

Davis v. United States,
131 S. Ct. 2419 (2011) 2.11.1, 6.4.2.1

Dean v. Dick’s Sporting Goods, Inc.,
No. CV 12-7313 FMO (MANx), 2013 U.S. Dist.
LEXIS 108549 (C.D. Cal. July 26, 2013) 2.7.9.3.1, 2.7.9.3.2, 2.7.9.3.3
Dendrite Int’l Inc. v. Doe,
No. 3, 775 A.2d 756 (Ct. App. Div. 2001) 6.5.2

Department of Motor Vehicles v. Superior Court,

Diaz v. Oakland Tribune, Inc.,
139 Cal. App. 3d 118 (Cal. Ct. App. 1983) 2.21.4

Digital Music News LLC v. Superior Court,

Dobbs v. Jackson Women’s Health Org.,
142 S. Ct. 2228, 2301 (2022) 2.2

Doe 1 v. AOL, LLC,
719 F. Supp. 2d 1102 (N.D. Cal. 2010) 2.5.2.3

Doe 14 v. Internet Brands, Inc.,
9th Cir., No. 12-56638, 2/24/15 6.5.1

Doe v. Borough of Barrington,
729 F. Supp. 376 (D.N.J. 1990) 2.11.1

Doe v. Friendfinder Network, Inc.,
540 F. Supp. 2d 288 (D.N.H. 2008) 6.5.1

Duguid v. Facebook, Inc.,
N.D. Cal., No. 15-CV-00985-JST (2/16/17) 2.22.3.4

E.E.O.C. v. Arabian Am. Oil Co.,
499 U.S. 244 (1991) 1.2.2.3

eBay v. Bidder’s Edge,
100 F. Supp. 2d 1058 (N.D. Cal. 2000) 2.5.10

Edgar v. MITE Corp.,
457 U.S. 624 (1982) 1.2.2.2

Eichenberger v. ESPN, Inc.,
876 F.3d 979 (9th Cir. 2017) 2.23.1.1, 2.23.1.4, 6.2.2.1

Eisenstadt v. Baird,
405 U.S. 438 (1972) 1.3.1

Evens v. Superior Court,
77 Cal. App. 4th 320 (Cal. Ct. App. 1999) 1.3.2

Facebook, Inc. v. ConnectU LLC,
489 F. Supp. 2d 1087 (N.D. Cal. 2007) 2.22.2, 2.22.2.2

Facebook Inc. v. Fisher,
2011 WL 250395 (N.D. Cal. 2011) 2.16.6.1

Facebook, Inc. v. MaxBounty, Inc.,
274 F.R.D. 279 (N.D. Cal. 2011) 2.22, 2.22.1.3.1

Facebook, Inc. v. Power Ventures, Inc.,
844 F. Supp. 2d 1025 (N.D. Cal. 2012) 2.5.10.2.3, 2.22.1.4.4
<table>
<thead>
<tr>
<th>Case</th>
<th>Decision Details</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook, Inc. v. Power Ventures, Inc.</td>
<td>No. C08-05780JW, 2010 WL 3291750</td>
<td>2.4.2.3.3, 2.4.2.4</td>
</tr>
<tr>
<td>Fair Housing Council of San Fernando Valley v. Roommates.com</td>
<td>521 F.3d 1157 (9th Cir. 2008)</td>
<td>6.5.1</td>
</tr>
<tr>
<td>FCC v. AT&amp;T Inc.</td>
<td>562 U.S. 397 (2011)</td>
<td>1.5.2, 2.11.3, 4.4.3</td>
</tr>
<tr>
<td>Feeney v. Young</td>
<td>181 N.Y.S. 481 (N.Y. App. Div. 1920)</td>
<td>6.2.1.1</td>
</tr>
<tr>
<td>Ferguson v. Friendfinders, Inc.</td>
<td>94 Cal. App. 4th 1255 (Cal. Ct. App. 2002)</td>
<td>1.2.2.2</td>
</tr>
<tr>
<td>Fisher et al. v. Capital One Financial Corporation et al.</td>
<td>3:19-CV-04485 (complaint filed 8/1/19)</td>
<td>6.2.1.2</td>
</tr>
<tr>
<td>Florez v. Linens ’N Things, Inc.</td>
<td>108 Cal. App. 4th 447 (2003)</td>
<td>2.7.9.3.1, 2.7.9.3.2</td>
</tr>
<tr>
<td>Fraley v. Facebook, Inc.</td>
<td>830 F. Supp. 2d 785 (N.D. Cal. 2011)</td>
<td>2.21.3, 2.21.4, 6.2.2.3</td>
</tr>
<tr>
<td>Freedman v. America Online, Inc.</td>
<td>325 F. Supp. 2d 638 (E.D. Va. 2004)</td>
<td>2.11.2</td>
</tr>
<tr>
<td>FTC v. Accusearch Inc.</td>
<td>570 F.3d 1187 (10th Cir. 2009)</td>
<td>4.4.4, 6.3.1</td>
</tr>
</tbody>
</table>
FTC v. Asset & Capital Management Group, et al.,
No. 8:13-cv-01107-DSF-JC (C.D. Cal. May 19, 2014) 2.7.5.4

FTC v. Stefanchik,
559 F.3d 924 (9th Cir. 2009) 6.3.1

FTC v. Tashman,
318 F.3d 1273 (11th Cir. 2003) 4.4.4

FTC v. Wyndham Worldwide Corp.,
10 F. Supp. 3d 602 (D.N.J. Apr. 7, 2014), motion to certify appeal granted (June 23, 2014) 6.3.1

FTC v. Wyndham Worldwide Corp.,
2013 WL 3475984 (D.N.J.) 6.3.1

Futrell v. Payday Calif., Inc.,
190 Cal. App. 4th 1419 (Cal. Ct. App. 2010) 2.6.2.2

Gade v. Nat’l Solid Wastes Mgmt. Ass’n,
505 U.S. 88 (1992) 1.2.2.2

Gaos v. Google Inc.,
No. 5:10-CV-4809 EJD, 2012 WL 1094646 (N.D. Cal. Mar. 29, 2012) 6.2.2.1

Gass v. Best Buy Co.,
279 F.R.D. 561 (C.D. Cal. 2012) 2.7.9.3.1, 2.7.9.3.2, 2.7.9.3.3

Gator.com Corp. v. L.L. Bean, Inc.,
341 F.3d 1072 (9th Cir. 2003) on reh’g en banc,
398 F.3d 1125 (9th Cir. 2005) 6.2.3.2

Gill v. Curtis Pub. Co.,
38 Cal.2d 273 (1952) 2.2

Goddard v. Google,
640 F. Supp. 2d 1193 (N.D. Cal. 2009) 6.5.1

Golden Eagle Insurance Co. v. Foremost Insurance Co.,
20 Cal. App. 4th 1372 (1993) 5.2.3.4

Gomon v. TRW, Inc.,
28 Cal. App. 4th 1161 (Cal. Ct. App. 1994) 2.7.4.1, 2.7.4.3.1

Gonzaga Univ. v. Doe,
536 U.S. 273 (2002) 2.19.2.4

Gonzales v. Arrow Fin. Servs., LLC,
660 F.3d 1055 (9th Cir. 2011) 2.7.5, 2.7.6

Gonzales v. Uber Technologies, Inc.,

Gonzalez v. Google,
234 F.R.D. 674 (N.D. Cal. 2006) 2.11.2
<table>
<thead>
<tr>
<th>Case</th>
<th>Volume</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Goodman v. HTC Am., Inc.</td>
<td></td>
<td>2.2.3</td>
</tr>
<tr>
<td>Gordon v. Virtumundo, Inc.</td>
<td></td>
<td>2.22.1</td>
</tr>
<tr>
<td>575 F.3d 1040 (9th Cir. 2009)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gorman v. Wolpoff &amp; Abramson, LLP</td>
<td></td>
<td>2.7.4.4</td>
</tr>
<tr>
<td>584 F.3d 1147 (9th Cir. 2009)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gormley v. Nike Inc.</td>
<td></td>
<td>2.7.9.3, 2.7.9.3.2</td>
</tr>
<tr>
<td>Gossoo v. Microsoft Corp.</td>
<td></td>
<td>2.7.9.4</td>
</tr>
<tr>
<td>Greb v. Diamond Int’l Corp.</td>
<td></td>
<td>1.2.2.3</td>
</tr>
<tr>
<td>56 Cal. 4th 243 (2013)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Griswold v. Connecticut</td>
<td></td>
<td>2.2</td>
</tr>
<tr>
<td>381 U.S. 479 (1965)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gucci America, Inc. v. Hall &amp; Associates</td>
<td></td>
<td>6.5.1</td>
</tr>
<tr>
<td>135 F. Supp. 2d 409 (S.D.N.Y. 2001)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hansberry v. Lee</td>
<td></td>
<td>6.2.2.3</td>
</tr>
<tr>
<td>311 U.S. 32 (1940)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hartford Fire Ins. Co. v. California</td>
<td></td>
<td>1.2.2.1</td>
</tr>
<tr>
<td>506 U.S. 764 (1993)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hartless v. Clorox Co.</td>
<td></td>
<td>6.2.1.3</td>
</tr>
<tr>
<td>No. CIV. 06CV2705JAH CAB, 2007 WL 3245260 (S.D. Cal. Nov. 2, 2007)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hataishi v. First Am. Home Buyers Prot. Corp.</td>
<td></td>
<td>6.2.2.3</td>
</tr>
<tr>
<td>Haug v. PetSmart, Inc.</td>
<td></td>
<td>1.2.2.2</td>
</tr>
<tr>
<td>Healy v. Beer Inst., Inc.</td>
<td></td>
<td>2.5.10</td>
</tr>
<tr>
<td>491 U.S. 324 (1989)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hecht v. Components Int’l, Inc.</td>
<td></td>
<td>6.2.3.2</td>
</tr>
<tr>
<td>Helicopteros Nacionales de Colombia, S.A. v. Hall,</td>
<td></td>
<td>6.2.1.3</td>
</tr>
<tr>
<td>466 U.S. 408 (1984)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hernandez v. Hillsides, Inc.</td>
<td></td>
<td>2.6.1</td>
</tr>
<tr>
<td>47 Cal. 4th 272 (2009)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Hernandez v. Path, Inc.,
No. 12-CV-01515 YGR, 2012 WL 5194120
(N.D. Cal. Oct. 19, 2012) 6.2.2.1

Hill v. Nat’l Collegiate Athletic Assn.,
7 Cal. 4th 1 (1994) 1.3.1, 2.2, 2.2.1, 2.2.2, 2.2.3, 2.3, 2.3.1

Hines v. Davidowitz,
312 U.S. 52 (1941) 1.2.2.2

hiQ Labs, Inc. v. LinkedIn Corp.,
31 F.4th 1180 (9th Cir 2022)
2.5.10.2.3, 2.11.2

Housh v. Peth,
133 N.E.2d 349 (Ohio 1956) 6.2.1.1

Howard v. Crim. Info. Servs., Inc.,
654 F.3d 887 (9th Cir. 2011) 2.19.4, 2.19.4.4

Hunter v. Philip Morris USA,
582 F.3d 1039 (9th Cir. 2009) 6.2.2.1

Hurtado v. Superior Court,
11 Cal. 3d 574 (1974) 1.2.2.3

Hypertouch, Inc. v. ValueClick, Inc.,
192 Cal. App. 4th 805 (Cal. Ct. App. 2011) 2.22.1, 2.22.2

In Florez v. Linens ’N Things, Inc.,
108 Cal. App. 4th 447 (Cal. Ct. App. 2003) 2.7.9.3.2

In re Adobe Sys., Inc. Privacy Litig.,
No. 13-CV-05226-LHK, 2014 WL 4379916
(N.D. Cal. Sept. 4, 2014) 6.2.2.1

In re Adobe Systems, Inc. Privacy Litigation,
No. 13-CV-05226, 2014 WL 4379916
(N.D. Cal. Sept. 4, 2014) 4.4.4.7

In re Calhoun,
121 Cal. App. 4th 1315 (Cal. Ct. App. 2004) 2.2, 2.3.1

In re Carrier IQ, Inc.,
78 F. Supp. 3d 1051 (N.D. Cal. 2015) 2.2.3

In re CVS Caremark Corp.,
FTC File No. C-4259 (F.T.C. June 18, 2009) 6.3.1

In re Dave & Buster’s, Inc.,
FTC File No. 082 3153 (F.T.C. May 20, 2010) 6.3.1

In re Equifax Information Services, LLC,
No. C-4387 (F.T.C. Mar. 15, 2013) 2.7.3.4
<table>
<thead>
<tr>
<th>Table of Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>In re Facebook Privacy Litig.,</strong> 791 F. Supp. 2d 705 (N.D. Cal. 2011) aff’d, 572 F. App’x 494 (9th Cir. 2014)</td>
</tr>
<tr>
<td><strong>In re Facebook, Inc.,</strong> FTC File No. 092 3184, No. C-43655 (F.T.C. Aug. 11, 2011)</td>
</tr>
<tr>
<td><strong>In re Facebook, Inc.,</strong> FTC File No. 092 3184, No. C-4365 (F.T.C. Nov. 29, 2011)</td>
</tr>
<tr>
<td><strong>In re Google Inc.,</strong> 806 F.3d 125, 150-1 (3d Cir. 2015)</td>
</tr>
<tr>
<td><strong>In re Google Inc. Cookie Placement Consumer Privacy Litig.,</strong> 806 F.3d 125 (3d Cir. 2015)</td>
</tr>
<tr>
<td><strong>In re Google Inc. Gmail Litig.,</strong> No. 13-MD-02430-LHK, 2014 WL 1102660 (N.D. Cal. Mar. 18, 2014)</td>
</tr>
<tr>
<td><strong>In re Google Inc. Gmail Litigation,</strong> Northern District of California, Case 5:13-md-02430-LHK, 2013 WL 5366963 (Sept. 26, 2013)</td>
</tr>
<tr>
<td><strong>In re Google Inc.,</strong> FTC File No. 102 3136, No. C-4336 (F.T.C. Oct. 13, 2011)</td>
</tr>
<tr>
<td><strong>In re Google, Inc. Privacy Litig.,</strong> 2012 WL 6378343 (N.D. Cal. Dec. 28, 2012)</td>
</tr>
<tr>
<td><strong>In re Hulu Privacy Litig.,</strong> No. 11-CV-03764-LB, 2015 WL 1503506 (N.D. Cal. Mar. 31, 2015)</td>
</tr>
<tr>
<td><strong>In re Hulu Privacy Litig.,</strong> No. C 11-03764 LB, 2014 WL 2758598, at *1 (N.D. Cal. June 17, 2014)</td>
</tr>
</tbody>
</table>
In re iPhone Application Litig.,
2011 WL 4403963 (N.D. Cal. Sept. 20, 2011) 6.2.2.1

In re iPhone Application Litig.,
844 F. Supp. 2d 1040 (N.D. Cal. 2012) 2.16.3.4, 2.24.1.3, 4.3.3, 4.4.5, 6.2.1.3, 6.2.2.1, 6.2.2.3

In re iPhone Application Litig.,
No. 11-MD-02250-LHK, 2011 WL 4403963 (N.D. Cal. Sept. 20, 2011) 6.2.1.3, 6.2.2.1

In re Lenz,
448 B.R. 832 (Bankr. D. Or. 2011) 2.7.1.4

In re LinkedIn User Privacy Litig.,
5:12-cv-03088-EJD, 2014 WL 1323713 (N.D. Cal. Mar. 18, 2014) 4.4.4.7

In re LinkedIn User Privacy Litig.,
932 F. Supp. 2d 1089 (N.D. Cal. 2013) 6.2.2.3

In Re Marriage Cases,
43 Cal. 4th 757 (2008) 2.2,

In re Microsoft Corp.,
FTC File No. 0123240 (F.T.C. Dec. 24, 2012) 6.3.1

In re MySpace LLC,
FTC File No. 1024369, No. C-4369 (F.T.C. Aug. 30, 2012) 6.3.1

In re Nationwide Mortg. Group, Inc.,
No. 9319, 2005 WL 996696 (F.T.C. Apr. 12, 2005) 2.7.1.4

In re Netflix Privacy Litig.,
No. 5:11-CV-00379 EJD, 2013 WL 1120801 (N.D. Cal. Mar. 18, 2013) 6.2.2.3

In re Pharmatrak, Inc.,
329 F.3d 9 (2003) 2.24.1.3, 2.24.1.4

In re Pomona Valley Med. Grp., Inc.,
476 F.3d 665 (9th Cir. 2007) 6.2.1.3

In re Rolando S.,
197 Cal. App. 4th 936 (Cal. Ct. App. 2011) 2.10

In re Sony Gaming Networks & Customer Data Sec. Breach Litig.,
903 F. Supp. 2d 942 (S.D. Cal. 2012) 6.2.1.1, 6.2.1.3, 6.2.2.1

