Olshan Frome Wolosky

From the SelectedWorks of Jonathan I. Ezor

Fall 2012

Privacy and Data Protection in Business: Laws and Practices (Sample Chapters)

Jonathan I Ezor

Available at: https://works.bepress.com/jonathan_ezor/9/
Privacy and Data Protection in Business: Laws and Practices
LexisNexis Law School Publishing
Advisory Board

William Araiza  
Professor of Law  
Brooklyn Law School

Ruth Colker  
Distinguished University Professor & Heck-Faust Memorial Chair in Constitutional Law  
Ohio State University, Moritz College of Law

Olympia Duhart  
Associate Professor of Law  
Nova Southeastern University Shepard Broad Law School

Samuel Estreicher  
Dwight D. Opperman Professor of Law  
Director, Center for Labor and Employment Law  
NYU School of Law

David Gamage  
Assistant Professor of Law  
UC Berkeley School of Law

Joan Heminway  
College of Law Distinguished Professor of Law  
University of Tennessee College of Law

Edward Imwinkelried  
Edward L. Barrett, Jr. Professor of Law  
UC Davis School of Law

Paul Marcus  
Haynes Professor of Law  
William and Mary Law School

Melissa Weresh  
Director of Legal Writing and Professor of Law  
Drake University Law School
Privacy and Data Protection in Business: Laws and Practices

Jonathan I. Ezor
ISBN: 9781422490969

Ezor, Jonathan
p. cm.
Includes index.
KF1357.5.E96 2012
346.73'065--dc23
2012028733

This publication is designed to provide authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. Matthew Bender and the Matthew Bender Flame Design are registered trademarks of Matthew Bender Properties Inc.

Copyright © 2012 Matthew Bender & Company, Inc., a member of LexisNexis. All Rights Reserved.

No copyright is claimed by LexisNexis or Matthew Bender & Company, Inc., in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

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

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

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

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

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

**Chapter 1**

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

I. STARTING POINT: WHAT IS “PRIVACY”? ........................................... 1
II. THE BUSINESS VALUE OF INFORMATION ........................................... 6
III. COMPUTERS AND DIGITAL MEDIA: THEIR IMPACT ON PRIVACY ........... 7
IV. THE ROLE (AND RULE) OF LAW ..................................................... 8
V. CHALLENGES FOR THE RISK MANAGER ......................................... 9

*From “A Face is Exposed for AOL Searcher No. 4417749”* ......................... 10
VI. THE APPROACH OF THIS BOOK: PRACTICAL UNDERSTANDING AND A PATH TO BEST PRACTICES ......................................................... 11

**Chapter 2**

CONSUMER PRIVACY: BALANCING VALUE TO CONSUMERS WITH VALUE OF CONSUMERS ........ 13

I. WHY CONSUMER PRIVACY MATTERS: A LESS THAN CHEERY SCENARIO ......................................................... 13
II. CONSUMER INFORMATION COLLECTION AND THE RISE OF E-COMMERCE ..................................................... 14

*A Redefinition of the Concept of Personal Privacy* ........................................... 14
III. CONSUMER PRIVACY AND CONSUMER PROTECTION: THE FTC .......... 18

*Unfair methods of competition unlawful; prevention by Commission* .......... 18
*Fair Information Practice Principles Generally* ........................................... 19
IV. ANATOMY OF A PRIVACY POLICY: THE FAIR INFORMATION PRACTICE PRINCIPLES IN ACTION ......................................................... 26

*a. Notice/Awareness: Spreading the (Accurate) Word* .............................. 26
*b. Choice/Consent: Getting Informed Permission* ....................................... 29

*May 24, 2001 Letter from FTC Bureau of Consumer Protection to Junkbusters Corp and Electronic Privacy Information Center* .................. 29
*c. Integrity/Security: Keeping Data Safe and Unaltered* .............................. 31

*BJ’s Wholesale Club Settles FTC Charges Agency Says Lax Security Compromised Thousands of Credit and Debit Cards* .................. 31
*ValueClick to Pay $2.9 Million to Settle FTC Charges* ............................. 33
*d. Enforcement/Redress: Remedies for Wrongs* ........................................ 34

V. OTHER FEDERAL LAWS INVOLVING CONSUMER PRIVACY ............. 34
VI. STATE CONSUMER PRIVACY LAWS: LOCAL LEGISLATION, WIDE-RANGING IMPACT ......................................................... 39

*Cal. Bus. & Prof. Code § 22575. Commercial Web site operators; posting of privacy policy; violation of subdivision for failure to post policy; policy requirements* ......................................................... 40
TABLE OF CONTENTS

Excerpt from Cal. Civ. Code § 1798.83: Personal Information; Disclosure to Direct Marketers ................................................................. 41

VII. CONCLUSION: BEST PRACTICES START WITH ACCURATE DISCLOSURE ................................................................. 44

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

I. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT: THE KEY FEDERAL STATUTE ......................................................... 48

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

III. CONCLUSION: SOCIAL MEDIA PRIVACY: SIGNIFICANT CHALLENGES AND BEST PRACTICES ......................................................... 64

Chapter 4 THE SPECIAL CASE OF CHILDREN ......................................................... 67

I. LAW AND SELF-REGULATION TO PROTECT CHILDREN’S PRIVACY ......................................................... 69
   a. Self-Regulation: The CARU Guidelines ......................................................... 69
   b. The Origins of COPPA ......................................................... 74

II. REQUIREMENTS OF COPPA ......................................................... 83
   April 22, 2002 News Release: FTC Protecting Children’s Privacy Online .................. 85
   Iconix Brand Group Settles Charges Its Apparel Web Sites Violated Children’s Online Privacy Protection Act Company Will Pay $250,000 Civil Penalty .......................... 86

III. COPPA, THE FTC, AND THE EVOLUTION OF NEW TECHNOLOGIES ......................................................... 87
TABLE OF CONTENTS

An Examination of Children’s Privacy: New Technology and the Children’s Online Privacy Protection Act ........................................... 88
July 12, 2010 Comments by Facebook, Inc. on COPPA Review ........... 89
European NGO Alliance for Child Safety Online Submission to the FTC Review of the COPPA Rule .................................................. 90

IV. CONCLUSION: CHILDREN’S PRIVACY: SIGNIFICANT CHALLENGES AND BEST PRACTICES ................................................. 97
[Consumer Reports] Survey: 7.5 Million Facebook Users are Under the Age of 13, Violating the Site’s Terms ........................................ 97
Kids Today: How the Class of 2011 Engages with Media ..................... 98
A-Gs to probe kids’ privacy on Facebook ........................................ 99