In re Sony Gaming Networks & Customer Data Sec. Breach Litig.,
996 F. Supp. 2d 942 (S.D. Cal. 2014) 2.15.1.3.3, 2.15.1.4, 6.2.2.3

In re Sunbelt Lending Servs., Inc.,
No. C-4129, 2005 WL 120875 (F.T.C. Jan. 3, 2005) 2.7.1.4
In re Syncor ERISA Litig.,
516 F.3d 1095 (9th Cir. 2008) 6.2.2.3

In re Target Corp. Data Sec. Breach Litig.,
No. MDL 14-2522 PAM/JJK, 2014 WL 7192478 (D. Minn. Dec. 18, 2014) 6.2.2.3

In re Tobacco II Cases,
46 Cal. 4th 298 (2009) 6.2.1.3

In re Toys R Us-Delaware, Inc.—Fair & Accurate Credit Transactions Act (FACTA) Litig.,
295 F.R.D. 438 (C.D. Cal. 2014) 2.7.3.4, 6.2.2.3

In re Toys R Us-Delaware, Inc.—Fair & Accurate Credit Transactions Act (FACTA) Litig.,
300 F.R.D. 347 (C.D. Cal. 2013) 6.2.2.3

In re Twitter, Inc.,
FTC File No. 092 3093 (F.T.C. Mar. 11, 2011) 6.3.1

In re U.S. for an Order Pursuant to 18 U.S.C. § 2703(D),
707 F.3d 283 (4th Cir. 2013) 2.11.2

In re Warrant to Search Certain E-mail Account Controlled and Maintained by Microsoft Corp.,
15 F. Supp. 3d 466 (S.D.N.Y. 2014) 2.11.2

In re Yahoo Mail Litig.,
7 F. Supp. 3d 1016 (N.D. Cal. 2014) 1.3.2, 2.24.1.3, 2.24.2.3

In re Yahoo! Inc. Customer Data Security Breach Litig.,
N.D. Cal. No. 16-md-02752, consolidated class complaint filed 4/13/17 2.15.1.4, 6.2.2.3

In re York,
9 Cal. 4th 1133 (1995) 2.2

In re Zynga Privacy Litig.,
750 F.3d 1098 (9th Cir. 2014) 2.24.1.3

In re: § 2703(d) Order,
787 F. Supp. 2d 430 (E.D. Va. 2011) 2.11.1

In the Matter of TRENDnet, Inc.,
FTC Docket No. C-4426 (Jan. 16, 2014) 2.5.9

Inabnit v. Berkson,
199 Cal. App. 3d 1230 (Cal. Ct. App. 1988) 2.9.2.4

Intel Corp. v. Hamidi,
30 Cal. 4th 1342 (2003) 2.5.10

International Airport Ctrs., L.L.C. v. Citrin,
440 F.3d 418 (7th Cir. 2006) 2.5.10.2.3
International Shoe Co. v. Wash.,
326 U.S. 310 (1945) 6.2.3.2

In the Matter of Google Inc.,
FTC Docket No. C-4336 (Oct. 24, 2011) 4.4.4.4, 5.2.3.4, 6.3.1

Ion Equip. Corp. v. Nelson,
110 Cal. App. 3d 868 (Cal. Ct. App. 1980) 2.24.2.4

Jacqueline Cohen v. Windsor Fashions, Inc.,
Los Angeles Superior Court No. BC381468 (2008) 2.7.9.4

James v. Newspaper Agency Corp.,
591 F.2d 579 (10th Cir. 1979) 2.6

Jewel v. NSA,
No. C 08-04373 JSW,
2019 U.S. Dist. LEXIS 217140 (N.D. Cal. Apr. 25, 2019) 2.8.1

Joffe v. Google, Inc.,
746 F.3d 920 (9th Cir. 2013) 6.2.2.3

Johnson v. Ashley Furniture Indus.,
No. 13-CV-2445-BTM-DHB, 2014 U.S. Dist. LEXIS 156601 (S.D. Cal. Nov. 4, 2014) 2.7.9.3.2

Jones v. Dirty World Entertainment Recording, LLC,
766 F. Supp. 2d 828 (E.D. Ky. 2011) 6.5.1

Jones v. Rath Packing Co.,
430 U.S. 519 (1977) 1.2.2.2

Jones v. Royal Admin. Servs.,
866 F.3d 1100 (9th Cir. 2017) 2.22.3.4

Juhline v. Ben Bridge Jeweler, Inc.,
No. 11cv2906-WQH-NLS, 2012 U.S. Dist. LEXIS 129413 (S.D. Cal. Sept. 7, 2012) 2.7.9.3.2

Katz v. United States,
389 U.S. 347 (1967) 1.3.1, 2.6

Katzberg v. Regents of Univ. of Calif.,
29 Cal. 4th 300 (2002) 2.2.4

Kearney v. Salomon Smith Barney, Inc.,
39 Cal. 4th 95 (2006) 1.2.1, 1.2.2.3, 2.24.2.2, 4.5

Keim v. Trader Joe’s Co.,
No. CV 19-10156 PSG (MRWx),
2020 U.S. Dist. LEXIS 20325 (C.D. Cal. Feb. 5, 2020) 6.2.2.1, 6.2.2.2

Kemp v. Cnty. of Orange,
211 Cal. App. 3d 1422 (Cal. Ct. App. 1989) 2.17.4

Kerwin v. Remittance Assistance Corp.,
559 F. Supp. 2d 1117 (D. Nev. 2008) 2.7.5.4
<table>
<thead>
<tr>
<th>Case</th>
<th>Citation</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kinderstart v. Google</td>
<td>No. C06-2057JFRS, 2007 WL 831806 (N.D. Cal. Mar. 16, 2007)</td>
<td>1.3.4</td>
</tr>
<tr>
<td>Korea Supply Co. v. Lockheed Martin Corp.</td>
<td>29 Cal. 4th 1134</td>
<td>6.2.1.3</td>
</tr>
<tr>
<td>Korn v. Polo Ralph Lauren Corp.</td>
<td>644 F. Supp. 2d 1212 (E.D. Cal. 2008)</td>
<td>2.7.9.3.4</td>
</tr>
<tr>
<td>Krottner v. Starbucks Corp.</td>
<td>628 F.3d 1139 (9th Cir. 2010)</td>
<td>6.2.2.1</td>
</tr>
<tr>
<td>Kwikset Corp. v. Superior Court</td>
<td>51 Cal. 4th 310 (2011)</td>
<td>6.2.1.3</td>
</tr>
<tr>
<td>Kyllo v. United States</td>
<td>533 U.S. 27 (2001)</td>
<td>2.11.1</td>
</tr>
<tr>
<td>LaCourt v. Specific Media, Inc.</td>
<td>2011 WL 2473399 (C.D. Cal. Apr. 28, 2011)</td>
<td>6.2.2.1</td>
</tr>
<tr>
<td>LaCourt v. Specific Media, Inc.</td>
<td>No. SACV 10-1256 GW JCGX, 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011)</td>
<td>6.2.2.1</td>
</tr>
<tr>
<td>Laird v. Tatum,</td>
<td>408 U.S. 1 (1972)</td>
<td>6.2.2.1</td>
</tr>
<tr>
<td>Lane v. Facebook, Inc.</td>
<td>696 F.3d 811 (9th Cir. 2012)</td>
<td>2.23.1.3, 6.2.2.3</td>
</tr>
<tr>
<td>Langdon v. Google</td>
<td>474 F. Supp. 2d 622 (D. Del. 2007)</td>
<td>1.3.4</td>
</tr>
<tr>
<td>Latner v. Mount Sinai Health Sys.</td>
<td>879 F.3d 52 (2d Cir. 2018)</td>
<td>2.22.3.3</td>
</tr>
<tr>
<td>Lawrence v. Texas</td>
<td>539 U. S. 558 (2003)</td>
<td>2.2</td>
</tr>
</tbody>
</table>
Lawson v. Halpern-Reiss, 212 A.3d 1213 (Vt., 2019) 2.9.1.4
Lefkoe v. Jos. A. Bank Clothiers Inc., 577 F.3d 240 (4th Cir. 2009) 6.5.2
Lin v. Universal Card Servs. Corp., 238 F. Supp. 2d 1147 (N.D. Cal. 2002) 2.7.4.4
Long Beach Police Officers Assn. v. City of Long Beach, 59 Cal. 4th 59 (2014) 2.19.6.5
Low v. LinkedIn Corp., 2011 WL 5509848 (N.D. Cal. Nov. 11, 2011) 6.2.2.1
Low v. LinkedIn Corp., 900 F. Supp. 2d 1010 (N.D. Cal. 2012) 2.2.3, 6.2.1.1, 6.2.2.3
Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992) 6.2.2.1
LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009) 2.5.10.1.4, 2.5.10.2.3
Maine v. Taylor, 477 U.S. 131 (1986) 1.2.2.2
Mapp v. Ohio, 367 U.S. 643 (1961) 6.4.2.1
Maracich v. Spears, 133 S. Ct. 2191 (2013) 2.19.4.4
Marks v. Crunch San Diego, LLC, 904 F.3d 1041 (9th Cir. 2018) 2.22.3, 2.22.3.3
<table>
<thead>
<tr>
<th>Case Name</th>
<th>Citation</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marks v. Jaffa</td>
<td>6 Misc. 290, 26 N.Y.S. 908</td>
<td>6.2.1.1</td>
</tr>
<tr>
<td>(Super. Ct. N.Y. City 1893)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Martinez v. Combs</td>
<td>49 Cal. 4th 35 (2010)</td>
<td>2.4.3.6, 2.6.2.2</td>
</tr>
<tr>
<td>Maryland v. Louisiana</td>
<td>451 U.S. 725 (1981)</td>
<td>1.2.2.2</td>
</tr>
<tr>
<td>Masuda v. Citibank, N.A.</td>
<td>38 F. Supp. 3d 1130 (N.D. Cal. 2014)</td>
<td>2.7.6.2</td>
</tr>
<tr>
<td>McDonald v. Aps</td>
<td>385 F. Supp. 3d 1022 (N.D. Cal. 2019)</td>
<td>2.2.3</td>
</tr>
<tr>
<td>McLaren v. Microsoft Corp.,</td>
<td>No. 05-97-00824-CV, 1999 Tex. App. LEXIS 4103 (May 28, 1999)</td>
<td>2.6.1</td>
</tr>
<tr>
<td>Medellin v. IKEA U.S.A. W., Inc.,</td>
<td>672 F. App’x 782 (9th Cir. 2017)</td>
<td>2.7.9.4</td>
</tr>
<tr>
<td>Metter v. Los Angeles Exam’r</td>
<td>35 Cal. App. 2d 304 (Cal. Ct. App. 1939)</td>
<td>6.2.1.1</td>
</tr>
<tr>
<td>Meyer v. Sprint Spectrum L.P.,</td>
<td>45 Cal. 4th 634 (2009)</td>
<td>6.2.1.3</td>
</tr>
<tr>
<td>Miles v. United States</td>
<td>103 U.S. 304 (1880)</td>
<td>6.4.1</td>
</tr>
<tr>
<td>Miller v. Hearst Comm’ns Inc.,</td>
<td>554 F. App’x 657 (9th Cir. 2014)</td>
<td>2.26.3</td>
</tr>
<tr>
<td>Milwaukee Cnty. v. M.E. White Co.,</td>
<td>296 U.S. 268 (1935)</td>
<td>1.2.2.4</td>
</tr>
<tr>
<td>Monsanto Co. v. Geertson Seed Farms,</td>
<td>561 U.S. 139 (2010)</td>
<td>6.2.2.1</td>
</tr>
</tbody>
</table>

611
Morey v. Louis Vuitton N. Am., Inc.,
461 Fed. App’x 642 (9th Cir. 2011) 2.7.9.4

Multiven, Inc. v. Cisco Sys., Inc.,
725 F. Supp. 2d 887 (N.D. Cal. 2010) 2.5.10.1.4, 2.5.10.2.3

Murray v. Time Inc.,
554 F. App’x 654 (9th Cir. 2014) 2.26.3

Muy v. IBM,
No. 4:19cv14-MW/CAS,
2019 U.S. Dist. LEXIS 228904 (N.D. Fla. Nov. 25, 2019) 2.13, 4.4.5, 4.4.6

MySpace, Inc. v. The Globe.com, Inc.,
No. CV 06-3391-RGK, 2007 WL 1686966 (C.D. Cal. Feb. 27, 2007) 2.22, 2.22.1.3.1

MySpace, Inc. v. Wallace,
498 F. Supp. 2d 1293 (C.D. Cal. 2007) 2.22, 2.22.1.3.1, 2.22.1.4.4

Narayan v. EGL, Inc.,
616 F.3d 895 (9th Cir. 2010) 2.6.2.2

Nathan Van Buren v. United States,
141 S.Ct. 1648 (2021) 2.5.10.2.3

National Basketball Ass’n v. Motorola, Inc.,
105 F.3d 841 (2d Cir. 1997) 1.3.3

Newcombe v. Adolf Coors Co.,
157 F.3d 686 (9th Cir. 1998) 2.21.1.4

Nix v. Williams,
467 U.S. 431 (1984) 6.4.2.1

Noble v. Sears, Roebuck & Co.,
33 Cal. App. 3d 654 (Cal. Ct. App. 1973) 2.17.3, 2.17.4

North Alaska Salmon Co. v. Pillsbury,
174 Cal. 1 (1916) 1.2.2.3

Norwest Mortgage, Inc. v. Superior Court,

O’Connor v. Ortega,
480 U.S. 709 (1987) 2.6, 2.6.1

Ojala v. Bohlin,

Oliver v. United States,
466 U.S. 170 (1980) 2.6.1

Olmstead v. United States,
277 U.S. 438 (1928) 1.3.1, 2.11.1

Oman v. Delta Air Lines, Inc.,
230 F. Supp. 3d 986, 992–93 (N.D. Cal. 2017) 2.6.2.2
### Table of Cases

**Omega World Travel, Inc. v. Mummagraphics, Inc.,**  
469 F.3d 348 (4th Cir. 2006)  

**O’Neil v. Comcast Corp.,**  
No. 18 C 4249, 2019 U.S. Dist. LEXIS 31031  
(N.D. Ill. Feb. 27, 2019) (Chapter 7)  

534 U.S. 426 (2002)  

**Pacific Aerospace & Elecs., Inc. v. Taylor,**  

**Party City Corp. v. Superior Court,**  

**Patriotic Veterans, Inc. v. Indiana,**  
736 F.3d 1041 (7th Cir. 2013)  

**Pavesich v. New England Life Ins. Co.,**  
122 Ga. 90, 50 S.E. 68 (Ga. 1905)  

**Pavlovich v. Superior Court,**  
29 Cal. 4th 262 (2002)  

**People ex rel. Bill Lockyer v. Fremont Life Ins. Co.,**  
as modified on denial of reh’g (Jan. 16, 2003)  

**People ex rel. Lynch v. San Diego Unified Sch. Dist.,**  

**People of the State of California v. Target Corporation,**  

**People v. Barba,**  

**People v. Barnes,**  

**People v. Childs,**  

**People v. Delta Air Lines, Inc.,**  
No. CGC-12-526741 (Sup. Ct. SF Cnty. Dec. 6, 2012)  

**People v. Delta Air Lines, Inc.,**  

**People v. Diaz,**  

**People v. Drennan,**  

**People v. Ferguson,**  
People v. Galvadon,
103 P.3d 923 (Colo. 2005) 2.6.1

People v. Gibbons,

People v. Guzman,
11 Cal. App. 5th 184, 192-94, 196
(Cal. Ct. App. 2011) 2.24.2.4

People v. Nakai,

People v. Nazary,

People v. Stipo,

Perkey v. Dep’t of Motor Vehicles,
42 Cal. 3d 185 (Cal. 1986) 2.19.5.3

Perkins v. LinkedIn Corp.,
No. 13-CV-04303-LHK, 2014 WL 2751053
(N.D. Cal. June 12, 2014) 6.2.2.3

Pettus v. Cole,
49 Cal. App. 4th 402 (1996) 2.2.1

Pierce v. Superior Court,
1 Cal. 2d 759 (1934) 6.3.2

Pike v. Bruce Church, Inc.,
397 U.S. 137 (1970) 1.2.2.2

Pineda v. Williams-Sonoma Stores, Inc.,
51 Cal. 4th 524 (2001) 1.5.2, 2.7.9.1, 2.7.9.3, 6.2.2.3

Pioneer Electronics (USA), Inc. v. Superior Court,
40 Cal. 4th 360 (2007) 1.3.1

Planned Parenthood v. Aakhus,
14 Cal. App. 4th 162 (Cal. Ct. App. 1993) 2.2.4

Planned Parenthood v. Casey,
505 U.S. 833 (1992) 2.2

PLIVA, Inc. v. Mensing,
131 S. Ct. 2567 (2011) 1.2.2.2

Porten v. Univ. of San Francisco,
64 Cal. App. 3d 825 (Cal. Ct. App. 1976) 2.2

Poulin v. The Thomas Agency,
760 F. Supp. 2d 151 (D. Me. 2011) 2.7.5.4

Powers v. Pottery Barn, Inc.,
177 Cal. App. 4th 1039 (Cal. Ct. App. 2009) 2.7.9
<table>
<thead>
<tr>
<th>Case</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prager Univ. v. Google LLC,</td>
<td>2.2.2</td>
</tr>
<tr>
<td>951 F.3d 991 (9th Cir. 2020)</td>
<td></td>
</tr>
<tr>
<td>Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC,</td>
<td>2.6.1</td>
</tr>
<tr>
<td>Raines v. Byrd,</td>
<td>6.2.2.1</td>
</tr>
<tr>
<td>521 U.S. 811 (1997)</td>
<td></td>
</tr>
<tr>
<td>Redner v. Workmen’s Comp. Appeals Bd.,</td>
<td>2.17.4</td>
</tr>
<tr>
<td>5 Cal. 3d 83 (1972)</td>
<td></td>
</tr>
<tr>
<td>Rees v. Souza’s Milk Transp., Co.,</td>
<td>2.5.4.1</td>
</tr>
<tr>
<td>No. 1:05-CV-00297AWITAG, 2006 WL 3251829</td>
<td></td>
</tr>
<tr>
<td>(E.D. Cal. Nov. 8, 2006)</td>
<td></td>
</tr>
<tr>
<td>Reich v. Purcell,</td>
<td>1.2.2.3</td>
</tr>
<tr>
<td>67 Cal 2d. 551 (1967)</td>
<td></td>
</tr>
<tr>
<td>Reid v. Superior Court,</td>
<td>2.19.6.6</td>
</tr>
<tr>
<td>Reilly v. Ceridian Corp.,</td>
<td>6.2.2.1</td>
</tr>
<tr>
<td>664 F.3d 38 (3d Cir. 2011)</td>
<td></td>
</tr>
<tr>
<td>Reit v. Yelp!, Inc.,</td>
<td>6.5.1</td>
</tr>
<tr>
<td>Renne v. Geary,</td>
<td>2.12.3</td>
</tr>
<tr>
<td>501 U.S. 312 (1991)</td>
<td></td>
</tr>
<tr>
<td>Reno v. American Civil Liberties Union,</td>
<td>6.5.1</td>
</tr>
<tr>
<td>521 U.S. 844 (1997)</td>
<td></td>
</tr>
<tr>
<td>Reno v. Condon,</td>
<td>2.19.4, 2.19.4.2</td>
</tr>
<tr>
<td>528 U.S. 141 (2000)</td>
<td></td>
</tr>
<tr>
<td>Revitch v. New Moosejaw, LLC.,</td>
<td>2.2.3</td>
</tr>
<tr>
<td>No. 18-cv-06827-VC, 2019 U.S. Dist. LEXIS 186955</td>
<td></td>
</tr>
<tr>
<td>(N.D. Cal. Oct. 23, 2019)</td>
<td></td>
</tr>
<tr>
<td>Richardson-Tunnell v. Schools Ins. Program for Emps.,</td>
<td>2.2.4</td>
</tr>
<tr>
<td>Richmond v. Dart Indus., Inc.,</td>
<td>6.2.2.3</td>
</tr>
<tr>
<td>29 Cal. 3d 462 (1981)</td>
<td></td>
</tr>
<tr>
<td>Riley v. California,</td>
<td>2.11.1</td>
</tr>
<tr>
<td>134 S. Ct. 2473 (2014)</td>
<td></td>
</tr>
<tr>
<td>Robins v. Spokeo, Inc.,</td>
<td>6.2.2.1</td>
</tr>
<tr>
<td>742 F.3d 409 (9th Cir. 2014)</td>
<td></td>
</tr>
<tr>
<td>Roe v. Wade,</td>
<td>1.3.1, 2.2</td>
</tr>
<tr>
<td>410 U.S. 113 (1972)</td>
<td></td>
</tr>
<tr>
<td>Rojas v. FAA,</td>
<td>2.8.1, 2.19.1</td>
</tr>
<tr>
<td>941 F.3d 392 (9th Cir. 2019)</td>
<td></td>
</tr>
</tbody>
</table>
No. 06CV1505 IEG (WMc), 2007 U.S. Dist. LEXIS 77144
(S.D. Cal. Oct. 16, 2007) 2.7.9.3.4

Rosario v. U.S.,
538 F. Supp. 2d 480 (D. P.R. 2008) 2.6.1

No. CV 11-03617 SJO (RZx), 2011 U.S. Dist. LEXIS 134515
(C.D. Cal. Nov. 17, 2011) 2.7.9.4

Roybal v. Equifax,
405 F. Supp. 2d 1177 (E.D. Cal. 2005) 2.7.4.4

Rubio v. Capital One Bank,
613 F.3d 1195 (9th Cir. 2010) 2.16.3.4

Ruiz v. Gap, Inc.,
380 F. App’x 689 (9th Cir. 2010), affirming

Ruiz v. Gap, Inc.,
622 F. Supp. 2d 908 (N.D. Cal. 2009) aff’d,
380 F. App’x 689 (9th Cir. 2010) 6.2.1.1

Ryan v. Jersey Mike’s Franchise Sys.,
No. 13-CV-1427-BEN WVG, 2014 WL 1292930
(S.D. Cal. Mar. 28, 2014) 2.22.6.4

Safari Club Int’l v. Rudolph,
845 F.3d 1250 (9th Cir. 2017) 1.5.3, 2.24.2, 2.24.2.3

Salmonson v. Microsoft Corp.,
(C.D. Cal. Jan. 6, 2012) 2.7.9.2

Samaniego v. Empire Today LLC,
205 Cal. App. 4th 1138 (2012) 1.5.4

Sams v. Yahoo! Inc.,
713 F.3d 1175 (9th Cir. 2011) 2.11.2

Sanders v. American Broadcasting Cos.,
20 Cal. 4th 907 (1999) 2.6.1

Sarver v. Experian Info Sys.,
390 F.3d 969 (7th Cir. 2004) 2.7.3.4

Saulic v. Symantec Corp.,
596 F. Supp. 2d 1323 (C.D. Cal. 2009) 2.7.9.2

Schnall v. Hertz Corp.,

Schwarzenegger v. Fred Martin Motor Co.,
374 F.3d 797 (9th Cir. 2004) 6.2.3.2
<table>
<thead>
<tr>
<th>Case Name</th>
<th>Citation</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.G. Borello &amp; Sons, Inc. v. Dept’t of Indus. Relations,</td>
<td>48 Cal. 3d 341 (1989)</td>
<td>2.6.2.2</td>
</tr>
<tr>
<td>Shabaz v. Polo Ralph Lauren Corp.,</td>
<td>586 F. Supp. 2d 1205 (C.D. Cal. 2008)</td>
<td>2.7.9.3.1, 2.7.9.4</td>
</tr>
<tr>
<td>Sheehan v. San Francisco 49ers, Ltd.</td>
<td>45 Cal. 4th 992 (2009)</td>
<td>2.2.3</td>
</tr>
<tr>
<td>Shelley v. Kraemer,</td>
<td>334 U.S. 1, 13 (1948)</td>
<td>2.2.2</td>
</tr>
<tr>
<td>Shulman v. Grp. W Prods., Inc.,</td>
<td>18 Cal. 4th 200 (1998)</td>
<td>2.21.1.1, 2.21.1.2, 2.27.1.3, 6.2.1.1</td>
</tr>
<tr>
<td>Siegler v. Best Buy Co. of Minnesota,</td>
<td>519 F. App’x 604 (11th Cir. 2013)</td>
<td>6.2.2.3</td>
</tr>
<tr>
<td>Sinibaldi v. Redbox Automated Retail, LLC,</td>
<td>754 F.3d 703 (9th Cir. 2014)</td>
<td>2.7.9.2, 2.7.9.3.3</td>
</tr>
<tr>
<td>Smith v. LoanMe, Inc.,</td>
<td>43 Cal. App. 5th 844, 257 Cal. Rptr. 3d 61 (2019)</td>
<td>2.24.2.3, 2.24.2.4</td>
</tr>
<tr>
<td>Smith v. Maryland,</td>
<td>442 U.S. 735 (1979)</td>
<td>2.11.1, 2.24.1.1</td>
</tr>
<tr>
<td>Solano v. Playgirl, Inc.,</td>
<td>292 F.3d 1078 (9th Cir. 2002)</td>
<td>2.21.1.3, 6.2.1.1</td>
</tr>
<tr>
<td>Southern California Acoustics Co., Inc. v. C. V. Holder, Inc.,</td>
<td>71 Cal. 2d 719 (1969)</td>
<td>5.2.3.4</td>
</tr>
<tr>
<td>Specht v. Netscape,</td>
<td>306 F.3d 17 (2d Cir. 2002)</td>
<td>5.2.5.3</td>
</tr>
</tbody>
</table>
Speyer v. Avis Rent a Car Sys., Inc.,
415 F. Supp. 2d 1090 (S.D. Cal. 2005) 1.2.2.3

Spokeo, Inc. v. Robins,
2015 WL 1879778 (April. 27, U.S.) 6.2.2.1

Sporer v. UAL Corp.,
No. C 08-02835, 2009 U.S. Dist. LEXIS 76852 (N.D. Cal. Aug. 27, 2009) 2.6.1

Stanley v. Georgia,
395 U.S. 557 (1969) 1.3.1

State ex rel. Stenehjem v. FreeEats.com, Inc.,
712 N.W.2d 828 (N.D. 2006) 2.22.3

Stearns v. Ticketmaster Corp.,
655 F.3d 1013 (9th Cir. 2011) 6.2.2.3

Sterk v. Redbox Automated Retail, LLC,
770 F.3d 618 (7th Cir. 2014) 2.23.1.2, 2.23.1.3

Stratton Oakmont, Inc. v. Prodigy Services Co.,
1995 WL 323710 (N.Y. Sup. Ct. 1995) 6.5.1

Sullivan v. Oracle Corp.,
51 Cal. 4th 1191 (2001) 2.6.2.2

Summers v. Earth Island Inst.,
555 U.S. 488 (2009) 6.2.2.1

Svenson v. Google Inc.,
No. 13-CV-04080-BLF, 2014 WL 3962820 (N.D. Cal. 2014) 2.12.3, 4.2.1

Sweet v. LinkedIn Corp., N.D. Cal.,
No. 5:14-cv-04531-PSG, 2015 WL 1744254 (N.D. Cal. April 4, 2014) 2.7.3.2

Taus v. Loftus,
40 Cal. 4th 683 (2007) 2.17.1

Taylor v. Bureau of Private Investigators & Adjusters,

TBG Ins. Servs. Corp. v. Sup. Ct.,

The People of the State of California v. Citibank,
No. RG13693591 (Cal. Super. Aug. 28, 2013) 2.7.1.4, 6-3.2

The People of the State of California v. Delta Air Lines, Inc.,
2012 WL 6061446 No. CGC-12-526741 (Cal. Super.) 1.2.2.2, 6.3.2

The People of the State of California v. Kaiser Foundation Health Plan, Inc.,
2014 WL 323740 No. RG14711370 6.3.2
<table>
<thead>
<tr>
<th>Case</th>
<th>Key Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>The TJX Companies Inc. v. Superior Court</td>
<td>2.7.9.4</td>
</tr>
<tr>
<td>Thompson v. Johnson Cnty. Cnty. Coll.</td>
<td>2.6.1</td>
</tr>
<tr>
<td>Thoms v. Walgreen Co.</td>
<td>2.7.9.3</td>
</tr>
<tr>
<td>Ticketmaster Corp. v. Tickets.com</td>
<td>2.5.10.2.3</td>
</tr>
<tr>
<td>Ticketmaster, LLC v. RMG Techs., Inc.</td>
<td>2.5.10</td>
</tr>
<tr>
<td>TJX Cos., Inc. v. Superior Court</td>
<td>2.7.9.4</td>
</tr>
<tr>
<td>Tom v. City and Cnty. of San Francisco</td>
<td>2.2, 2.2.3</td>
</tr>
<tr>
<td>Trammell v. Citizen’s News Co., Inc.</td>
<td>6.2.1.1</td>
</tr>
<tr>
<td>Travelers Ins. Co. v. Work. Comp. App. Bd.</td>
<td>1.2.2.3</td>
</tr>
<tr>
<td>Travis v. Reno</td>
<td>2.19.4.4</td>
</tr>
<tr>
<td>Trujillo v. City of Ontario</td>
<td>2.7.4.4</td>
</tr>
<tr>
<td>Tucker v. Pac. Bell Mobile Servs.</td>
<td>6.2.1.3</td>
</tr>
<tr>
<td>Turnbull v. ABC</td>
<td>2.27.1.2</td>
</tr>
<tr>
<td>U.S. Parole Comm’n v. Geraghty</td>
<td>6.2.2.3</td>
</tr>
<tr>
<td>U.S. v. Councilman</td>
<td>2.24.1.3, 6.4.1</td>
</tr>
<tr>
<td>U.S. v. Drew</td>
<td>2.5.10, 2.5.10.2.3</td>
</tr>
<tr>
<td>U.S. v. Jones</td>
<td>2.11.1</td>
</tr>
</tbody>
</table>
U.S. v. Miller,
425 U.S. 435 (1976) 2.7.7, 2.11.1

U.S. v. Taketa,
923 F.2d 665 (9th Cir. 1991) 2.6.1

United States Golf Ass’n v. Arroyo Software Corp.,
69 Cal. App. 4th 607 (1999) 1.3.3

United States of America v. HireRight Solutions, Inc.,
No. 112-cv-01313 (D.D.C. Aug. 8, 2012) 2.7.3.4

United States of America v. Spokeo, Inc.,
No. CV12-05001 (C.D. Cal. June 7, 2012) 2.7.3.2, 2.7.3.4

United States v. Aguilar,
756 F.2d 1418 (9th Cir. 1985) 1.2.2.1

United States v. Barrows,
481 F.3d 1246 (10th Cir. 2007) 2.6.1

United States v. Cella,
568 F.2d 1266 (9th Cir. 1977) 6.4.2.1

United States v. Fregoso,
60 F.3d 1314 (8th Cir. 1995) 6.4.2.2

United States v. Glassdoor, Inc. (In re Grand Jury Subpoena),
875 F.3d 1179 (9th Cir. 2017) 2.11.2

United States v. Jacobsen,
466 U.S. 109 (1984) 2.11.1

United States v. Jones,
565 U.S. 400 (2012), 2.2, 2.11.1, 2.13, 2.13.1.3

United States v. Jones,
132 S. Ct. 945 (2012) 1.3.1, 2-2, 2-13, 2-13.1.3, 6.4.2.1

United States v. Leija-Sanchez,
602 F.3d 797 (7th Cir. 2010) 1.2.2.1

United States v. Miller,
425 U.S. 435 (1976) 2.11.1

109 F.3d 1 (1st Cir. 1997) 1.2.2.1

United States v. Nosal,
676 F.3d 854 (9th Cir. 2012) 2.5.10.2.3

United States v. Standefer,
No. 06-CR-2674-H, 2007 WL 2301760
(S.D. Cal. Aug. 8, 2007) 1.3.2

United States v. Verdugo-Urquidez,
52 La. L. Rev. 455 (1991) 2.2, 2-11.1
<table>
<thead>
<tr>
<th>Case</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States v. Verdugo-Urquidez</td>
<td>2.2, 2-11.1</td>
</tr>
<tr>
<td>United States v. Verdugo-Urquidez</td>
<td>2.2, 2.8.1, 2.11.1</td>
</tr>
<tr>
<td>United States v. Warshak</td>
<td>2.11.1, 2.11.2</td>
</tr>
<tr>
<td>USA v. Michael Marr et. al., Case No. 14-cr-00580-PJH, Pretrial Order No. 3 (N.D. California 2016)</td>
<td>1.5.3</td>
</tr>
<tr>
<td>Van Patten v. Vertical Fitness Grp., LLC, No. 12CV1614-LAB MDD, 2014 WL 2116602 (S.D. Cal. May 20, 2014)</td>
<td>2.22.6.4</td>
</tr>
<tr>
<td>Van Patten v. Vertical Fitness Grp., LLC, 2017 BL 26058 (9th Cir., No. 14-55980, 1/30/17)</td>
<td>2.22.3.4</td>
</tr>
<tr>
<td>Vega-Rodriguez v. P.R. Tel. Co., 110 F.3d 174 (1st Cir. 1997)</td>
<td>2.6.1</td>
</tr>
<tr>
<td>Vera v. O'Keefe, 791 F. Supp. 2d 959 (S.D. Cal. 2011)</td>
<td>2.24.2.4</td>
</tr>
<tr>
<td>Vergara v. Uber Techs. Inc., No. 1:15-CV-06942 (N.D. Ill. May. 19, 2016)</td>
<td>2.22.3.4</td>
</tr>
<tr>
<td>Vons Cos., Inc. v. Seabest Foods, Inc., 14 Cal. 4th 434 (1996)</td>
<td>6.2.3.2</td>
</tr>
<tr>
<td>W. Lynn Creamery, Inc. v. Healy, 512 U.S. 186 (1994)</td>
<td>1.2.2.2</td>
</tr>
<tr>
<td>Warth v. Seldin, 422 U.S. 490 (1975)</td>
<td>6.2.2.1</td>
</tr>
<tr>
<td>Washington Mut. Bank, FA v. Superior Court, 24 Cal. 4th 906 (2001)</td>
<td>6.2.2.3</td>
</tr>
<tr>
<td>Watson v. Employers Liability Assurance Corp., 348 U.S. 66 (1954)</td>
<td>1.2.2.3</td>
</tr>
</tbody>
</table>
Wayne v. Bureau of Private Investigators & Adjusters,
201 Cal. App. 2d 427 (Cal. Ct. App. 1962) 2.17.3, 2.17.4