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

I. HEALTH CONDITIONS AND GENETIC CODE: PREVENTING DISCRIMINATION AND DISCLOSURE ...................................... 102
Doe v. Borough of Barrington ....................................................... 107

II. OBLIGATIONS TO DISCLOSE: CASES AND STATUTES ..................... 121
Tarasoff v. Regents of University of California .................................. 122
Leonard v. Latrobe Area Hosp. ....................................................... 134
Persons and officials required to report cases of suspected child abuse or maltreatment .................................................. 139

III. THE CHALLENGES OF DIGITAL PERSONAL HEALTH INFORMATION .................................................. 140

IV. FEDERAL STATUTORY DIRECTIVES REGARDING ELECTRONIC MEDICAL RECORDS: HIPAA AND HITECH ....................... 141
a. Electronic Storage: The HIPAA Statutory Framework .................... 142
Recommendations With Respect to Privacy of Certain Health Information. .................................................. 142
Sec. 1173: Standards to Enable Electronic Exchange .......................... 143
b. HIPAA Regulations: The Privacy and Security Rules .................... 145
§ 160.103 Definitions. 45 CFR § 160.103. ...................................... 146
c. The HITECH Act and Revisions to HIPAA .................................. 157


**TABLE OF CONTENTS**

- HHS Enforcement of the HIPAA Privacy and Security Rules ................. 161
- University of California settles HIPAA Privacy and Security case involving UCLA Health System facilities UCLAHS to improve policies and procedures to better safeguard patient information ........................................... 163
- Rite Aid Agrees to Pay $1 Million to Settle HIPAA Privacy Case Company agrees to substantial corrective action to safeguard consumer information .................................................. 164
- STATE HEALTH PRIVACY LAWS .................................................. 165
- PRIVATE ENFORCEMENT OF PHI AND RELATED PRIVACY RIGHTS ................................................................. 167
  - *Sorrell v. Ims Health Inc.* .......................................................... 167

Chapter 6  FINANCIAL PRIVACY: INFORMATION AND VALUE . . 183

- I. VERIFIABLE IDENTITY FOR FINANCIAL TRANSACTIONS ......... 183
- II. THE RIGHT TO FINANCIAL PRIVACY ACT ............................... 184
- III. THE FAIR CREDIT REPORTING ACT ........................................ 187
  - From “40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations” ............................................. 209
- IV. THE GRAMM-LEACH BLILEY ACT ............................................ 210
  - Credit Report Resellers Settle FTC Charges; Security Failures Allowed Hackers to Access Consumers’ Personal Information ........................................ 214
- V. OTHER RELEVANT LAWS ......................................................... 216
- VI. PURCHASE PRIVACY: SELF-REGULATION AND INDUSTRY GUIDANCE ON LEGISLATION ......................................................... 216

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

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

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

II. EMPLOYEE PERSONAL INFORMATION: A NON-CONSUMER CONTEXT ..................................................... 257

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

I. THE CAUSES AND SCOPE OF DATA BREACHES ................. 260
    United States v. Ivanov ............................................. 262

II. LEGAL OBLIGATIONS TO PREVENT DATA BREACH ............ 270
    a. Self-Imposed Obligations: Contracts, Disclosure and Internal Policies ............................................. 270
    b. Spotting Potential Data Breach Vulnerability: The FTC’s Red Flags Rule ........................................ 279

III. POST-BREACH: DISCLOSURE AND LIABILITY .................... 282
        § 1798.81.5. Security procedures and practices with respect to personal information about California residents ............................................. 283
        § 1798.82. Civil actions; violation of title ............................................. 284
    b. Litigation Arising out of Data Breach ............................ 288
        Agency Announces Settlement of Separate Actions Against Retailer TJX, and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers’ Data ............................................. 288


In Re: Heartland Payment Systems, Inc. Customer Data Security Breach Litigation ............................................. 295

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

I. JURISDICTION: WHAT LAWS APPLY? ............................ 329

II. TWO MAJOR RELEVANT REGIMES: THE EU DATA PROTECTION DIRECTIVE AND PIPEDA ......................... 331
    a. The EU Data Protection Directive and the U.S. Safe Harbor ............................................. 331
    i. The EU Data Protection Directive ............................................. 331

SECTION IX: NOTIFICATION ............................................. 332

Chapter IV: Transfer of Personal Data to Third Countries ............................................. 334
## TABLE OF CONTENTS

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

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

#### I. THE FOURTH AMENDMENT AND DATA SEARCHES 350

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Guest v. Leis</td>
</tr>
<tr>
<td></td>
<td>United States v. Adjani</td>
</tr>
<tr>
<td></td>
<td>U.S. v. Horowitz</td>
</tr>
</tbody>
</table>

#### II. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT AND LAW ENFORCEMENT 379

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>People v. Harris</td>
</tr>
</tbody>
</table>

#### III. EYES IN THE GROUND AND SKY: THE USE OF GPS TRACKING AND DRONES IN LAW ENFORCEMENT 385

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>U.S. v. Jones</td>
</tr>
<tr>
<td></td>
<td>From “Did a Surveillance Drone Help in the Arrest of a North Dakota Farmer?”</td>
</tr>
</tbody>
</table>

### Chapter 11 ATTORNEYS: CLIENT PRIVACY AND ETHICS 397

#### I. APPLICABILITY OF PRIVACY LAWS AND REGULATIONS TO ATTORNEYS 397

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>American Bar Ass’n v. F.T.C.</td>
</tr>
<tr>
<td></td>
<td>Lawyer for preeminent firms pleads guilty in $37 million insider trading scheme using information stolen from employers</td>
</tr>
</tbody>
</table>

#### II. CLIENT CONFIDENTIAL INFORMATION: UNINTENTIONAL DISCLOSURE BY LAWYERS 416
# TABLE OF CONTENTS

Table of Cases ......................................................... TC-1

Index ................................................................. I-1
Chapter 1
INTRODUCTION: THE MEANING OF PRIVACY AND THE VALUE OF INFORMATION

I. STARTING POINT: WHAT IS “PRIVACY”?

Privacy means many things to many people. It can encompass everything from thought to action to location to identity to association to one’s very body. It is described as if it were physical; privacy can be “breached,” “lost,” “violated” or “protected,” even though it is not itself tangible. The earliest known uses of the English word “privacy” itself are from the 16th Century, potentially via a misspelling of the earlier “privity”.