Weiner v. ARS Nat. Servs., Inc.,
887 F. Supp. 2d 1029 (S.D. Cal. 2012) 2.24.2.4

Whalen v. Roe,
429 U.S. 589 (1977) 1.3.1, 2.2

White v. Davis,
13 Cal. 3d 757 (1975) 2.2.1, 2.2.3, 2.2.4

White v. Experian Info. Solutions, Inc.,
Nos. 05-CV-1070, 05-CV-1073, 05-CV-7821, 06-CV-3924, 05-CV-1172, 06-CV-5060 2011 WL 10796643 (C.D. Cal. Sept. 15, 2011) 2.7.3.4

White v. Samsung Electronics Am., Inc.,
971 F.2d 1395 (9th Cir. 1992) 2.21.1.4, 6.2.1.1

Wilhelm v. Pray, Price, Williams & Russell,

Williams v. City of Tulsa,
393 F. Supp. 2d 1124 (N.D. Okla. 2005), aff’d, 204 Fed. App’x 762 (10th Cir. 2006) 2.6.1

Williams v. Superior Court,
__ Cal. 5th __ (July 13, 2017, S227228 Cal. Supreme Court) 2.11.2

Wilner v. Sunset Life Ins. Co.,

Wilson v. Hewlett-Packard Co.,
668 F.3d 1136 (9th Cir. 2012) 6.2.1.3

Wilson v. Superior Court,
51 Cal. App. 4th 1136 (Ct. App. 1996) 2.19.6.5

Winston v. Lee,
470 U.S. 753 (1985) 1.3.1

Woodbridge Structured Funding, LLC v. Pissed Consumer,
N.Y.S.2d, 2015 WL 686383 (February 19, 2015) 6.5.2

Yahoo! Inc. v. La Ligue contre Le Rasisme et L’Antisemitisme,
433 F.3d 1199 (9th Cir. 2006) 1.2.2.4

Yelp, Inc. v. Hadeed Carpet Cleaning, Inc.,

Yeoman v. Ikea U.S.A. West, Inc.,
No. 11-cv-00701-BAS (BGS), 2014 U.S. Dist. LEXIS 168968 (S.D. Cal. Dec. 4, 2014) 2.7.9.3, 2.7.9.4
<table>
<thead>
<tr>
<th>Case</th>
<th>Citation</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yunker v. Pandora Media, Inc.</td>
<td>No. 11-CV-03113 JSW, 2013 WL 1282980</td>
<td>6.2.1.3</td>
</tr>
<tr>
<td></td>
<td>(N.D. Cal. Mar. 26, 2013)</td>
<td></td>
</tr>
<tr>
<td>Zeran v. America Online, Inc.</td>
<td>129 F.3d 327 (4th Cir. 1997)</td>
<td>6.5.1</td>
</tr>
<tr>
<td>Zhang v. Baidu,</td>
<td>No. 11 CIV. 3388 JMF, 2014 WL 1282730</td>
<td>1.3.4</td>
</tr>
<tr>
<td></td>
<td>(S.D.N.Y. Mar. 28, 2014)</td>
<td></td>
</tr>
</tbody>
</table>
Index

A
ABORTION, 2.2, 2.2.3, 2.24.7
ADAD (AUTOMATIC DIALING-ANNOUNCING DEVICE), 2.22.4.
See also ROBOCALLING LAW (STATE)
AFFIRMATIVE CONSENT, 2.13, 2.22.7, 2.23.2.3, 4.4.4.2.3, 4.4.6, 5.2.2, 5.2.3.5, 7.2.2.5. See also CONSENT FORMS, DRAFTING OF
AGENCIES (FEDERAL), 6.3
   FEC enforcement actions, 6.3.1
   FTC, 6.3.1
   state AG enforcement actions, 6.3.2
AGENCIES (STATE)
   access to records maintained by, 2.19.6.1
   CalOPPA coverage and notice requirements, 2.16.3.1-2.16.3.4
   legislative proposals
      on data security, 2.18.1
      on data sharing, collection and coordination, 2.18.3
      on information privacy, 2.18.2
AGREEMENTS, 4.2.3, 5.3. See also PRIVACY NOTICES, DRAFTING OF; PRIVACY POLICIES, DRAFTING OF
   commercial agreements, 5.3.4
   consent instead of, 5.3.3
   with data subjects vs. consent from data subjects, 5.3.1
   express acceptance vs. general privacy notices, 5.3.2
   terms
      agreements between data controllers, 5.3.8
      data processing services, 5.5.6
      data subprocessing, 5.3.6
      by law and compliance agendas, 5.3.8
AIRLINE Deregulation Act (FEDERAL), 6.3.2
AIRSPACE PRIVACY, 2.21.1.5, 2.27.1.3
ALL WRITS ACT, 2.11.2
ALLEN, ANITA L., 1.3.1
ALUMNI, OF STATE UNIVERSITY SYSTEM
  - opt-out notice for mailings, 2.22
    - unsolicited marketing communications to, 2.22.9
ANTI-DISCRIMINATION LAWS, EMPLOYEE PRIVACY AND, 2.6.5.7
ANTI-PHISHING LAW (STATE), 2.16.6.1
ANTI-SPAM ACT (FEDERAL), 1.2.2.1, 2.22.1
  - compliance, 2.22.1.2, 2.22.1.3
    - email messages covered, 2.22.1.3.1
    - header information, 2.22.1.3.2
    - notice documentation, 4.2.3
    - opt-out option, 2.22.1.3.3
    - sexually explicit messages, 2.22.1.3.4
  - data protection, 2.22.1.1
  - sanctions and remedies, 2.22.1.4
    - by FTC, 2.22.1.4.2
    - multiple emails, 2.22.1.4.1
    - provider of internet access services, 2.22.1.4.4
    - sexually explicit messages, 2.22.1.4.5
    - by state, 2.22.1.4.3
ANTI-SPAM LAW (STATE), 2.22.2
  - compliance, 2.22.2.2, 2.22.2.3
  - notice documentation, 4.2.3
  - data protection, 2.22.2.1
  - sanctions and remedies, 2.22.2.4
AREIAS CREDIT CARD FULL DISCLOSURE ACT OF 1986, 2.7.11
  - compliance, 2.7.11.2, 2.7.11.3
  - data protection, 2.7.11.1
  - sanctions and remedies, 2.7.11.4
ARTICLE I (STATE CONSTITUTION), 2.2
  - compliance, 2.2.2, 2.2.3
  - data protection, 2.2.1
  - sanctions and remedies, 2.2.4
ARTICLE III (FEDERAL CONSTITUTION) STANDING DOCTRINE, 6.2.2.1
ASSEMBLY BILLS, PROPOSED (STATE)
on anonymized trip date, 2.18.2
on broad privacy protection, 2.18.2
on CalECPA, 2.18.4
on contact tracing, 2.18.3, 2.18.4
on CPPA expertise, 2.18.2
on data broker and transfer, 2.18.2
on data information research, 2.18.3
on data security, 2.18.1
on data sharing, collection and coordination, 2.18.3
on information privacy, 2.18.2
on insurance privacy, 2.18.3
on protection of children online, 2.18.2
on shielding children, 2.18.3

AUTOMATED LICENSE PLACE READERS, 2.5.5, 2.5.5.2, 2.13, 2.15.1.12.15.1.4, 2.19.6.9

AUTOMOBILE BLACK BOXES, LOCATION DATA FROM, 2.13, 2.13.2
   compliance, 2.13.2.2, 2.13.2.3
data protection, 2.13.2.1
   sanctions and remedies, 2.13.2.4

AUTOMOBILE (RENTAL CAR) ELECTRONIC SURVEILLANCE LAW (STATE), 2.13, 2.13.4
   compliance, 2.13.4.2, 2.13.4.3
data protection, 2.13.4.1
   sanctions and remedies, 2.13.4.4

AUTONOMY PRIVACY ("BEING LET ALONE"), 1.3.1, 2.2
   compliance, 2.2, 2.3.2, 2.3.3
data protection, 2.3.1
   sanctions and remedies, 2.3.4

AVIATION AND TRANSPORTATION SECURITY ACT OF 2001, 2.8.1

B

BACKGROUND CHECKS/CONSUMER REPORTS
   alerts, by consumer credit report agency, 2.5.4.1
   CCRAA (state), 2.7.4
      compliance, 2.7.4.2, 2.7.4.3
data protection, 2.7.4.1
sanctions and remedies, 2.7.4.4
consent, 5.2.1
employee privacy, accommodations by employers, 2.6.5.3, 2.7
FCRA (federal), 2.7.3
  compliance, 2.7.3.2, 2.7.3.3
data protection, 2.7.3.1
sanctions and remedies, 2.7.3.4

BANK SECRECY ACT, 2.7.12

BANKS/FINANCIAL INSTITUTIONS, REGULATION OF
FIPA (state), 2.7.2
  compliance (sharing with affiliates/nonaffiliates), 2.7.2.2, 2.7.2.3
data protection, 2.7.2.1
sanctions and remedies, 2.7.2.4
GLBA (federal), 2.7.1
  compliance, 2.7.1.2, 2.7.1.3
data protection, 2.7.1.1
sanctions and remedies, 2.7.1.4

BIVENS ACTION, 6.4.2.1

“BOOK SERVICES” PRIVACY (STATE), 2.23.2
  compliance, 2.23.2.2, 2.23.2.3
data protection, 2.23.2.1
sanctions and remedies, 2.23.2.4

BOT DISCLOSURE LAW, 4.9

BRANDEIS, LOUIS, 1.3.1, 2.21, 6.2.1.1

BULLYING. See CYBERBULLYING

C

CAADCA (CALIFORNIA AGE-APPROPRIATE DESIGN CODE ACT), 2.16.4

CABLE COMMUNICATIONS POLICY ACT OF 1984, 2.23.4

CALEPICA (CALIFORNIA ELECTRONIC COMMUNICATIONS PRIVACY ACT), 2.11.2

CALOPPA (CALIFORNIA ONLINE PRIVACY PROTECTION ACT), 1.2.2.2, 2.16.2
  Airline Deregulation Act (federal) and, 2.16.3.2.5, 6.3.2
Index

applicability of, 1.2.2.3
causes of action, 6.2.1.3
compliance, 2.16.3.2, 2.16.3.3
  businesses, websites/online services for, 2.16.3.2
  children, websites/online services for, 2.16.3.2.4
  data processors, 2.16.3.2.2
  exemptions, under federal law, 2.16.3.2.5
  passive websites, 2.16.3.2.1
data protection, 2.16.3.1
sanctions and remedies, 2.16.3.4
website privacy notices, 4.2.3, 4.4.1
  business-to-business sharing, 4.4.3
  cookies and tracking pixels, 4.4.4.7
  data categories, 4.4.4.1
  data security, 4.4.4.8
  data sharing under CalOPPA, 4.4.4.2.1
  do not track signals, 4.4.6
  effective date, 4.4.4.5
  notice of material changes to, 4.4.4.4

CALIFORNIA
  Constitution, 2.2, 6.3.2
  demographics, 1.2
  “long arm” statute, jurisdiction, 6.2.3.2
  personal jurisdiction, in private civil litigation, 6.3
    personal jurisdiction, 6.2.3.2
    subject matter jurisdiction, 6.2.3.1
  state laws, scope and applicability, 1.2.2
    conflict of law rules, 1.2.2.3
    enforceability outside state, 1.2.2.4
    under federal law, 1.2.2.2
    under international law, 1.2.2.1
  state laws made by, 1.2.1

CALIFORNIA AGE-APPROPRIATE DESIGN CODE ACT (CAADCA), 2.16.4

CALIFORNIA ANTI-PHISHING ACT OF 2005, 2.16.6.1
CALIFORNIA ATTORNEY GENERAL

enforcement actions by, 6.3.2

Privacy on the Go: Recommendations for the Mobile Ecosystem, 4.4.1

CALIFORNIA BUSINESS AND PROFESSIONAL CODE

§§ 17529-17529.9, anti-spam law (See ANTI-SPAM LAW (STATE))

§§ 17538.41, unsolicited text ads (See TEXT MESSAGES, UNSOLICITED (STATE))

§§ 17590-17594, do not call law (See DO NOT CALL LAW (STATE))

§§ 17940-43 (See CALIFORNIA BOT DISCLOSURE LAW), 4.9

§§ 22575 et seq. (See CALOPPA)

CALIFORNIA CIVIL CODE

§ 52.7, ID device implants, 2.6.5.2, 2.13, 2.13.3, 5.2.1

compliance, 2.13.3.2, 2.13.3.3
data protection, 2.13.3.1

sanctions and remedies, 2.13.3.4

§53.5, guest and passenger records, 2.19.6.10

§ 1708.8, paparazzi law, 2.27, 2.27.1

compliance, 2.27.1.2, 2.27.1.3
data protection, 2.27.1.1

sanctions and remedies, 2.27.1.4

§ 1725, retail transactions, 2.7.10

compliance, 2.7.10.2, 2.7.10.3
data protection, 2.7.10.1

sanctions and remedies, 2.7.10.4

§ 1747.08, excess customer information, 2.7.9.3

§ 1747.09, credit card information, 2.7.9.3

§ 1788.18, debt collectors and identity theft victims, 2.10

§ 1798.24, research use of personal data, 2.19.6.8

§ 1798.82, security breach notification law, 2.15, 2.4.1.3, 2.4.4.2,

§ 1798.85, disclosure of SSNs, 2.5.4, 6.3.2

§ 1798.90.1, swiping driver’s license information, 2.19.6.2

§ 1798.91, collection of PHI for marketing, 2.9.5.1, 5.2.1

§ 1798.93, cross-claiming by victim of identity theft, 2.10

§ 1799.3, video privacy, 2.23

§ 1936, rental car electronic surveillance, 2.13, 2.13.4

compliance, 2.13.4.2, 2.13.4.3
Index

data protection, 2.13.4.1
sanctions and remedies, 2.13.4.4
§ 1798.5(c), data security for contracts with third parties, 2.12.2
§§ 1798.90-1798.90.01, reader privacy act, 2.23

CALIFORNIA CODE OF CIVIL PROCEDURE
§ 382, class action lawsuits, 6.2.2.3
§ 1985.6, subpoenas for release of employee records, 2.6.5.6

CALIFORNIA CONSUMER PRIVACY ACT of 2018 (CCPA), 1.2.2.3, 1.5.4, 2.3, 2.4
scope, 1.2.2.3

CALIFORNIA DEPARTMENT OF MOTOR VEHICLES.
See DMV.