The term’s very broadness makes it a challenging one to understand and use especially in the context of law and compliance. In U.S. law, the word “privacy” does not appear anywhere in the Constitution; the idea of a “right to privacy” is generally attributed to future Justice Louis D. Brandeis and his co-author Samuel D. Warren in their 1890 Harvard Law Review article of that title. In that groundbreaking article, Brandeis and Warren ascribe the growing need for this new right to the rise of business and technology:

"Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right “to be let alone.” Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the house-tops.” For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer. The alleged facts of a somewhat notorious case brought before an inferior tribunal in New York a few months ago, directly involved the consideration of the right of circulating portraits; and the question whether our law will recognize and protect the right to privacy in this and in other respects must soon come before our courts for consideration."
In the more than a century since the publication of the Brandeis and Warren article, a succession of Supreme Court cases have gleaned and defined a “right to privacy” arising from a number of the Constitution’s provisions, notably the Fourth, Fifth and Fourteenth Amendments, beginning with *Griswold v. Connecticut*:

*By Pierce v. Society of Sisters, supra, the right to educate one’s children as one chooses is made applicable to the States by the force of the First and Fourteenth Amendments. By Meyer v. State of Nebraska, supra, the same dignity is given the right to study the German language in a private school. In other words, the State may not, consistently with the spirit of the First Amendment, contract the spectrum of available knowledge. The right of freedom of speech and press includes not only the right to utter or to print, but the right to distribute, the right to receive, the right to read (Martin v. City of Struthers, 319 U.S. 141, 143, 63 S.Ct. 862, 863, 87 L.Ed. 1313) and freedom of inquiry, freedom of thought, and freedom to teach (see Wiener v. Updegraff, 333 U.S. 183, 195, 73 S.Ct. 215, 220, 97 L.Ed. 216)—indeed the freedom of the entire university community. Sweezy v. State of New Hampshire, 354 U.S. 257, 259–260, 77 S.Ct. 1203, 1211, 1217–1218, 1 L.Ed.2d 1311; 81 Barenblatt v. United States, 360 U.S. 109, 112, 79 S.Ct. 1081, 1085, 3 L.Ed.2d 1115; Baggett v. Bullitt, 377 U.S. 360, 369, 385 S.Ct. 1316, 1321, 12 L.Ed.2d 377. Without those peripheral rights the specific rights would be less secure. And so we reaffirm the principle of the Pierce and the Meyer cases.*

*In NAACP v. State of Alabama, 357 U.S. 449, 462, 78 S.Ct. 1163, 1172, we protected the ‘freedom to associate and privacy in one’s associations,’ noting that freedom of association was a peripheral First Amendment right. Disclosure of membership lists of a constitutionally valid association, we held, was invalid ‘as entailing the likelihood of a substantial restraint upon the exercise by petitioner’s members of their right to freedom of association.’ Ibid. In other words, the First Amendment has a penumbra where privacy is protected from governmental intrusion. In like context, we have protected forms of ‘association’ that are not political in the customary sense but pertain to the social, legal, and economic benefit of the members. NAACP v. Button, 371 U.S. 415, 430–431, 83 S.Ct. 328, 336–337. In Schwart v. Board of Bar Examiners, 353 U.S. 232, 77 S.Ct. 752, 1 L.Ed.2d 796, we held it not permissible to bar a lawyer from practice, because he had once been a member of the Communist Party. The man’s ‘association with that Party was not shown to be “anything more than a political faith in a political party” (id., at 244, 77 S.Ct. at 759) and was not action of a kind proving bad moral character. Ibid., at 245–246, 77 S.Ct. at 759–760.*

*Those cases involved more than the ‘right of assembly’—a right that extends to all irrespective of their race or ideology. De Jonge v. State of Oregon, 299 U.S. 353, 57 S.Ct. 255, 81 L.Ed. 278. The right of ‘association,’ like the right of belief (West Virginia State Board of Education v. Barnette, 319 U.S. 624, 63 S.Ct. 1178), is more than the right to attend a meeting; it includes the right to express one’s attitudes or philosophies by membership in a group or by affiliation with it or by other lawful means. Association in that context is a form of expression of opinion; and while it is not expressly included in the
First Amendment its existence is necessary in making the express guarantees fully meaningful.

The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. See Poe v. Ullman, 367 U.S. 497, 516–522, 81 S.Ct. 1752, 6 L.Ed.2d 989 (dissenting opinion). Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers ‘in any house’in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the ‘right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.’ The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: ‘The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.’

The Fourth and Fifth Amendments were described in Boyd v. United States, 116 U.S. 616, 630, 6 S.Ct. 524, 532, 29 L.Ed. 746, as protection against all governmental invasions ‘of the sanctity of a man’s home and the privacies of life.’ We recently referred in Mapp v. Ohio, 367 U.S. 643, 656, 81 S.Ct. 1684, 1692, 6 L.Ed.2d 1081, to the Fourth Amendment as creating a ‘right to privacy, no less important than any other right carefully and particularly reserved to the people.’ See Beaney, The Constitutional Right to Privacy, 1962 Sup.Ct.Rev. 212; Griswold, The Right to be Let Alone, 55 Nw.U.L.Rev. 216 (1960).


The present case, then, concerns a relationship lying within the zone of privacy created by several fundamental constitutional guarantees. And it concerns a law which, in forbidding the use of contraceptives rather than regulating their manufacture or sale, seeks to achieve its goals by means having a maximum destructive impact upon that relationship. Such a law cannot stand in light of the familiar principle, so often applied by this Court, that a governmental purpose to control or prevent activities constitutionally subject to state regulation may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms.’ NAACP v. Alabama, 377 U.S. 288, 307, 84 S.Ct. 1302, 1314, 12 L.Ed.2d 325. Would we allow the police to search the sacred precincts of marital bedrooms
for telltale signs of the use of contraceptives? The very idea is repulsive to the
notions of privacy surrounding the marriage relationship.

We deal with a right of privacy older than the Bill of Rights—older than our
political parties, older than our school system. Marriage is a coming together
for better or for worse, hopefully enduring, and intimate to the degree of being
sacred. It is an association that promotes a way of life, not causes; a harmony
in living, not political faiths; a bilateral loyalty, not commercial or social
projects. Yet it is an association for as noble a purpose as any involved in our
prior decisions.4

This “right” has been evoked in cases involving the permissibility of banning
medical procedures such as abortion,5 border searches of computers,6 and other
contexts, and is often evoked in the context of attempted governmental action.

Brandeis and Warren, though, showed true insight in recognizing that it was the
confluence of technological development and economic growth that would be at the
heart of the debate over whether a person should have the right “to be let alone.” For
them, the most serious affront was the rise of the popular press and its publication of
gossip:

Of the desirability — indeed of the necessity — of some such protection,
there can, it is believed, be no doubt. The press is overstepping in every
direction the obvious bounds of propriety and of decency. Gossip is no longer
the resource of the idle and of the vicious, but has become a trade, which is
pursued with industry as well as effrontery. To satisfy a prurient taste the
details of sexual relations are spread broadcast in the columns of the daily
papers. To occupy the indolent, column upon column is filled with idle gossip,
which can only be procured by intrusion upon the domestic circle. The
intensity and complexity of life, attendant upon advancing civilization, have
rendered necessary some retreat from the world, and man, under the refining
influence of culture, has become more sensitive to publicity, so that solitude
and privacy have become more essential to the individual; but modern
enterprise and invention have, through invasions upon his privacy, subjected
him to mental pain and distress, far greater than could be inflicted by mere
bodily injury. Nor is the harm wrought by such invasions confined to the
suffering of those who may be made the subjects of journalistic or other
enterprise. In this, as in other branches of commerce, the supply creates the
demand. Each crop of unseemly gossip, thus harvested, becomes the seed of
more, and, in direct proportion to its circulation, results in a lowering of
social standards and of morality. Even gossip apparently harmless, when
widely and persistently circulated, is potent for evil. It both belittles and
perverts. It belittles by inverting the relative importance of things, thus
dwarfing the thoughts and aspirations of a people. When personal gossip
attains the dignity of print, and crowds the space available for matters of real

6 U.S. v. Cotterman, 637 F.3d 1068 (9th Cir. 2011).
interest to the community, what wonder that the ignorant and thoughtless mistake its relative importance. Easy of comprehension, appealing to that weak side of human nature which is never wholly cast down by the misfortunes and frailties of our neighbors, no one can be surprised that it usurps the place of interest in brains capable of other things. Triviality destroys at once robustness of thought and delicacy of feeling. No enthusiasm can flourish, no generous impulse can survive under its blighting influence.\(^7\)

The inherent definition of “privacy” here is one of behavior, and its invasion or breach occurs when an individual’s behavior is monitored and then reported via popular press. There are two drivers: the “prurient” interest of the consumer public, and the desire for businesses to increase revenues by feeding that interest. To the extent that the individuals whose behavior is being reported have any competing interest (as Brandeis and Warren assert), that personal interest in “privacy” may not be able to counterweigh the others, especially if there is no legal support for the aggrieved party to complain.\(^8\) In their analysis of existing cases, they see a gap where traditional property and contract rights fail to explain how courts have prohibited certain types of disclosure and publication, and suggest that this implies (and requires) a separate right to privacy that should be formally recognized by the law.

There is, though, a second major meaning of “privacy” that is relevant for businesses in particular, which was not explicitly discussed in Brandeis and Warren’s piece: the collection and use of information relating to an individual’s identity, otherwise known as “personally identifiable information” or PII. The types of data that can constitute PII are quite varied. Certainly, specific data that refer to unique individuals (or at most a small group) are generally included: name, street address, telephone number, Social Security and similar identification numbers, and biological features (called biometrics) such as fingerprints, retinal patterns, voiceprints, and even DNA. PII, though, may encompass even those features and elements that are not particularly unique, such as occupation, hair or eye color, age, nationality, religion and family status, if these data in combination serve to identify a unique individual. As a fanciful example, consider these unrelated data points: male, 6’2” in height, black hair, blue eyes, grew up in Kansas. While there could hypothetically be many men who fit this description, adding a few more separate data points (newspaper reporter,...

\(^7\) 4 Harv. L. Rev. 193, 196 (1890).

\(^8\) To the extent that reported gossip is untrue, there might well be recourse in defamation laws, which were well established by Brandeis and Warren’s time, and are understood to be an exception to the right to free speech set forth in the First Amendment. See, e.g., Chaplinsky v. N.H., 315 U.S. 568, 571 (1942):

Allowing the broadest scope to the language and purpose of the Fourteenth Amendment, it is well understood that the right of free speech is not absolute at all times and under all circumstances. There are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which has never been thought to raise any Constitutional problem. These include the lewd and obscene, the profane, the libelous, and the insulting or ‘fighting’ words-those which by their very utterance inflict injury or tend to incite an immediate breach of the peace. It has been well observed that such utterances are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality. ‘Resort to epithets or personal abuse is not in any proper sense communication of information or opinion safeguarded by the Constitution, and its punishment as a criminal act would raise no question under that instrument.’ Cantwell v. Conn., 310 U.S. 296, 309, 310, 60 S.Ct. 900, 906, 84 L.Ed. 1213, 128 A.L.R. 1352.
superhero), themselves not unique (at least in the comic books), yields a single individual’s identity (or, perhaps secret identity): Clark Kent, aka Superman.

II. THE BUSINESS VALUE OF INFORMATION

For businesses, both user behavior and user identity can have substantial value. Companies sell more to customers when the offerings are better aligned with the customers’ preferences demonstrated through their shopping pattern. For that matter, knowing what a customer does and buys outside one’s own store can be tremendously helpful in enticing that customer into the store. Broader demographic information about potential customer populations can also assist companies in their strategic planning and advertising; this is why so many industries have sought to add specific queries to the decennial U.S. census:

> For much of American history, business interests have shaped questions in order to capture marketing data from the census. For instance, the 2000 census long form asked numerous questions about home and consumption habits. Even in the late 19th Century, business associations have played a strong role in the creation of specific census questions. Rather than just including the original questions of race, age, sex, the census grew to include complex socioeconomic questions. Various statistical associations along with the Chairperson of the Board of the American Marketing Association appoint the members of the official Census Advisory Committee of Professional Associations . . . .

Knowing the identity of current customers means that companies can offer a faster, more tailored experience, providing those goods or services the customer has previously or regularly purchased in a more prominent location, or being ready to give the customer “her usual.” Knowing who one’s potential customers are enables more effective sales pitches and solicitations; as much as consumers may be jaded when it comes to “personalized” messages in this database age, such messages are still more likely to catch their attention than those without the consumers’ names on the envelope or e-mail subject line.

Companies have also long understood that their customer records may have value to other firms, and have sought to monetize that value. Whether through sharing, renting or selling customer lists, or by sending third-party solicitations to one’s own customers, businesses are able to lower costs and generate revenue well outside their ordinary operations through data mining and marketing, at times beyond the earnings potential from their core businesses. Just as auto manufacturers have at times made more from their financing divisions than their dealerships, companies with detailed, high-worth customer lists can substantially boost their bottom lines without ever selling a single actual product to those customers. The same data may represent a substantial part of the value of the company as a whole to acquirers, financiers, and investors, whether directly or as a driver of the company’s success (through the ability

---

to better target the advertising whose sales are the company’s revenue source). Ultimately, in an economy driven by knowledge and information, knowing more things, about more people, will always be an asset. Absent any countervailing pressures, businesses and institutions would therefore continue to maximize their acquisition and exploitation of information about their customers (and even their own employees).