CALIFORNIA’S EARLY LEARNING PERSONAL INFORMATION PROTECTION ACT (“ELPIPA”), 2.5.6, 2.16

CALIFORNIA EDUCATION CODE
contracts with service providers, 2.12.2
cyberbullying, 2.16.6.4
school records privacy, 2.19.2
  compliance, 2.19.2.2, 2.19.2.3
data protection, 2.19.3.1
  sanctions and remedies, 2.19.3.4
§§ 89090-89090.5, marketing to state university alumni, 2.22.8

CALIFORNIA ELECTRONIC COMMUNICATIONS PRIVACY ACT. See CALEPCA

CALIFORNIA FAMILY CODE, 2.19.6.3

CALIFORNIA FINANCIAL INSTITUTIONS PRIVACY ACT OF 2003. See FIPA

CALIFORNIA GOVERNMENT CODE
§ 6254, victims of sex offenses, 2.19.6.6
§ 6254.21(b), removal of home address from web, 2.16.3.3
§ 12511, Attorney General authority, 6.3.2
§ 8310.3, 2.8.2

CALIFORNIA HEALTH AND SAFETY CODE, 2.9.5.3

CALIFORNIA HEALTH CARE COST AND QUALITY DATABASE (LEGISLATIVE PROPOSAL), 2.18.3

CALIFORNIA INFORMATION PRACTICES ACT OF 1977. See IPA

CALIFORNIA INSURANCE CODE, 2.9.5.6
CALIFORNIA LABOR CODE
§ 96k, anti-discrimination, 2.6.5.7
§ 226, 2.6.2
  compliance, 2.6.2.2, 2.6.2.3
  data protection, 2.5.4.2, 2.6.2.1
  sanctions and remedies, 2.6.2.4
§ 435, 2.6.3
  compliance, 2.6.3.2, 2.6.3.3
  data protection, 2.6.3.1
  sanctions and remedies, 2.6.3.4
  in the workplace, 2.6.1
§ 980, 2.6.4
  compliance, 2.6.4.2, 2.6.4.3
  data protection, 2.6.4.1
  sanctions and remedies, 2.6.4.4
§ 1026, drug/alcohol rehabilitation program, 2.6.5.1

CALIFORNIA MEDICAL INFORMATION ACT, 2.6.5.4, 2.9.2, 5.2.2

CALIFORNIA ONLINE PRIVACY PROTECTION ACT. See CALOPPA

CALIFORNIA PENAL CODE
§ 293, victims of sex offenses, 2.19.6.6
§ 483.5, deceptive ID, 2.10
§ 529.7, drivers licenses, 2.10
§ 530.5, willfully obtaining personal ID, 2.10
§§ 629.50–629.98, electronic eavesdropping, 2.24.5
§ 631, consent, 5.2.1
§§ 631–632, privacy notices for callers, 4.5
§ 637.5, satellite/cable television providers, restrictions, 2.22.3
§ 637.7, tracking devices, 2.13, 2.13.1
  compliance, 2.13.1.2, 2.13.1.3
  data protection, 2.13.1.1
  remedies and sanctions, 2.13.1.4
§ 964, government protection of personal information in court, 2.11.3
§ 1202.4(L), victim compensation, 2.10
§ 4017.1, personal information and community service work, 2.11.3
§ 11414, criminal paparazzi law, 2.27
  compliance, 2.27.2.2, 2.27.2.3
protection of celebrities’ children, 2.27.2.1
sanctions and remedies, 2.27.2.4

CALIFORNIA PRIVACY PROTECTION AGENCY (CPPA), 2.4
California Children’s Data Protection Working Group, 2.16.4
data subject rights, 2.4.3.4
data minimization, 2.4.3.9
legislative proposal, 2.18.2

CALIFORNIA PRIVACY RIGHTS ACT (CPRA), 2.18.2
CALIFORNIA PRIVATE INVESTIGATOR ACT. See PIA

CALIFORNIA PUBLIC RECORDS ACT, 2.8.2, 2.19.6.5, 2.23.4
FOIA vs., 2.8.2, 2.11.3, 2.19.6.5

CALIFORNIA PUBLIC UTILITIES CODE
§§ 2871-2876, robocalling (See ROBOCALLING LAW (STATE))
§ 2891, no access to personal information without consent, 2.8.2
§ 2891.1, telephone number access, 2.22.7.1
§ 2891(a)-(d), telecommunications customer privacy, 2.24.3

CALIFORNIA READER PRIVACY ACT, 2.23.2
compliance, 2.23.2.2, 2.23.2.3
data protection, 2.23.2.1
sanctions and remedies, 2.23.2.4

CALIFORNIA RELIGIOUS FREEDOM ACT, § 8310.3, 2.8.2

CALIFORNIA RULES OF PROFESSIONAL CONDUCT, ON PRIVATE INVESTIGATORS, 2.17.3

CALIFORNIA SUPREME COURT, “GOVERNMENTAL INTEREST” ANALYSIS BY, 1.2.2.3

CALIFORNIA UNIFORM FOREIGN-COUNTRY MONEY JUDGMENTS RECOGNITION ACT, 1.2.2.4

CALIFORNIA VEHICLE CODE, § 9951
automobile “black boxes,” 2.13, 2.13.2
compliance, 2.13.2.2, 2.13.2.3
data protection, 2.13.2.1
remedies and sanctions, 2.13.2.4

CALIFORNIA WELFARE AND INSTITUTIONS CODE, 2.9.5.5, 2.19.6.7
§ 18999.8, 2.8.2

CAN-SPAM ACT (CONTROLLING THE ASSAULT OF NON-SOLICITED PORNOGRAPHY AND MARKETING ACT) OF 2003, 2.22.1
compliance, 2.22.1.2, 2.22.1.3
email messages covered, 2.22.1.3.1
header information, 2.22.1.3.2
opt-out option, 2.22.1.3.3
sexually explicit messages, 2.22.1.3.4
data protection, 2.22.1.1
enforcement by FTC, 6.3.1
sanctions and remedies, 2.22.1.4
  by FTC, 2.22.1.4.2
  multiple emails, 2.22.1.4.2
  provider of internet access services, 2.22.1.4.4
  sexually explicit messages, 2.22.1.4.5
  by state, 2.22.1.4.3

CCCDAFA (CALIFORNIA COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT), 2.5.10
  generally, 2.510.1.1
  compliance, 2.510.1.2, 2.510.1.3
  data protection, 2.510.1
  sanctions and remedies, 2.510.1.4
  “without authorization” and “exceeds authorized access” cases, 2.510.1.3
    scraping, data harvesting, 2.510.2.3
    unauthorized computer access, 2.510.2.3
    website terms and Drew case, 2.510.2.3

CCPA (CALIFORNIA CONSUMER PRIVACY ACT), 1.2.2.3, 2.4

CCRAA (CALIFORNIA CONSUMER CREDIT REPORTING AGENCIES ACT), 2.7.4
  compliance, 2.7.4.2, 2.7.4.3
  data protection, 2.7.4.1
  sanctions and remedies, 2.7.4.4

CDA (COMMUNICATIONS DECENCY ACT) OF 1996, 6.5.1

CFAA (COMPUTER FRAUD AND ABUSE ACT), 2.5.10
  generally, 2.5.10.1
  compliance, 2.5.10.1.2, 2.5.10.1.3
  data protection, 2.5.10.1.1
  sanctions and remedies, 2.5.10.1.4

CHILDREN’S ONLINE PRIVACY PROTECTION ACT. See COPPA

CIPA (CALIFORNIA INVASION OF PRIVACY ACT), 2.24.2
  compliance, 2.24.2.2, 2.24.2.3
data protection, 2.24.2.1
sanctions and remedies, 2.24.2.4

CIVIL LITIGATION (PRIVATE), 6.2
Article III standing, 6.2.2.1
causes of action, 6.2.1
  common law, 6.2.1.1
  privacy statutes, 6.2.1.2
  unfair competition law, 6.2.1.3
class action litigation, 6.2.2
Fourth Amendment violations, Bivens action, 6.4.2.1
personal jurisdiction, 6.3
  personal jurisdiction, 6.2.3.2
  subject matter jurisdiction, 6.2.3.1

CIVIL RIGHTS ACT OF 1964, TITLE IV, 2.6.5.7
THE CLARIFYING LAWFUL OVERSEAS USE OF DATA (CLOUD) Act, 2.11.2

CLASS ACTION LITIGATION, 6.2.2.2
  under CalOPPA, 2.16.2.4
  under CCRAA, 2.7.4.4
  under CLRA, 6.2.1.3
  for contractual breach, 2.12.3
  for data security breach, 2.15.1.4
    under ECPA, 2.24.1.3
    under FCRA, 2.7.3.4
    under FDCPA, 2.7.5.4
  for improper disclosure of SSNs, 2.5.4.1
    under Rosenthal Act, 2.7.6.4
    under Shine the Light law, 2.26.4
    under Song-Beverly Credit Card Act, 2.7.9.4
    under TCPA, 2.22.3.4
    under UCL, 6.2.1.3
    under VPPA, 2.23.1.3

CLINICAL LABORATORY IMPROVEMENT AMENDMENTS OF 1988 (CLIA), 2.9.5.7

CLOUD COMPUTING SOLUTIONS. See DATA CONTROLLERS/PROCESSORS

CLRA (CONSUMER LEGAL REMEDIES ACT), 6.2.1.3
CMIA (CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT), 2.9.3
  breach of contract, 2.12.3
  compliance, 2.9.2.2, 2.9.2.3
  data protection, 2.9.2.1
  sanctions and remedies, 2.9.2.4
COMMERCIAL CLAUSE, 1.2.2.2
COMMON LAW CAUSE OF ACTION, 6.2.1.1
COMMUNICATIONS PRIVACY, 2.24
  conflict of laws, 1.2.2.3
  electronic communications privacy (federal), 2.24.1
    compliance, 2.24.1.2, 2.24.1.3
    data protection, 2.24.1.1
    sanctions and remedies, 2.24.1.4, 6.4.2.2
  electronic eavesdropping, by state law enforcement officials, 2.24.5
  government intrusion and Fourth Amendment protection, 2.11
  invasion of privacy (state), 2.24.2
    compliance, 2.24.2.2, 2.24.2.3
    data protection, 2.24.2.1
    sanctions and remedies, 2.24.2.4
  skimming RFID, 2.24.4
  telecommunications customer privacy (state), 2.24.3
    compliance, 2.24.3.2, 2.24.3.3
    data protection, 2.24.3.1
    sanctions and remedies, 2.24.3.4
COMPLIANCE CHECKLISTS, 4.2.3, 7.2.2
  data security protocols, 7.2.2.3
  draft contracts to allow compliance with requirements, 7.2.2.6
  excess data, 7.2.2.7
  in-charge employee/data security officer, 7.2.2.1
  marketing activities, 7.2.2.5
  notices and consents, 7.2.2.4
  training, 7.2.2.2
COMPLIANCE PROGRAMS, 7.2. See also COMPLIANCE CHECKLISTS
  beginning, 3.2, 4.2.3
  best approach, 3.9
  compliance binders, for documenting decisions, 5.6
compliance checklists, 4.2.3, 7.2.2
formal program, 7.2.1
inventory of data, 3.7
maintenance, 3.12, 7.2.3
mobilizing resources, to protect data, 3.4
  why?, 3.4
  why governments protect data, 3.4
objectives/priorities, define, 3.8
privacy officer, appointment of, 3.5, 4.2.3
requirements for, 3.10
taking charge, assigning personnel, 3.3
task execution, 3.11
task list, preparation of, 3.6
COMPUTER INTERFERENCE LAWS, 2.4, 4.2.3
COMPUTER SPYWARE, CONSUMER PROTECTION AGAINST, 2.16.6.2
“CONCEPTUALIZING PRIVACY” (SOLOVE), 1.3.1
CONFIDENTIALITY, OF MEDICAL INFORMATION (STATE), 2.9.2
  compliance, 2.9.2.2, 2.9.2.3
  data protection, 2.9.2.1
  sanctions and remedies, 2.9.2.4
CONFLICT OF LAW RULES, 1.2.2.3
CONNECTED TELEVISIONS
CONSENT FORMS, DRAFTING OF, 5.2. See also PRIVACY NOTICES, DRAFTING OF
  consent declarations
    consent placement, 5.2.5.3
    with focused consent, 5.2.5.2
    with notice, 5.2.5.1
  notice documentation, 4.2.3
  obtaining consent, by data controller vs. data processor, 5.2.5.4
  opt-in, above and beyond, 5.2.4
  opt-in/opt-out options, 5.2.3
    affirmative, express consent, 5.2.2, 5.2.3.5
    consent mechanisms, examples of, 5.2.3.1
    implementation options, 5.2.3.3
    minimum requirements, 5.2.3.2
silence, as consent, 5.2.3.4
valid consent, obtaining, 5.2.2
when to seek/not seek consent, 5.2.1

**CONSUMER PROTECTION. See also DEBT COLLECTION**
causes of action, 6.2.1.3
against computer spyware, 2.16.6.2

**CONSUMER PROTECTION AGAINST COMPUTER SPYWARE ACT (STATE), 2.16.6.2**

**CONSUMER REPORTING AGENCIES**
compliance under CCRAA
  - agency obligations, 2.7.4.3.1
  - furnishers of credit information, obligations of, 2.7.4.3.3
  - users of consumer credit reports, requirements on, 2.7.4.3.2
compliance under FCRA, 2.7.3.3.1
  - consumer reports, users of, 2.7.3.3.2
  - reports, furnishers of, 2.7.3.3.3

**CONSUMER REPORTS. See BACKGROUND CHECKS/CONSUMER REPORTS**

**CONTRACTS. See also AGREEMENTS**
breach of, common law cause of action, 6.2.1.1
contracting requirements, 2.12
  - in contracts, 2.12.3
  - federal law requirements, 2.12.1
  - notice documentation, 4.2.3
  - state law requirements, 2.12.2
risk mitigation and, 7.4
risks for breaching, by companies, 2.4.2.3
written consent, 5.2.2 (See also CONSENT FORMS, DRAFTING OF)

**CONTROLLING THE ASSAULT OF NON-SOLICITED PORNOGRAPHY AND MARKETING ACT OF 2003. See CAN-SPAM ACT**

**COOKIES**2.24.1.3, 4.3.2.3, 4.4.4.1

**COPPA (CHILDREN’S ONLINE PRIVACY PROTECTION ACT), 1.2.2.1, 2.16.1**
  - compliance, 2.16.1.2, 2.16.1.3
  - data protection, 2.16.1.1
  - parental consent, 5.2.1
  - sanctions and remedies, 2.16.1.4
Index

website privacy notices, 4.4.1

Coronavirus, COVID-19 pandemic, 2.6.1, 2.9.5.7

CPUC (CALIFORNIA PUBLIC UTILITIES COMMISSION), 2.22.4.4.
   See also ROBOCALLING LAW (STATE)

CRAIGSLIST, SCRAPING AND DATA HARVESTING CONTENT FROM, 2.4.2.3.3

CREDIT CARD INDUSTRY. See also BACKGROUND CHECKS/CONSUMER REPORTS
   consumer information, restrictions on (state), 2.7.9
      compliance, 2.7.9.2, 2.7.9.3
      data protection, 2.5.1.1, 2.7.9.1
      sanctions and remedies, 2.7.9.4
   credit card full disclosure (state), 2.7.11
      compliance, 2.7.11.2, 2.7.11.3
      data protection, 2.7.11.1
      sanctions and remedies, 2.7.11.4
   credit card information, restrictions on, 2.7
      data security requirements, 2.5.5
      payment card industry standards, 2.5.5, 2.7.13

CRIMINAL PAPARAZZI LAW (STATE), 2.27.2
   compliance, 2.27.2.2, 2.27.2.3
   data protection, 2.27.2.1
   sanctions and remedies, 2.27.2.4

CRIMINAL PROCEEDINGS, ENFORCEMENT OF PRIVACY LAWS, 6.4
   criminal prosecution, 6.4.1
   privacy, for criminal defendants, 6.4.2
      statutory remedy, 6.4.2.2
      suppression remedy, 6.4.2.1

CUSTOMER RECORDS, DISPOSAL OF, 2.5.2
   compliance, 2.5.2.2, 2.5.2.3
   data protection, 2.5.2.1
   sanctions and remedies, 2.5.2.4

CYBERBULLYING
   state law, 2.16.6.4
   website terms and Drew case, 2.4.2.3.1

CYBERSECURITY 2-5.8
DARK PATTERNS, 2.4.3.10, 5.2.2, 5.2.5.3

DATA BREACH, NOTIFICATION OF, 2.15. See also DATA SECURITY REQUIREMENTS

compliance, 2.15.1.2, 2.15.1.3
  account credentials compromise, 2.15.1.3.5
  breach, definition, 2.15.1.3.1
  data processors, 2.15.1.3.7
  form and content of notifications, 2.15.1.3.4
  good faith access by unauthorized employees, 2.15.1.3.2
  identity theft protection, 2.15.1.3.8
  mass breaches, 2.15.1.3.6
  risk mitigation, 2.15.1.3.10
  timing, 2.15.1.3.3
  waivers, 2.15.1.3.9

DATA CONTROLLERS/PROCESSORS

agreements between data controllers, terms for, 5.2.8
data processing service agreements, 5.3.4
terms for, 2.12, 5.3.5
data security violation, by Adobe Systems, 4.4.4.7
data subprocessing agreements, terms for, 5.3.6
definitions, 1.5.2
obtaining consent, 5.2.5.4
policy notice, 4.3.1
data categories, 4.3.2.3
data collection purposes, 4.3.2.4
data sharing, 4.3.2.5
scope, 4.3.2.2
who is issuing notice?, 4.3.2.1

DATA SECURITY AND PROTECTION

data privacy, security and, 1.3.2
definitions, 1.5.2
in Europe, 1.5.4
free speech and information and, 1.3.4
President’s Executive Order No. 13636, 2.5
privacy policy examples, 4.2.3
property rights and, 1.3.3
data security by design 2-5.9