III. COMPUTERS AND DIGITAL MEDIA: THEIR IMPACT ON PRIVACY

Historically, one major countervailing pressure reducing organizations’ pursuit and use of behavioral and personal information as assets was the cost and difficulty of the effort. Observation of individuals often required dedicated personnel to track them, and manual record keeping was slow. The records themselves took up space, especially when the volume of records mounted, and sorting and sifting the records for useful data was also slow and expensive. Sharing the information required either giving up the original record or making a copy (which took almost as long as creating the original), and the copies were only as portable as the available transportation for them could handle: a warehouse worth of records required as much effort to move as a warehouse worth of goods.

Beginning in the 19th Century, though, new technologies sharply and permanently reduced the time, cost, and effort needed to create and share collections of data about individuals, steam engines powering land (railroad) and sea (steamships) vehicles meant that interstate and international travel and cargo carriage was both more reliable and could carry greater volumes of materials (including ledgers and other data records). Remote wired and wireless communications methods (from the telegraph to facsimile to the telephone and teletype and beyond) allowed for sharing of data with distant recipients. Handwritten records gave way to typewritten ones, manual duplication was superseded by carbon paper, mimeography, and photocopying, and written notes were replaced by punched cards.
These technologies, though, tended to be one-to-one in nature (one sender to one recipient; one original to one copy at a time), and also were prone to data corruption and loss. Each copy made was of lower quality than the original, making copies from copies accelerated the quality loss, and the original itself could be damaged by too-frequent copying. Transmission of records was also limited by the speed and quality of the connection. Further, even with methods for compressing information into machine-readable records like punch cards, the amount of storage required for a single set of records could be daunting, and each copy of the set required the same amount of storage. To copy a warehouse full of customer records, one needed enough boxes and trucks to move the contents of the warehouse, and a second warehouse to store the copy. These conditions placed practical limits on the amount of information any single organization could and would collect, and the extent to which that information could and would be shared with others.

IV. THE ROLE (AND RULE) OF LAW

With the ubiquity of computers, high-speed data networks and large-capacity storage, all at low and ever-lowering costs, organizations of every size collect, use, and share more data about users and their activities than ever before. Consumer awareness of, and concern about, this reality are also at historic highs. While market forces may exert some pressure on businesses to moderate their data collection and use practices (or at least to disclose them), they are insufficient, especially when the rewards for businesses for more and broader data exploitation are so great. Even where consumers may complain individually or in a group, they are rarely successful in engineering change in one organization, let alone many.

Just as Brandeis and Warren posited, the most effective way to set and enforce any limitations on privacy breaches by companies and other organizations is through the legal system. Legislation and regulation can (ideally) act to reflect the standards of the community, extend those standards to new situations, and ensure that those standards are met, and the context of privacy is no exception. Proactively (through establishing permissible and prohibited data collection and use) and reactively (via enforcement authorities and private rights of action in the courts), the law creates the structure for whether and how businesses may monitor, or learn more about, their users and customers.

The law focuses as well on many other privacy contexts, of course. Two in particular have close parallels to questions about businesses and their customers' information: the collection and use by companies of their employees' private information, and the acquisition and exploitation of individuals' PII and activities by governments and their agencies. In both of these other cases, actual and feared abuses, and the inability for either market forces or personal objections to ensure proper conduct, once more make the law a better avenue for change.

Neither legislation nor litigation, however, are the most efficient or rapid processes. The former is frequently subject to political process as well as legislators' subject matter expertise (or lack thereof), and the latter to barriers of cost and access to overburdened courts. For some types of risks and disputes, these real-world delays are
acceptable; when it comes to privacy issues driven by constantly changing technology, though, they can render the remedies all but useless.

V. CHALLENGES FOR THE RISK MANAGER

Risk is a key element in any venture or initiative. Risks cannot and should not be avoided; the key to successful growth of any initiative is to identify and manage the risks rather than letting them get out of control. Proper management in turn requires access to relevant information, and understanding the information and its context.

Given the complexity of privacy and data protection generally, and the particular impact of digital technologies on them, managing the related risks can be similarly complex for a few reasons. First, because the information needed for risk management may not be readily available. Even in a sole proprietorship, the owner and operator may not be completely aware of all personal information flowing into and out of the company, especially when the information is collected through automated processes or as a secondary effect. When a customer makes a payment by a personal check, the check itself may contain not only the customer’s bank and account number, but home address and even the name of the customer’s spouse or other joint account holder. The business may not have asked for that information, but it is presented with it just the same. Fax headers may include the sender’s name and fax number, single-line e-mail messages may have long signature blocks filled with personal information automatically inserted at the bottom, and so on. Internet-based communications come with their own set of automatically included information that can include arguably personal data. For example, any Web page request, instant message transmission or e-mail will include the sender’s IP address, which some courts and jurisdictions treat as personally identifiable information.18

Even less obvious a source of personal information is the referrer, a standard feature of Web browser software through which every Web page request is accompanied by a report of the page last visited. Most Web servers will collect and store that information in their log files. Ordinarily, referrer information does not contain personally identifiable information, but because of the way some Web sites construct their URLs, it can, which can have significant and unexpected legal consequences. Imagine a user who searches for references to himself via the Google search engine. Google search result pages include the query within their URLs. If his search was, for example, Jonathan Ezor, the first result page has this URL:

http://www.google.com/search?q=Jonathan%20Ezor

The next page the user visits, then, will receive as the “referrer” that Google search URL, including the user’s first and last name. If the site retains the referrer data in its logs, it is thereby collecting and storing the user’s personal information, even if it didn’t intend to. The privacy implications of referrer data have been raised in contexts

18 See, e.g., Joshua J. McIntyre, BALANCING EXPECTATIONS OF ONLINE PRIVACY: WHY INTERNET PROTOCOL (IP) ADDRESSES SHOULD BE PROTECTED AS PERSONALLY IDENTIFIABLE INFORMATION, 60 DePaul L. Rev. 895 (Spring 2011).
including the Tracking Protection Working Group of the World Wide Web Consortium, the standards body for the Web.\textsuperscript{19}

This is not just hypothetical. In one case, \textit{In re Pharmatrak, Inc.},\textsuperscript{20} a company that provided Web site analytical services to pharmaceutical companies was sued for collecting personal information of users in violation of its stated practices. The company did not \textit{intend} to collect the data; rather, its methodology enabled referrer data to be collected and saved, and those data were discovered to include personal information for a small percentage of site visitors. Out of the myriad visitors to the site, [fewer than 200] users' personal information was discovered among the referrer and similar information in the user logs, but that was sufficient to expose Pharmatrak to class action liability for breaching its privacy disclosure.

A similar situation arose involving the unintentional release of personally identifiable information. On August 6, 2006, AOL publicly released a database containing 20 million search queries from 658,000 “anonymized” users, as a research tool. While there were in fact no names or other expressly personal information provided, the database included numerical identifiers that allowed legitimate researchers (and anyone else) to group the searches by user. Given that many people tend to search terms relevant to their personal lives, reporters from the New York Times were able within two days to group, analyze, and positively identify a set of queries as coming from a specific individual:

\textbf{From “A Face Is Exposed for AOL Searcher No. 4417749”}

\textit{Buried in a list of 20 million Web search queries collected by AOL and recently released on the Internet is user No. 4417749. The number was assigned by the company to protect the searcher’s anonymity, but it was not much of a shield.}

\textit{No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from “numb fingers” to “60 single men” to “dog that urinates on everything.” . . . There are queries for “landscapers in Lilburn, Ga,” several people with the last name Arnold and “homes sold in shadow lake subdivision gwinnett county georgia.”}

\textit{It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends’ medical ailments and loves her three dogs . . . .}\textsuperscript{21}

Although AOL had already publicly withdrawn the data within a day of its being made available due to complaints,\textsuperscript{22} the database was already mirrored around the


\textsuperscript{22} Michael Arrington, \textit{AOL: “This Was a Screw Up,”} TECHCRUNCH (Aug. 7, 2006), http://techcrunch.com/2006/08/07/aol-this-was-a-screw-up/.
world, and remains available for diligent searchers as of August 2011. The incident was both embarrassing (the two key researchers responsible for the database’s release were terminated and the company’s Chief Technology Officer resigned, while Business 2.0 magazine called the publication of the database one of the “101 Dumbest Moments in Business for 2006” and legally problematic (a class action suit was pursued in California, and the Electronic Frontier Foundation filed a complaint with the FTC).

VI. THE APPROACH OF THIS BOOK: PRACTICAL UNDERSTANDING AND A PATH TO BEST PRACTICES

These situations highlight the unique challenges of digital privacy and the law: effective compliance and risk management requires not only knowledge of applicable laws and regulations, but at least a basic understanding of relevant technologies and the processes of the company or other organization that is collecting and/or using the personal information or monitoring behavior. Accordingly, the remaining chapters of this book are structured to provide a framework for law and other students to both learn the law and place it in the necessary technological and practical context, divided into topic areas such as children’s privacy, health information, governmental requirements, employee data, and more. The examples and best practices, study questions, and links to additional materials for each chapter (and supplemented through dedicated Web-based content) should be approached by readers not only as aids to understanding the law, but as guides for future counseling and decisionmaking.

---

26 See, e.g., Doe 1 v. AOL, LLC, 552 F.3d 1077 (9th Cir. 2009).
Chapter 2

CONSUMER PRIVACY: BALANCING VALUE TO CONSUMERS WITH VALUE OF CONSUMERS

Consumer privacy is both a general descriptor of privacy-related ideas (covering health, finance, commerce, and many other areas) and a more specific term. In its limited aspect, it refers to the collection, use and sharing by businesses of the personally identifiable information of (or about) potential or actual customers, whether in connection with a transaction or otherwise. Unlike many of the other areas of data privacy discussed in this book, there is currently no overall federal statute mandating specific business practices with regard to consumer privacy. Instead, it is left to companies to essentially police themselves via self-regulation, although as will be seen, enforcement authorities and the courts stand ready to take action if this self-regulation fails.

I. WHY CONSUMER PRIVACY MATTERS: A LESS THAN CHEERY SCENARIO

While there is a significant amount of discussion and attention on general consumer privacy, it may be somewhat difficult to understand why, when compared to areas of seemingly greater risk such as children’s privacy and the protection of financial and health information. To illustrate the potential concerns arising out of consumer privacy, consider the classic television sitcom “Cheers,” named for the fictional eponymous Boston bar where most of the “action” took place. The title of the show’s theme song, “Where Everybody Knows Your Name” by Gary Portnoy, was reflected in the way the main characters (the bar’s staff and the regular customers) knew about and got involved in each other’s lives. For the regulars, it was a given that they would be greeted by name and served their preferred drink as soon as they mounted the bar’s stools.

Imagine, though, a new customer named Fred walks into Cheers for the first time and discovers that everybody in fact knows his name and the bartender pours his favorite brand of beer without his even having to order it. Next, imagine this same customer traveling from Boston and encountering identical familiarity at every new bar into which he walks anywhere in the country, except that after the third week, every bartender insists the man’s name is Murray, and only serves him dry martinis. Even worse, at a few of the bars, he is welcomed with a bill for the three rounds of drinks he has told he has already purchased for the patrons before even walking through the door. On returning home and heading to his local pharmacy, the

pharmacist hands him an unasked-for bottle of ibuprofen for the headache he “must have after visiting so many bars,” and his mailbox is stuffed with coupons and offers from other brands of alcoholic beverages, who want him to switch away from his preferred beer. Would this situation be a problem? After all, our hypothetical bar visitor has been given the same type of favored service that Norm and Cliff enjoyed at Cheers. The crucial difference is that the visitor did not get a chance to choose to share (or withhold) his name, his drink preference, his travel history with the establishments in which he entered. Rather than feeling pampered, he is likely to be at best disturbed and at worst quite paranoid about the unwanted invasion into his identity and preferences.