DATA SECURITY REQUIREMENTS, 2.5. See also COMPLIANCE PROGRAMS
for contracting (federal), 2.12.1
for contracting (state), 2.12.2
for disposal of customer records, 2.5.2
    compliance, 2.5.2.2, 2.5.2.3
data protection, 2.5.2.1
    sanctions and remedies, 2.5.1.4
legislative proposals (state), 2.18.1
notice documentation, 4.2.3
for payment card industry, 2.5.5
for social security numbers, 2.5.1.1, 2.5.4
    general restrictions, 2.5.4.1
    number truncation on pay stubs, 2.5.4.2
for wireless networks, 2.5.3
    compliance, 2.5.3.2, 2.5.3.3
data protection, for unauthorized access, 2.5.3.1
    sanctions and remedies, 2.5.3.4

DATA SHARING. See THIRD PARTY DATA SHARING

DATA SUBMISSION FORMS, 4.2.3. See also PRIVACY NOTICES, DRAFTING OF; PRIVACY POLICIES, DRAFTING OF

DEBT COLLECTION
FDCPA, 2.7.5
    compliance, 2.7.5.2, 2.7.5.3
data protection, 2.7.5.1
    sanctions and remedies, 2.7.5.4
Rosenthal Act (state), 2.7.6
    compliance, 2.7.6.2, 2.7.6.3
data protection, 2.7.6.1
    sanctions and remedies, 2.7.6.4
DEEPFAKE, 2.25.1

DMV (DEPARTMENT OF MOTOR VEHICLES)
  driver’s license information confidentiality, 2.19.5
  compliance, 2.19.5.2, 2.19.5.3
  data protection, 2.19.5.1
  sanctions and remedies, 2.19.5.4
  legislative proposal, 2.18.2

DO NOT CALL LAW (FEDERAL), 2.22.3, 6.3.1
  compliance, 2.22.3.2, 2.22.3.3
  data protection, 2.22.3.1
  sanctions and remedies, 2.22.3.4

DO NOT CALL LAW (STATE), 2.22.5. See also ROBOCALLING LAW (STATE)
  compliance, 2.22.5.2, 2.22.5.3
  data protection, 2.22.5.1
  sanctions and remedies, 2.22.5.4

DO NOT CALL REGISTRY, 2.21.3.3, 2.22.5.3

DO NOT TRACK SIGNALS, WEBSITE PRIVACY NOTICES AND, 4.4.4.6

DONAHOE HIGHER EDUCATION ACT, LEGISLATIVE PROPOSAL ON, 2.18.3

DPPA (DRIVER’S PRIVACY PROTECTION ACT OF 1994), 2.8.1, 2.19.4
  compliance, 2.19.4.2, 2.19.4.3
  data protection, 2.19.4.1
  sanctions and remedies, 2.19.4.4

DRIVER’S LICENSE INFORMATION CONFIDENTIALITY (STATE), 2.19.5
  compliance, 2.19.5.2, 2.19.5.3
  data protection, 2.5.1.1, 2.19.5.1
  sanctions and remedies, 2.19.5.4

DRONES (AIRSPACE PRIVACY), 2.27

DRUG/ALCOHOL REHABILITATION PROGRAMS, EMPLOYEE PRIVACY AND, 2.6.5.1

DUE DILIGENCE AND AUDITS (PRIVACY COMPLIANCE), 7.3
  in M&A scenarios, 7.3.1
  questions to ask, 7.3.2
  service providers/vendors and, 7.3.3
Index

E

E-GOVERNMENT ACT OF 2002, 2.8.1
privacy impact assessments (“PIAs”), 2.8.1

EAVESDROPPING. See COMMUNICATIONS PRIVACY

ECPA (ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986)
causes of action, 6.2.1.2
class action lawsuits, 6.2.2.2
compliance, 2.24.1.2, 2.24.1.3
data protection, 2.24.1, 2.24.1.1
sanctions and remedies, 2.24.1.4, 6.4.2.2

EDUCATION
data security when third party contracting (state), 2.12.2
Education Sciences Reform Act Of 2002 (ESRA), 2.19.6.10
legislative proposal, 2.18.3
school records privacy, for minors (federal), 2.19.2
compliance, 2.19.2.2, 2.19.2.3
data protection, 2.19.2.1
sanctions and remedies, 2.19.2.4
school records privacy, for minors (state), 2.19.3
compliance, 2.19.3.2, 2.19.3.3
data protection, 2.19.3.1
sanctions and remedies, 2.19.3.4

EDUCATION SCIENCES REFORM ACT OF 2002 (ESRA), 2.19.6.10

EEOC (EQUAL EMPLOYMENT OPPORTUNITY COMMISSION), 2.9.1.4

ELECTRONIC COMMERCE ACT OF 1984 (STATE), 4.7

ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986.
See COMMUNICATIONS PRIVACY; ECPA

ELECTRONIC TRACKING DEVICES. See TRACKING DEVICES, LOCATION DATA FROM

EMAILS, PROTECTION FROM UNSOLICITED (FEDERAL), 2.22.1
compliance, 2.22.1.2, 2.22.1.3
e-mail messages covered, 2.22.1.3.2
header information, 2.22.1.3.2
opt-out option, 2.22.1.3.3, 4.7
sexually explicit messages, 2.22.1.3.4
data protection, 2.22.1.1
sanctions and remedies, 2.22.1.4
  by FTC, 2.22.1.4.2
  multiple emails, 2.22.1.4.1
  provider of internet access services, 2.22.1.4.4
  sexually explicit messages, 2.22.1.4.5
  by state, 2.22.1.4.3

EMAILS, PROTECTION FROM UNSOLICITED (STATE), 2.22.2
  compliance, 2.22.2.2, 2.22.2.3
  data protection, 2.22.2.1
  sanctions and remedies, 2.22.2.4

EMPLOYEE PRIVACY, 2.6
  workplace privacy, generally, 2.6.1
  California Labor Code, § 226, 2.6.2
    compliance, 2.6.2.2, 2.6.2.3
    data protection, 2.6.2.1
    sanctions and remedies, 2.6.2.4
  California Labor Code, § 435, 2.6.3
    compliance, 2.6.3.2, 2.6.3.3
    data protection, 2.6.3.1
    sanctions and remedies, 2.6.3.4
  California Labor Code, § 980, 2.6.4
    compliance, 2.6.4.2, 2.6.4.3
    data protection, 2.6.4.1
    sanctions and remedies, 2.6.4.4
  notice documentation, 4.2.3
  privacy notices, for employees, 4.6

EMPLOYEE PRIVACY, ACCOMMODATIONS BY EMPLOYERS, 2.6.5
  anti-discrimination laws, 2.6.5.7
  background checks, 2.6.5.3
  for drug/alcohol rehabilitation programs, 2.6.5.1
  health information, 2.6.5.4
  polygraphs, 2.6.5.5
  restrictions on ID device implants, 2.6.5.2
  subpoenas for release of records, 2.6.5.6
ENCRYPTION
ENFORCEMENT, OF PRIVACY LAWS
generally, 6.1
in criminal proceedings, 6.4
criminal prosecution, 6.4.1
privacy for criminal defendants, 6.4.2
by government agencies, 6.3
FTC enforcement actions, 6.3.1
state AG enforcement actions, 6.3.2
against online service providers, 6.5
contributory liability and immunities of, 6.5.1
identity information, demands for, 6.5.2
through private civil litigation, 6.2
Article III standing, 6.2.2.1
causes of action, 6.2.1
class action litigation, 6.2.2
EU-U.S. PRIVACY SHIELD, 3-12
EUROPE, DATA PROTECTION IN, 1.3.2
California laws vs., 1.5.4
“right to be forgotten,” 1.3.4
terminology, definitions, 1.5.2
EUROPEAN UNION, 1.2.2.1
“EXCLUSIONARY RULE,” SUPPRESSION REMEDY OF, 6.4.2.1
EXPLICIT CONSENT, 5.2.2. See also CONSENT FORMS, DRAFTING OF
EXPRESS CONSENT, 5.2.2, 5.2.3.5. See also CONSENT FORMS, DRAFTING OF
in questionnaires/data submission forms, 5.5

F
FACIAL RECOGNITION, 2.5.1.1, 2.11.3, 2.18.4, 6.2.2.3
FACTA (FAIR AND ACCURATE CREDIT TRANSACTIONS ACT), 4.4.1
FAIR CREDIT AND REPORTING ACT. See FCRA
FAIR DEBT COLLECTION PRACTICES ACT OF 1978. See FDCPA
FAIR EMPLOYMENT AND HOUSING ACT (STATE), 2.6.5.7
FALSE LIGHT TORT, 2.21.1.3, 6.2.1.1
FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT OF 1974. See FERPA

FCC (FEDERAL COMMUNICATIONS COMMISSION), 2.22.3, 2.22.3.4

FCRA (FAIR CREDIT REPORTING ACT) (FEDERAL), 2.7.3
  background checks, 2.6.5.3
  CCRAA vs., 2.7.4
  class action lawsuits, 6.2.2.2
  compliance, 2.7.3.2, 2.7.3.3
  consent, background checks, 5.2.1
  data protection, 2.7.3.1
  enforcement by FTC, 6.3.1
  notice documentation, 4.2.3
  sanctions and remedies, 2.7.3.4
  website privacy notices, 4.4.1

FDCPA (FAIR DEBT COLLECTION PRACTICES ACT OF 1978), 2.7.5
  compliance, 2.7.5.2, 2.7.5.3
  data protection, 2.7.5.1
  financial information, 2.7
  sanctions and remedies, 2.7.5.4

FEDERAL DATA MINING REPORTING ACT OF 2007, 2.8.1
  searches and analyses of databases, 2.8.1

FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014, 2.8.1
  information security programs, 2.8.1

FEDERAL PROSECUTORS, CRIMINAL PROSECUTION BY, 6.4.1

FEDERAL RULES OF CIVIL PROCEDURE
  Rule 23(a)-(b), class action lawsuits, 6.2.2.2
  Rule 4(k)(1)(A), jurisdiction, 6.2.3.2

FEDERAL TRADE COMMISSION ACT
  § 5, website privacy notices, 4.4.1, 6.3.1
  § 5, website privacy notices, contents, 4.4.4

FEDERAL TRADE COMMISSION (FTC)
  enforcing laws, lawsuits, 1.5.3
  compliance, with COPPA requirements, 2.16.1.3
  data privacy security violation, by Petco, Inc., 4.4.4.7
  data privacy security violation, by Wyndham Hotels, 4.4.4.7, 6.3.1
do-not-call-requirements, 2.22.3
enforcement actions, 6.3.1
enforcement actions, against revenge porn websites, 2.25.4

 Protecting Consumer Privacy in an Era of Rapid Change, 4.4.5
sanctions by, 2.5, 2.7.3.4
sanctions by, under COPPA, 2.16.1.4
sanctions by, under FDCPA, 2.7.5.4
website privacy notices
   for business-to-business sharing, 4.4.3
data categories, 4.4.4.1
data security violation, in notice placement by Sears, 4.4.6, 5.2.1
   placement, 4.4.6
website privacy notices, for business-to-business sharing, 4.4.3

FERPA (FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT OF 1974), 2.19.2
   compliance, 2.19.2.2, 2.19.2.3
data protection, 2.19.2.1
   sanctions and remedies, 2.19.2.4

FILING REQUIREMENTS, 1.5-4
   data protection registries, 1.5-4
   no filing requirements, 1.5-4

FINANCIAL INFORMATION, 2.7
   consumer information, restrictions on (state), 2.7.9
      compliance, 2.7.9.2, 2.7.9.3
data protection, 2.7.9.1
      sanctions and remedies, 2.7.9.4
customer reports and background checks (federal), 2.7.3
      compliance, 2.7.3.2, 2.7.3.3
data protection, 2.7.3.1
      sanctions and remedies, 2.7.3.4
customer reports and background checks (state), 2.7.4
      compliance, 2.7.4.2, 2.7.4.3
data protection, 2.7.4.1
      sanctions and remedies, 2.7.4.4
credit card full disclosure, 2.7.11
      compliance, 2.7.11.2, 2.7.11.3
data protection, 2.7.11.1
sanctions and remedies, 2.7.11.4
financial institutions regulation (federal), 2.7.1
financial institutions regulation (state), 2.7.2
general laws, 2.7.12
negotiable instruments, in retail transactions, 2.7.10
payment card industry standards, 2.7.13
right to financial privacy (federal), 2.7.8
right to financial privacy (state), 2.7.8

FINANCIAL INSTITUTIONS REGULATION (FEDERAL), 2.7.1
compliance, 2.7.1.2, 2.7.1.3
data protection, 2.7.1.1
sanctions and remedies, 2.7.1.4

FINANCIAL INSTITUTIONS REGULATION (STATE), 2.7.2
compliance, 2.7.2.2, 2.7.2.3
affiliates, sharing with, 2.7.2.3.2
nonaffiliated financial institutions, sharing with, 2.7.2.3.3
third parties (nonaffiliates), sharing with, 2.7.2.3.1
data protection, 2.7.2.1
sanctions and remedies, 2.7.2.4

FINANCIAL SERVICES MODERNIZATION ACT OF 1999. See GLBA

FIPA (FINANCIAL INSTITUTIONS PRIVACY ACT) (STATE), 2.7.2
compliance, 2.7.2.2, 2.7.2.3
affiliates, sharing with, 2.7.2.3.2
nonaffiliated financial institutions, sharing with, 2.7.2.3.3
third parties (nonaffiliates), sharing with, 2.7.2.3.1
data protection, 2.7.2.1
sanctions and remedies, 2.7.2.4

FISA (FOREIGN INTELLIGENCE SURVEILLANCE ACT), 6.2.2.1
minimize collection of personal data, 2.8.1
surveillance targeted at agents of foreign powers, 2.8.1

FOIA (FREEDOM OF INFORMATION ACT), 2.8.1
privacy protection, in court/government proceedings, 2.11.3
public access to government agency records, 2.19.6.5

FOURTH AMENDMENT DATA PRIVACY PROTECTION, 2.11.1,
2.13.1.3
FREE SPEECH AND INFORMATION, 1.3.4
FREIWALD, SUSAN, 1.3.1
FRIED, CHARLES, 1.3.1
FTC. See FEDERAL TRADE COMMISSION (FTC)
FULL FAITH AND CREDIT CLAUSE, 1.2.2.4

G

GAVISON, RUTH, 1.3.1
GENERAL LAWS, 2.7.12
GINA (GENETIC INFORMATION NONDISCRIMINATION ACT OF 2008), 2.9, 2.9.1
compliance, 2.9.1.2, 2.9.1.3
data protection, 2.9.1.1
sanctions and remedies, 2.9.1.4
GLASS-STEAGALL ACT, 2.7.1
GLBA (GRAMM-LEACH-BLILEY ACT) OF 1999
compliance, 2.7.1.2, 2.7.1.3
data protection, 2.7.1.1
Safeguards Rule, data security requirements, 2.5, 2.7.3
sanctions and remedies, 2.7.1.4
website privacy notices, 4.4.1
GOVERNMENT
generally, 2.8
communications privacy laws, 2.24, 4.2.3
constitutional privacy safeguards, 2.2, 2.3, 2.11
federal statutes, 2.8.1
mobilizing resources, to protect data, 3.4.2
records privacy laws, 2.19
state online privacy, 2.19.1.5
state statutes, 2.8.2
surveillance program, standing to challenge, 6.2.2.1

H

HACKING SERVICES
HARRIS, KAMALA D., 6.3.2
HEALTH/MEDICAL INFORMATION. *See* MEDICAL/HEALTH INFORMATION

HEALTH/SAFETY CODE (STATE), 2.9.5.3

HIPAA (HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996), 2.6.5.4, 2.9.2

- compliance, 2.9.2.2, 2.9.2.3
- compliance program requirement, privacy officer, 4.2.3
- consent, under privacy rule, 5.2.1
- data breach notification requirements, 2.15.2
- data protection, 2.9.2.1
- notice documentation, 4.2.3
- required standard terms, 5.2.8
- sanctions and remedies, 2.9.2.4

Security Rule, for data security requirements, 2.5

unsolicited calls from health care entities, 2.21.3.1

HITECH (HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT), 2.15.2

HOME ADDRESSES, REMOVAL FROM WEB (STATE), 2.16.3.3

HOMELAND SECURITY ACT OF 2002, 2.8.1

- mission, Chief Privacy Officer, 2.8.1

I

ID IMPLANTS, LOCATION DATA FROM, 2.13.3

- compliance, 2.13.3.2, 2.13.3.3
- data protection, 2.13.3.1
- employee privacy, accommodations by employers, 2.6.5.2
- sanctions and remedies, 2.13.3.4