II. CONSUMER INFORMATION COLLECTION AND THE RISE OF E-COMMERCE

Concerns such as those arising in the above hypothetical have informed discussions about best practices in consumer privacy for decades, especially in connection with computers and other information technologies. One of the most influential analyses of consumer privacy is Records, Computers and the Rights of Citizens (the “HEW Report”), prepared by the U.S. Department of Health, Education and Welfare (now Health and Human Services) in July 1973, particularly in its Section III:

A Redefinition of the Concept of Personal Privacy

Our review of existing law leads to the conclusion that agreement must be reached about the meaning of personal privacy in relation to records and record-keeping practices. It is difficult, however, to define personal privacy in terms that provide a conceptually sound framework for public policy about records and record keeping and a workable basis for formulating rules about record-keeping practices. For any one individual, privacy, as a value, is not absolute or constant; its significance can vary with time, place, age, and other circumstances. There is even more variability among groups of individuals. As a social value, furthermore, privacy can easily collide with others, most notably free speech, freedom of the press, and the public’s “right to know”

Dictionary definitions of privacy uniformly speak in terms of seclusion, secrecy, and withdrawal from public view. They all denote a quality that is not inherent in most record-keeping systems. Many records made about people are public, available to anyone to see and use. Other records, though not public in the sense that anyone may see or use them, are made for purposes that would be defeated if the data they contain were treated as absolutely secluded, secret, or private. Records about people are made to fulfill purposes that are shared by the institution maintaining them and the people to whom they pertain. Notable exceptions are intelligence records maintained for criminal investigation, national security, or other purposes. Use of a record about someone requires that its contents be accessible to at least one other person—and usually many other persons.

Once we recognize these characteristics of records, we must formulate a concept of privacy that is consistent with records. Many noteworthy attempts to address this need have been made.
Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

This is the core of the “right of individual privacy” — the right of the individual to decide for himself, with only extraordinary exceptions in the interests of society, when and on what terms his acts should be revealed to the general public.

The right to privacy is the right of the individual to decide for himself how much he will share with others his thoughts, his feelings, and the facts of his personal life.

As a first approximation, privacy seems to be related to secrecy, to limiting the knowledge of others about oneself. This notion must be refined. It is not true, for instance, that the less that is known about us the more privacy we have. Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.

The significant elements common to these formulations are (1) that there will be some disclosure of data, and (2) that the data subject should decide the nature and extent of such disclosure. An important recognition is that privacy, at least as applied to record-keeping practices, is not inconsistent with disclosure, and thus with use. The further recognition of a role for the record subject in deciding what shall be the nature and use of the record is crucial in relating the concept of personal privacy to record-keeping practices.

Each of the above formulations, however, speaks of the data subject as having a unilateral role in deciding the nature and extent of his self-disclosure. None accommodates the observation that records of personal data usually reflect and mediate relationships in which both individuals and institutions have an interest, and are usually made for purposes that are shared by institutions and individuals. In fact, it would be inconsistent with this essential characteristic of mutuality to assign the individual record subject a unilateral role in making decisions about the nature and use of his record. To the extent that people want or need to have dealings with record-keeping organizations, they must expect to share rather than monopolize control over the content and use of the records made about them.

Similarly, it is equally out of keeping with the mutuality of record-generating relationships to assign the institution a unilateral role in making decisions about the content and use of its records about individuals. Yet it is our observation that organizations maintaining records about people commonly behave as if they had been given such a unilateral role to play. This is not to suggest that decisions are always made to the disadvantage of the record subject; the contrary is often the case. The fact, however, is that the record subject usually has no claim to a role in the decisions organizations make about records that pertain to him. His opportunity to participate in those decisions depends on the willingness of the record-keeping organization to let him participate and, in a few instances, on specific rights provided by law.

Here then is the nub of the matter: Personal privacy, as it relates to personal-data
record keeping must be understood in terms of a concept of mutuality. Accordingly, we offer the following formulation:

An individual’s personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record. A record containing information about an individual in identifiable form must, therefore, be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it. Any recording, disclosure, and use of identifiable personal information not governed by such procedures must be proscribed as an unfair information practice unless such recording, disclosure or use is specifically authorized by law.

This formulation does not provide the basis for determining a priori which data should or may be recorded and used, or why, and when. It does, however, provide a basis for establishing procedures that assure the individual a right to participate in a meaningful way in decisions about what goes into records about him and how that information shall be used.

Safeguards for personal privacy based on our concept of mutuality in record-keeping would require adherence by record-keeping organizations to certain fundamental principles of fair information practice.

- There must be no personal-data record-keeping systems whose very existence is secret.
- There must be a way for an individual, to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

These principles should govern the conduct of all personal-data record-keeping systems. Deviations from them should be permitted only if it is clear that some significant interest of the individual data subject, will be served or if some paramount societal interest can be clearly demonstrated; no deviation should be permitted except as specifically provided by law.2

From the early 1970s, though, computers and networks expanded in functionality and ease of use (and dropped in cost), and spread from the largest corporations and

---

organizations to the smallest sole proprietorship. As a result, the definition of “record-keeping organization” evolved, and the quantity and diversity of those organizations increased far beyond what the drafters of the HEW Report may have assumed. When customer records were stored on paper, creating and managing them required significant physical space and manpower, and large-scale copying could take hours or days. With personal computers’ entry into businesses, file rooms, and archive warehouses were replaced with hard drives, and copying could be done with a click. With the addition of Internet connectivity, records could be shared and copied remotely, in bulk, by someone in another office or another country. This meant that every company could potentially market its customer list to other firms, and there were now many more sources of information about consumers for businesses to access and utilize.

While the revolution in customer data collection and use occurred in all types of companies, the broad adoption of the Internet by consumers revived a form of commerce that had been less popular for decades: mail order purchases via online storefronts. Historically, mail order had once been a key retail channel for the many rural communities that could not support larger shops; throughout the 20th Century, the archetypical Wells Fargo wagon and rural free delivery gave way to department stores anchoring shopping malls and big box retailers, with mail order becoming largely the province of specialty products and direct marketing (including “infomercials”). This trend began to reverse with two otherwise unrelated developments at around the same time: the invention of the World Wide Web protocol by Tim Berners-Lee at the CERN physics lab in 1989–90 and the withdrawal of the ban on commercial use of the Internet previously contained in the National Science Foundation’s Acceptable Use Policy for the Internet. As the now-commerce friendly Internet offered a growing series of retailing Web sites, as shoppers got Internet connections both at home and at work to access them, and as encryption technologies such as Secure Sockets Layer (“SSL”) were added to Web browser programs to increase both security and consumer confidence, mail order once again became a standard method for buying even products commonly available in local brick-and-mortar stores. Those same traditional offline retailers, seeing the new competition (and seeking to reduce the real estate and staffing-related costs of doing business), themselves created or

---


enhanced their mail-order and other online shopping resources. All of these online retailers, whether new or existing, were collecting much more information from and about consumers than would be true for most offline purchases: full names and delivery addresses, telephone numbers, credit card billing addresses, e-mail addresses for confirmation, and so on. The collection was not just to facilitate the transactions and reduce the chance of fraud: the retailers saw both research and resale value in the customer data.  