IDENTITY THEFT. *See also* REVENGE PORN LAW (STATE)

consumer credit reporting agencies, compliance obligations, 2.7.4.3.1

- federal and state statutes, 2.10
  - compliance, 2.10.2, 2.10.3
  - data protection, 2.10.1
  - sanctions and remedies, 2.10.4

injury-in-fact, Article III standing causes of action, 6.2.2.1

international data security laws and, 1.3.2

legislative proposals (state), 2.18.1
users of consumer credit reports, requirements on, 2.7.4.3.2
using social security numbers, 2.5.4.1
INDIVIDUALS WITH DISABILITIES ACT, 2.19.6.10
INFORMED CONSENT, 5.2.2. See also CONSENT FORMS, DRAFTING OF
INJURY-IN-FACT, ARTICLE III STANDING CAUSES OF ACTION, 6.2.2.1
INNESS, JULIE, 1.3.1
INSURANCE, RISK MITIGATION AND, 7.5
INSURANCE CODE (STATE), 2.9.5.6
INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS TORT, 6.2.1.1
INTERNATIONAL LAW, PRIVACY AND, 1.2.2.1
data security laws, 1.3.2
enforceability of state laws outside state, 1.2.2.4
INTERNET, STATE REGULATION OF, 1.2.2.2
INTERNET ACCESS SERVICE PROVIDERS. See also ECPA
obtaining consent, by data controllers vs. data processors, 5.2.5.4
policy notices, 4.3.1
remedies for, under CAN-SPAM Act, 2.22.1.4.4
INTRUSION UPON SECLUSION TORT, 2.21.1.1, 6.2.1.1
INVASION OF PRIVACY (STATE), 2.24.2
causes of action, 2.2.3, 2.3.3
compliance, 2.24.2.2, 2.24.2.3
data protection, 2.24.2.1
sanctions and remedies, 2.24.2.4
INVASIONS INTO PRIVACY (STALKING), 2.21.1.5
IPA (INFORMATION PRACTICES ACT OF 1977), 2.8.2, 2.9.5.4, 2.19.6.1
IPPA (INSURANCE INFORMATION AND PRIVACY PROTECTION ACT), 2.9.5.6

J
JUDICIAL PROCEEDINGS AND LAW ENFORCEMENT, 2.11, 6.4
Fourth Amendment, 2.11.1, 6.4.2.1
privacy in court and proceedings, 2.11.3, 6.4.2
subpoenas, companies challenges to, 2.11.2
“JUST IN TIME” FOLLOW-UP NOTICES, 5.2.4
JUSTICE SYSTEM IMPROVEMENT ACT OF 1979, 2.8-
protect and limit disclosure of information, 2.8.1
Census Bureau, disclose personal data, 2.8.1

L

LAW ENFORCEMENT

electronic eavesdropping by, 2.24.5
judicial proceedings and, 2.11
   Fourth Amendment, 2.11.1
   privacy in court and proceedings, 2.11.3
   subpoenas, companies challenges to, 2.11.2
legislative proposals, body cameras and privacy, 2.18.2
tracking devices, lawful use by, 2.13.1
   compliance, 2.13.1.2, 2.13.1.3
   data protection, 2.13.1.1
   sanctions and remedies, 2.13.1.4
video taping by, 2.27.1.1

LEGISLATIVE PROPOSALS (STATE), 2.18
   on data security, 2.18.1
   on data sharing, collection and coordination, 2.18.3
   on information and general privacy, 2.18.2

LGBT (LESBIAN, GAY, BISEXUAL, TRANSGENDER) DATA COLLECTION, LEGISLATIVE PROPOSAL FOR, 2.18.3

LICENSE PLATE DATA

LIMITATIONS
   California jurisdiction, 1.2.2.2
   under federal law, 1.2.2.2

LOCATION DATA, 2.13
   automobile black boxes, 2.13.2
      compliance, 2.13.2.2, 2.13.2.3
      data protection, 2.13.2.1
      sanctions and remedies, 2.13.2.4
   ID implants, 2.13.3
      compliance, 2.13.3.2, 2.13.3.3
      data protection, 2.13.3.1
      sanctions and remedies, 2.13.3.4
rental car surveillance, 2.13.4
  compliance, 2.13.4.2, 2.13.4.3
  data protection, 2.13.4.1
  sanctions and remedies, 2.13.4.4
tracking devices, 2.13.1
  compliance, 2.13.1.2, 2.13.1.3
  data protection, 2.13.1.1
  sanctions and remedies, 2.13.1.4

M
M&A (MERGERS AND ACQUISITIONS), DUE DILIGENCE IN, 7.3.1
MAIL (POSTAL), DATA SECURITY OF, 2.14
MAKING YOUR PRIVACY PRACTICES PUBLIC (STATE DOJ), 4.4.1, 4.4.5
MARRIAGE LICENSES/FAMILY RECORDS PROTECTION (STATE), 2.19.6.3
MASS BREACHES, NOTIFICATION OF, 2.15.1.3.6, 2.15.2
MEDICAL/HEALTH INFORMATION, 2.9
  agency records (state), 2.9.5.4
  Americans with Disabilities Act of 1990, 2.9.5.7
  CLIA (laboratory test results), 2.9.5.7
  CMIA (confidentiality), 2.9.2
    compliance, 2.9.2.2, 2.9.2.3
    data protection, 2.9.2.1
    sanctions and remedies, 2.9.2.4
  collection, for direct marketing purposes, 2.9.5.1
  data security breach notification, 2.9.6
  Drug Abuse Office and Treatment Act, 2.9.5.7
    substance use disorder information, 2.9.5.7
  employee privacy, accommodations by employers, 2.6.5.1
  GINA (genetic information), 2.9.3
    compliance, 2.9.3.2, 2.9.3.3
    data protection, 2.9.3.1
    notice documentation, 4.2.3
    sanctions and remedies, 2.9.4.4
  health/safety code (state), 2.9.5.3
  HIPAA, 2.9.1
compliance, 2.9.1.2, 2.9.1.3
data protection, 2.9.1.1
sanctions and remedies, 2.9.1.4
insurance code (state), 2.9.5.6
notice documentation, 4.2.3
Patient Safety & Quality Improvement Act of 2005 (PSQIA), 2.9.4.72.9.5.7
“Shine the Light” law, 2.9.5.2, 2.26
welfare/institutions code (state), 2.9.5.5

MINORS
access to personal information by, 2.11.3
cyberbullying, 2.16.6.4
education records privacy (federal), 2.19.2
  compliance, 2.19.2.2, 2.19.2.3
data protection, 2.19.2.1
  sanctions and remedies, 2.19.2.4
education records privacy (state), 2.19.3
  compliance, 2.19.3.2, 2.19.3.3
data protection, 2.19.3.1
  sanctions and remedies, 2.19.3.4
online privacy law (federal), 2.16.1
  compliance, 2.16.1.2, 2.16.1.3
data protection, 2.16.1.1
  sanctions and remedies, 2.16.1.4
online privacy law (state), 2.16.2
  compliance, 2.16.2.2, 2.16.2.3
data protection, 2.16.2.1
  sanctions and remedies, 2.16.2.4
paparazzi law, 2.27.2
  compliance, 2.27.2.2, 2.27.2.3
data protection, 2.27.2.1
  sanctions and remedies, 2.27.2.4
parental consent, as invasion of privacy rights of, 2.2.3
parental consent, when to seek, 5.2.1
website privacy notices, 4.4.1
websites catering to K-12 schools, see SOPIPA, 2.5.6

MISAPPROPRIATION OF NAME/LIKENESS TORT, 2.21.1.4, 6.2.1.1
MOBILE APPLICATIONS
AG enforcement actions under CalOPPA, 6.3.2
legislative proposals, consumer notice, 2.18.2
standardized permission categories, 5.2.4
as tracking devices, 2.13.1.3, 5.2.4

MOBILE APPLICATIONS, PRIVACY NOTICES FOR, 4.4
applicable laws, 4.4.1
business-to-business transfer of personal data, 4.4.3
combined/multiple notices, 4.4.2
notice contents, 4.4.4
  changes, 4.4.4.4
data access, update process, 4.4.4.3
data categories, 4.4.4.1
data security, 4.4.4.7
do not track signals, 4.4.4.6
effective date, 4.4.4.5
third party data sharing, 4.4.4.2
notice placement, 4.4.6
style and organization, 4.4.5

MOBILE PHONE SERVICE PROVIDERS, 2.22.8.3.2. See also TRACKING DEVICES, LOCATION DATA FROM

MOTOR VEHICLE RECORDS PROTECTION (STATE), 2.19.5
compliance, 2.19.5.2, 2.19.5.3
data protection, 2.5.1.1, 2.19.5.1
sanctions and remedies, 2.19.5.4

N
NATIONAL SECURITY ACT, 2.8-1
  protection of classified information, 2.8.1
NEGligence, COMMON LAW CAUSES OF ACTION, 6.2.1.1
NEGOTIABLE INSTRUMENTS, IN RETAIL TRANSACTIONS, 2.7, 2.7.10
  compliance, 2.7.10.2, 2.7.10.3
data protection, 2.7.10.1
sanctions and remedies, 2.7.10.4
NISSENBAUM, HELEN, 1.3.1
NLRB (NATIONAL LABOR RELATIONS BOARD), § 7, 4.6
NOTICES, 4.2.3. See also PRIVACY NOTICES, DRAFTING OF; PRIVACY POLICIES, DRAFTING OF

O

ONLINE PRIVACY, 2.16. See also CIPA; ECPA
anti-phishing law, 2.16.6.1
CalOPPA, 2.16.2
 compliance, 2.16.2.2, 2.16.2.3
data protection, 2.16.2.1
sanctions and remedies, 2.16.2.4
COPPA, 2.16.2
 compliance, 2.16.2.2, 2.16.2.3
data protection, 2.16.2.1
sanctions and remedies, 2.16.2.4
cyberbullying (state), 2.16.6.4
government privacy policies (state), 2.16.6.5
home addresses, removal from web (state), 2.16.6.3
policy documentation examples, 4.2.3
removal of home address from web, 2.16.6.3
spyware law (state), 2.16.3.2

ONLINE SERVICE PROVIDERS
due diligence and audits (privacy compliance), 7.3.3
enforcement against, 6.5
 contributory liability and immunities, 6.5.1
identity information, demands for, 6.5.2

ONLINE SERVICES, PRIVACY NOTICES FOR, 4.4
applicable laws, 4.4.1
business-to-business transfer of personal data, 4.4.3
combined/multiple notices, 4.4.2
notice contents, 4.4.4
 changes, 4.4.4.4
data access, update process, 4.4.4.3
data categories, 4.4.4.1
data security, 4.4.4.7
do not track signals, 4.4.4.6
effective date, 4.4.4.5
third party data sharing, 4.4.4.2
notice placement, 4.4.6
style and organization, 4.4.5
OPT-IN/OPT-OUT NOTICES
anti-spam act (federal), 2.22.1.3.3
in consent forms, 5.2.3
  affirmative, express consent, 5.2.2, 5.2.3.5
  consent mechanisms, examples of, 5.2.3.1
  implementation options, 5.2.3.3
  minimum requirements, 5.2.3.2
  silence, as consent, 5.2.3.4
for direct marketing communications, 4.7
ORWELL, GEORGE, 1.3.4

P
pandemic, 2.6.1
PAPARAZZI LAWS, 2.27
  intrusion into seclusion (state), 2.27.1
  compliance, 2.27.1.2, 2.27.1.3
  data protection, 2.27.1.1
  sanctions and remedies, 2.27.1.4
  protecting children (state), 2.27.2
  compliance, 2.27.2.2, 2.27.2.3
  data protection, 2.27.2.1
  sanctions and remedies, 2.27.2.4
PAPERWORK REDUCTION ACT OF 1995, 2.8.1
  collecting information from individuals, 2.8.1
PARETO PRINCIPLE, 3.9
PATIENT SAFETY & QUALITY IMPROVEMENT ACT OF 2005 (PSQIA), 2.9.5.7
PAYMENT CARD INDUSTRY (PCI) STANDARDS, 2.5.5, 2.7.13. See also CREDIT CARD INDUSTRY
PEN REGISTER ACT, 6.4.2.2. See also ECPA
PERSONAL HEALTH INFORMATION (PHI). See DATA SECURITY BREACH, NOTIFICATION OF
PERSONAL INFORMATION
banks/financial institutions (federal), regulation of
   compliance, 2.7.1.2, 2.7.1.3
   data protection, 2.5, 2.7.1.1, 2.7.3
   sanctions and remedies, 2.7.1.4
banks/financial institutions (state), regulation of, 2.7.2
   compliance, 2.7.2.2, 2.7.2.3
   data protection, 2.7.2.1
   sanctions and remedies, 2.7.2.4
data security requirements (state), 2.5.1
   compliance, 2.5.2, 2.5.3
   data protection, scope of, 2.5.1
   sanctions and remedies, 2.5.1.4
personal data, definition, 1.5.2
research use of (state), 2.19.6.8

PERSONAL JURISDICTION, IN CIVIL LITIGATION (PRIVATE), 6.2.3
   personal jurisdiction, in state, 6.2.3.2
   subject matter jurisdiction, 6.2.3.1

PIA (CALIFORNIA PRIVATE INVESTIGATOR ACT), 2.17
   compliance, 2.17.2, 2.17.3
   data protection, 2.17.1
   sanctions and remedies, 2.17.4

POLYGRAPHS, EMPLOYEE PRIVACY AND, 2.6.5.5

PRIOR CONSENT, 5.2.1. See also CONSENT FORMS, DRAFTING OF
PRIVACY, 1.3
   concept definitions, 1.3.1
   data protection, security and, 1.3.2
   free speech, information, 1.3.4
   property, 1.3.3

PRIVACY ACT OF 1974, 2.8.1, 2.19.1

PRIVACY AND FREEDOM (WESTIN), 1.3.1

PRIVACY LAW (STATE). See also CALIFORNIA
   generally, 1.5
   key features, 1.5.3
   scope, 1.5.1
   terminology, 1.5.2
definitions, 1.2
law vs. best practices, 1.4
omnibus data protection and, 1.5.4
privacy, 1.3
  data protection, security and, 1.3.2
  free speech, information, 1.3.4
  property, 1.3.3
  rights to privacy and data privacy, 1.3.1

PRIVACY LITIGATION, 6.2. See also CLASS ACTION LITIGATION
  Article III standing, 6.2.2.1
  causes of action, 6.2.1
    common law, 6.2.1.1
    privacy statutes, 6.2.1.2
    unfair competition law, 6.2.1.3
  class action litigation, 6.2.2
  personal jurisdiction, 6.3
    personal jurisdiction, 6.2.3.2
    subject matter jurisdiction, 6.2.3.1

PRIVACY NOTICES, DRAFTING OF
  generally, 4.3
    issuing, service provider vs. customer, 4.3.1
    requirements, for form and delivery, 4.3.4
    topics, notices to data subjects, 4.3.2
    topics to avoid, 4.3.3
  for callers, 4.5
  for employees, 4.6
  opt-out notices
    anti-spam act (federal), 2.22.1.3.3
    for direct marketing communications, 4.7
  for websites/apps/online services, 4.4
    applicable laws, 4.4.1
    business-to-business transfer of personal data, 4.4.3
    combined/multiple notices, 4.4.2
    notice contents, 4.4.4
    notice placement, 4.4.6
    style and organization, 4.4.5
PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM (STATE AGO), 4.4.1

PRIVACY POLICIES, DRAFTING OF. See also PRIVACY NOTICES, DRAFTING OF
  generally, 4.1
  considerations, 4.2
    audience identification, 4.2.2
    rationale for drafting, 4.2.1
    term use, “policy” vs. “notice,” 4.2.3

PRIVACY (PROSSER), 2.21, 6.2.1.1

PRIVACY PROTECTION ACT, 2.8.1

PRIVATE INVESTIGATORS, 2.17
  compliance, 2.17.2, 2.17.3
  data protection, 2.17.1
  sanctions and remedies, 2.17.4

PROCESSING
  definition, 1.5.2
  prohibition of data processing, California vs. Europe, 1.5.4

PROPERTY RIGHTS, DATA PRIVACY LAWS AND, 1.3.3

PROSSER, WILLIAM, 2.21, 6.2.1.1

PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (FTC), 4.4.5

PROTECTION OF PUPIL RIGHTS, 2.19.2

PROTOCOLS, FOR PROCESSING/PROTECTING DATA, 4.2.3, 5.4.
  See also PRIVACY NOTICES, DRAFTING OF; PRIVACY POLICIES, DRAFTING OF
  sample, direct communications protocol, 5.4.1

PUBLIC DISCLOSURE OF PRIVATE FACTS TORT, 2.21.1.2, 6.2.1.1

PUBLIC HEALTH SERVICE ACT, 2.8.1
  Secretary of Health and Human Services, 2.8.1
  mental health, 2.8.1
  Centers for Disease Control and Prevention (CDC), 2.8.1
  Department of Veterans, 2.8.1

PUBLIC INTERNATIONAL LAW, PRIVACY AND, 1.2.2.1

PUBLIC RECORDS LAWS (FEDERAL AND STATE), 2.19.6.5
Index

Q

QUESTIONNAIRES/DATA SUBMISSION FORMS, 4.2.3, 5.5

R

RADIO-FREQUENCY IDENTIFICATION (RFID), 2.13.3.3. See also ID IMPLANTS, LOCATION DATA FROM

READER PRIVACY (STATE), 2.23.2
  compliance, 2.23.2.2, 2.23.2.3
  data protection, 2.23.2.1
  sanctions and remedies, 2.23.2.4

REAL ID ACT, 2.8.1
  driver's licenses, 2.8.1
  identification cards, 2.8.1

RECORDS, 2.19
  agency access (state), 2.19.6.1
  customer records, disposal of, 2.5.2
    compliance, 2.5.2.2, 2.5.2.3
    data protection, 2.5.2.1
    sanctions and remedies, 2.5.2.4
  driver's privacy protection (federal), 2.19.4
    compliance, 2.19.4.2, 2.19.4.3
    data protection, 2.19.4.1
    sanctions and remedies, 2.19.4.4
  driver's privacy protection (state), 2.19.5
    compliance, 2.19.5.2, 2.19.5.3
    data protection, 2.19.5.1
    sanctions and remedies, 2.19.5.4
  educational records, of minors (federal), 2.19.2
    compliance, 2.19.2.2, 2.19.2.3
    data protection, 2.19.2.1
    sanctions and remedies, 2.19.2.4
  educational records, of minors (state), 2.19.3
    compliance, 2.19.3.2, 2.19.3.3
    data protection, 2.19.3.1
  marriage licenses/family records (state), 2.19.6.3
  Privacy Act (federal), 2.19.1

Privacy Act (federal), 2.19.1
public records laws (federal and state), 2.19.6.5
research use of personal data (state), 2.19.6.8
sex offense victim protection (state), 2.19.6.6
vehicle dealer records protection (state)
  legislative proposal, 2.18.2
vehicle dealer records (state), 2.19.6.4
welfare records (state), 2.19.6.7

RENTAL CAR SURVEILLANCE, LOCATION DATA FROM, 2.13.4
  compliance, 2.13.4.2, 2.13.4.3
  data protection, 2.13.4.1
  sanctions and remedies, 2.13.4.4

RESEARCH USE OF PERSONAL RECORDS DATA (STATE), 2.19.6.8

RETAIL TRANSACTIONS, COLLECTION OF PERSONAL/CREDIT CARD INFORMATION IN, 2.7.10
  compliance, 2.7.10.2, 2.7.10.3
  data protection, 2.7.10.1
  sanctions and remedies, 2.7.10.4

REVENGE PORN LAW (STATE), 2.25
  compliance, 2.25.2, 2.25.3
  data protection, 2.25.1
  legislative proposals, 2.18.2
  sanctions and remedies, 2.25.4

RFID (RADIO-FREQUENCY IDENTIFICATION), 2.13.3.3. See also ID IMPLANTS, LOCATION DATA FROM

RIGHT OF PUBLICITY TORT, 2.21.1.4, 6.2.1.1
“RIGHT TO BE FORGOTTEN,” 1.3.4

RIGHT TO FINANCIAL PRIVACY ACT OF 1978 (FEDERAL), 2.7.8
RIGHT TO FINANCIAL PRIVACY ACT OF 1976 (STATE), 2.7.8

THE RIGHT TO PRIVACY (WARREN AND BRANDEIS), 1.3.1, 2.21, 6.2.1.1

RISK MITIGATION
  breaches notification, 2.15.1.3.10
  compliance program, 7.2
    compliance checklist, 7.2.2.8
    formal program, 7.2.1
    maintenance, 7.2.3
  contracts, 7.4
due diligence and audits, 7.3
in M&A scenarios, 7.3.1
questions to ask, 7.3.2
service providers/vendors and, 7.3.3
insurance, 7.5
ROBOCALLING LAW (FEDERAL), 2.22.3
compliance, 2.22.3.2, 2.22.3.3
data protection, 2.22.3.1
sanctions and remedies, 2.22.3.4
ROBOCALLING LAW (STATE), 2.22.4
compliance, 2.22.4.2, 2.22.4.3
data protection, 2.22.4.1
“no robot” scripts, 2.4.2.3
sanctions and remedies, 2.22.4.4
ROSENTHAL FAIR DEBT COLLECTION PRACTICES ACT, 2.7.6
compliance, 2.7.6.2, 2.7.6.3
data protection, 2.7.6.1
sanctions and remedies, 2.7.6.4
SAFE AT HOME PROGRAM, 2.16.4.3
victims of sexual or domestic violence, 2.16.6.3
SAN FRANCISCO STOP SECRET SURVEILLANCE ORDINANCE, 2.11.3
SCA (STORED COMMUNICATIONS ACT). See ECPA
SCHMIDT, ERIC, 1.3.4
SCHOOLS, 2.19.2, 2.19.3
SCHWARTZ, PAUL, 1.3.1
“SELFIES.” See REVENGE PORN LAW (STATE)
SENATE BILLS, PROPOSED (STATE)
AB 859, public agency demand anonymized trip data, 2.18.2
AB 1490, CPPA members, Californian with expertise in privacy, technology, consumer rights, 2.18.2
AB 2486, create Office for the Protection of Children Online in the CCPA, 2.18.2
AB 2871, permanently extend exemption relating to employee’s personal information, 2.18.2
SB 1059, definition of data broker and transfer authority, responsibilities, 2.18.2

SEX OFFENSE VICTIM RECORDS PROTECTION (STATE), 2.19.6.6
SEXUALLY EXPLICIT EMAIL MESSAGES (SEXTING), 2.22.1.3.4, 2.22.1.4.5

SHINE THE LIGHT LAW, 2.9.5.2, 2.26
  compliance, 2.26.2, 2.26.3
  consent, 5.2.1
  data protection, 2.26.1
  data sharing under, for direct marketing purposes, 4.4.4.2.3
  sanctions and remedies, 2.26.4
  website privacy notices, 4.4.1, 4.4.6

SILENCE AS CONSENT, IN OPT-IN/OPT-OUT NOTICES, 5.2.3.4

SKIMMING RFID, 2.24.4

SOCIAL MEDIA
  access by employers to employee accounts, 2.6.4.1
  data security violation, by LinkedIn Corporation, 4.4.4.7
  data security violation, by Snapchat, 4.4.4.7
  data sharing violation, by Facebook, 4.4.4.4
  data sharing violation, by Google, 4.4.4.4, 6.3.1
  data sharing violation, by MySpace, 4.4.4.2.1, 6.3.1
  deceptive trade practices, by Twitter, 6.3.1
  “right to be forgotten” and, 1.3.4
  website service providers, enforcement against, 6.5
    contributory liability and immunities, 6.5.1
    identity information, demands for, 6.5.2
  website terms and *Drew* case, 2.4.2.3.1

SOCIAL SECURITY NUMBERS
  data security breach, causes of action, 6.2.2.1
  data security requirements, 2.5.1.1, 2.5.4
    general restrictions, 2.5.4.1
      number truncation on pay stubs, 2.5.4.2
    protected data under CMIA, 2.9.3.1

SOLOVE, DANIEL, 1.3.1

SONG-BEVERLY CREDIT CARD ACT OF 1971, 2.7, 2.7.9
  causes of action, 6.2.1.2
  class action lawsuits, 6.2.2.2
compliance, 2.7.9.2, 2.7.9.3
  consumer consent, 2.7.9.3.1
  data collection vs. credit card processing, 2.7.9.3.2
  express statutory exceptions, 2.7.9.3.3
  returns and refunds, 2.7.9.3.4

consent, 5.2.1

  data protection, 2.7.9.1

  sanctions and remedies, 2.7.9.4

SOPIPA (STUDENT ONLINE PERSONAL INFORMATION PROTECTION ACT), 2.16.3, 6.2.1.3

SPECIFIC CONSENT, 5.2.2. See also CONSENT FORMS, DRAFTING OF

SPYWARE, CONSUMER PROTECTION AGAINST, 2.16.6.2

STALKING (ONLINE AND OFFLINE), 2.21.1.5. See also PAPARAZZI LAWS

STORED COMMUNICATIONS ACT, 6.4.2.2, 6.5.2

STUDENTS

  SUBPOENAS FOR RELEASE OF RECORDS, EMPLOYEE PRIVACY AND, 2.6.5.6, 6.5.2

SUPERMARKET CLUB CARD DISCLOSURE ACT OF 1999, 2.20

  compliance, 2.20.2, 2.20.3

  data protection, 2.20.1

  sanctions and remedies, 2.20.4

SUPREMACY CLAUSE, 1.2.2.2

T

TAX BOARD/ASSESSORS, LEGISLATIVE PROPOSAL FOR DATA SHARING, 2.18.2

TCPA (TELEPHONE CONSUMER PROTECTION ACT OF 1991) (FEDERAL), 2.22.3, 6.2.1.2, 6.2.2.2

TELECOMMUNICATIONS CUSTOMER PRIVACY (STATE), 2.24.3

  compliance, 2.24.3.2, 2.24.3.3

  data protection, 2.24.3.1

  sanctions and remedies, 2.24.3.4

TELEPHONE NUMBER DIRECTORIES, 2.22.8

TELEVISION

  TENANTS, INVASION OF PRIVACY RIGHTS OF, 2.2.3

TERMS OF USE (TOU) VIOLATIONS, 2.5.10.2.3
TEXT MESSAGES, UNSOLICITED (STATE), 2.22.6
  compliance, 2.22.6.2, 2.22.6.3
  data protection, 2.22.6.1
  sample, direct communications protocol, 5.4.1
  sanctions and remedies, 2.22.6.4

THIRD PARTY DATA SHARING, 4.4.4.2. See also PRIVACY NOTICES, DRAFTING OF
  generally, 4.4.4.2.1
  business-to-business, website privacy notices, 4.4.3
  under CalOPPA, 4.4.4.2.2
  for contracts, 2.12.2
  for direct marketing purposes, 4.2.3, 4.4.4.2.3
  under FIPA, 2.7.2.3.2
  of personal information
    by banks/financial institutions (federal), 2.7.1.3
  privacy notices, identifying parties, 4.3.2.5
  risk mitigation via contracts, 7.4

TICKET HOLDERS, INVASION OF PRIVACY RIGHTS OF, 2.2.3

TORTS, 2.21
  common law cause of action, 6.2.1.1
  compliance, 2.21.2, 2.21.3
  data protection
    false light, 2.21.1.3
    intrusion upon seclusion, 2.21.1.1
    public disclosure of private facts, 2.21.1.2
    right to publicity, 2.21.1.4
    stalking/invasions into privacy, 2.21.1.5
  sanctions and remedies, 2.21.4

TRACKING DEVICES, LOCATION DATA FROM, 2.13.1
  compliance, 2.13.1.2, 2.13.1.3
  data protection, 2.13.1.1
  sanctions and remedies, 2.13.1.4

TRACKING PIXELS, 4.4.4.2.2, 4.4.4.7
INDEX

U

UCL (CALIFORNIA UNFAIR COMPETITION LAW), 2.20.4, 6.2.1.3
UNAMBIGUOUS CONSENT, 5.2.2. See also CONSENT FORMS, DRAFTING OF
UNFAIR COMPETITION
AG enforcement actions, 6.3.2
causes of action, 6.2.1.3
enforcement by FTC, 6.3.1
misleading consent language, 5.1.5.2
UNITED KINGDOM, PRIVACY LAW IN, 1.2.2.1
UNITED STATES ATTORNEYS, CRIMINAL PROSECUTION BY, 6.4.1
UNITING AND STRENGTHENING AMERICA BY FULFILLING RIGHTS AND ENSURING EFFECTIVE DISCIPLINE OVER MONITORING ACT OF 2015 (USA FREEDOM ACT), 2.8.1
collecting physical and electronic information about individuals, 2.8.1
UNSOLICITED MARKETING COMMUNICATIONS, 2.22
anti-spam act (federal), 2.22, 2.22.1
compliance, 2.22.1.2, 2.22.1.3
data protection, 2.22.1.1
sanctions and remedies, 2.22.1.4
anti-spam act (state), 2.22.2
compliance, 2.22.2.2, 2.22.2.3
data protection, 2.22.2.1
sanctions and remedies, 2.22.2.4
do not call law (state), 2.22.5
compliance, 2.22.5.2, 2.22.5.3
data protection, 2.22.5.1
sanctions and remedies, 2.22.5.4
robocalling law (state), 2.22.4
compliance, 2.22.4.2, 2.22.4.3
data protection, 2.22.4.1
sanctions and remedies, 2.22.4.4
to state university alumni, 2.22.8
sanctions and remedies, 2.22.8.4
telephone consumer protection (federal), 2.22, 2.22.3
compliance, 2.22.3.2, 2.22.3.3
data protection, 2.22.3.1
sanctions and remedies, 2.22.3.4
telephone number directories, 2.22.8
unsolicited text ads, 2.22.6
compliance, 2.22.6.2, 2.22.6.3
data protection, 2.22.6.1
sanctions and remedies, 2.22.6.4
USA FREEDOM ACT (UNITING AND STRENGTHENING AMERICA BY FULFILLING RIGHTS AND ENSURING EFFECTIVE DISCIPLINE OVER MONITORING ACT OF 2015), 2.8.1
U.S. CONSTITUTION
Article III standing doctrine, 6.2.2.1
California Constitution vs., 2.2
Fourteenth Amendment, 6.2.3.2
Fourth Amendment data privacy protection, 2.11.1, 6.4
suppression remedy, 6.4.2.1
U.S. POSTAL SERVICE, MAIL DATA PROTECTION BY, 2.14
U.S. SUPREME COURT, 1.3.1
U.S.C.
§ 1028, identity theft, 2.10
§§ 1703 and 1708, postal mail data protection, 2.14

V

VEHICLE DEALER RECORDS PROTECTION (STATE), 2.19.6.4
VIDEOS AND BOOKS, 2.23
reader privacy (state), 2.23.2
compliance, 2.23.2.2, 2.23.2.3
data protection, 2.23.2.1
sanctions and remedies, 2.23.2.4
video privacy, website privacy notice violation by TRENDnet, 4.4.4.7
video privacy (federal and state) (See also PAPARAZZI LAWS)
compliance, 2.23.1.2, 2.23.1.3
data protection, 2.23.1.1
sanctions and remedies, 2.23.1.4
in the workplace, 2.6.1
VOLUNTARY CONSENT, 5.2.2. See also CONSENT FORMS, DRAFTING OF
VPPA (VIDEO PRIVACY PROTECTION ACT) (FEDERAL), 2.23.1
causes of action, 6.2.1.2
class action lawsuits, 6.2.2.2
compliance, 2.23.1.2, 2.23.1.3
data protection, 2.23.1.1
sanctions and remedies, 2.23.1.4
website privacy notices, 4.4.1

W
WARREN, SAMUEL, 1.3.1, 2.21, 6.2.1.1
WEBSITE SERVICE PROVIDERS, ENFORCEMENT AGAINST, 6.5
contributory liability and immunities, 6.5.1
identity information, demands for, 6.5.2
WEBSITES, PRIVACY NOTICES FOR, 4.4
applicable laws, 4.4.1
business-to-business transfer of personal data, 4.4.3
combined/multiple notices, 4.4.2
document, 4.2.3
jurisdiction, “general” vs. “specific,” 6.2.3.2
notice contents, 4.4.4
changes, 4.4.4.4
data access, update process, 4.4.4.3
data categories, 4.4.4.1
data security, 4.4.4.7
do not track signals, 4.4.4.6
effective date, 4.4.4.5
third party data sharing, 4.4.4.2
notice placement, 4.4.6
style and organization, 4.4.5
unfair competition, privacy violation for, 6.2.1.3
using cookies, do not track signals and, 4.4.4.6
using cookies, tracking without consent, 6.2.2.1
WELFARE/INSTITUTIONS CODE (STATE), 2.9.5.5
WELFARE RECORDS PROTECTION (STATE), 2.19.6.7
WERRO, FRANZ, 1.3.4
WESTIN, ALAN, 1.3.1

WIRELESS NETWORK PROVIDERS
  data security requirements, 2.5.3
  compliance, 2.5.3.2, 2.5.3.3
  data protection, for unauthorized access, 2.5.3.1
  sanctions and remedies, 2.5.3.4
  providing personal data, to government, 2.11.2

WIRETAP ACT. See ECPA

WIRETAPPING. See COMMUNICATIONS PRIVACY

WORKPLACE PRIVACY OF EMPLOYEES, 4.6. See also EMPLOYEE PRIVACY
generally, 2.6.1

Y

“YOUR PRIVACY RIGHTS” LANGUAGE (STATE), 2.26
  compliance, 2.26.2, 2.26.3
  data protection, 2.26.1
  sanctions and remedies, 2.26.4

Z

ZIP CODES, COLLECTION OF, 2.7.9.3, 2.7.9.3.3