III. CONSUMER PRIVACY AND CONSUMER PROTECTION: THE FTC

With the expansion of collection and use of consumers' PII came the expansion of abuse potential. Consumer protection agencies such as the FTC and state Attorney General sharply expanded their monitoring and reporting of information practices, with the FTC in particular issuing a stream of reports and guidance for both Congress and businesses. The overall authority for the FTC's activities regarding privacy protection arises from Section 5 of the Federal Trade Commission Act, the statute (originally enacted in 1914) which established and empowered the FTC as the federal agency responsible for consumer protection:

Unfair methods of competition unlawful; prevention by Commission

(a) Declaration of unlawfulness; power to prohibit unfair practices; inapplicability to foreign trade

(1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.

(2) The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions described in section 57a(f)(3) of this title, Federal credit unions described in section 57a(f)(4) of this title, common carriers subject to the Acts to regulate commerce, air carriers and foreign air carriers subject to part A of subtitle VII of Title 49, and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921, as amended [7 U.S.C.A. § 181 et seq.], except as provided in section 406(b) of said Act [7 U.S.C.A. § 227(b)], from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

(3) This subsection shall not apply to unfair methods of competition involving commerce with foreign nations (other than import commerce) unless —


(A) such methods of competition have a direct, substantial, and reasonably foreseeable effect —

(i) on commerce which is not commerce with foreign nations, or on import commerce with foreign nations; or

(ii) on export commerce with foreign nations, of a person engaged in such commerce in the United States; and

(B) such effect gives rise to a claim under the provisions of this subsection, other than this paragraph.

If this subsection applies to such methods of competition only because of the operation of subparagraph (A)(ii), this subsection shall apply to such conduct only for injury to export business in the United States.

(4)(A) For purposes of subsection (a) of this section, the term “unfair or deceptive acts or practices” includes such acts or practices involving foreign commerce that —

(i) cause or are likely to cause reasonably foreseeable injury within the United States; or

(ii) involve material conduct occurring within the United States . . . .

In its 1998 “Privacy Online — A Report to Congress,” the FTC sets forth a detailed description of the “Fair Information Practice Principles” that it views as underlying responsible data collection:

**Fair Information Practice Principles Generally**

Over the past quarter century, government agencies in the United States, Canada, and Europe have studied the manner in which entities collect and use personal information — their “information practices” — and the safeguards required to assure those practices are fair and provide adequate privacy protection. The result has been a series of reports, guidelines, and model codes that represent widely-accepted principles concerning fair information practices. Common to all of these documents (hereinafter referred to as “fair information practice codes”) are five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.

1. **Notice/Awareness**

The most fundamental principle is notice. Consumers should be given notice of an entity’s information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information. Moreover, three of the other principles discussed below — choice/consent, access/participation, and enforcement/redress —

---

are only meaningful when a consumer has notice of an entity's policies, and his or her rights with respect thereto.

While the scope and content of notice will depend on the entity's substantive information practices, notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information:

- identification of the entity collecting the data;
- identification of the uses to which the data will be put;
- identification of any potential recipients of the data;
- the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information);
- whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and
- the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.

Some information practice codes state that the notice should also identify any available consumer rights, including:

- any choice respecting the use of the data;
- whether the consumer has been given a right of access to the data; the ability of the consumer to contest inaccuracies; the availability of redress for violations of the practice code; and how such rights can be exercised.

In the Internet context, notice can be accomplished easily by the posting of an information practice disclosure describing an entity's information practices on a company's site on the Web. To be effective, such a disclosure should be clear and conspicuous, posted in a prominent location, and readily accessible from both the site's home page and any Web page where information is collected from the consumer. It should also be unavoidable and understandable so that it gives consumers meaningful and effective notice of what will happen to the personal information they are asked to divulge.

2. Choice/Consent

The second widely-accepted core principle of fair information practice is consumer choice or consent. At its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information — i.e., uses beyond those necessary to complete the contemplated transaction. Such secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.

Traditionally, two types of choice/consent regimes have been considered: opt-in or opt-out. Opt-in regimes require affirmative steps by the consumer to allow the
collection and/or use of information; opt-out regimes require affirmative steps to prevent the collection and/or use of such information. The distinction lies in the default rule when no affirmative steps are taken by the consumer. Choice can also involve more than a binary yes/no option. Entities can, and do, allow consumers to tailor the nature of the information they reveal and the uses to which it will be put. Thus, for example, consumers can be provided separate choices as to whether they wish to be on a company's general internal mailing list or a marketing list sold to third parties. In order to be effective, any choice regime should provide a simple and easily-accessible way for consumers to exercise their choice.

In the online environment, choice easily can be exercised by simply clicking a box on the computer screen that indicates a user's decision with respect to the use and/or dissemination of the information being collected. The online environment also presents new possibilities to move beyond the opt-in/opt-out paradigm. For example, consumers could be required to specify their preferences regarding information use before entering a Web site, thus effectively eliminating any need for default rules.

3. Access/Participation

Access is the third core principle. It refers to an individual's ability both to access data about him or herself — i.e., to view the data in an entity's files — and to contest that data's accuracy and completeness. Both are essential to ensuring that data are accurate and complete. To be meaningful, access must encompass timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients.

4. Integrity/Security

The fourth widely accepted principle is that data be accurate and secure. To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form.

Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem.
5. Enforcement/Redress

It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them. Absent an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles. Among the alternative enforcement approaches are industry self-regulation; legislation that would create private remedies for consumers; and/or regulatory schemes enforceable through civil and criminal sanctions.

a. Self-Regulation

To be effective, self-regulatory regimes should include both mechanisms to ensure compliance (enforcement) and appropriate means of recourse by injured parties (redress). Mechanisms to ensure compliance include making acceptance of and compliance with a code of fair information practices a condition of membership in an industry association; external audits to verify compliance; and certification of entities that have adopted and comply with the code at issue. A self-regulatory regime with many of these principles has recently been adopted by the individual reference services industry.

Appropriate means of individual redress include, at a minimum, institutional mechanisms to ensure that consumers have a simple and effective way to have their concerns addressed. Thus, a self-regulatory system should provide a means to investigate complaints from individual consumers and ensure that consumers are aware of how to access such a system.

If the self-regulatory code has been breached, consumers should have a remedy for the violation. Such a remedy can include both the righting of the wrong (e.g., correction of any misinformation, cessation of unfair practices) and compensation for any harm suffered by the consumer. Monetary sanctions would serve both to compensate the victim of unfair practices and as an incentive for industry compliance. Industry codes can provide for alternative dispute resolution mechanisms to provide appropriate compensation.

b. Private Remedies

A statutory scheme could create private rights of action for consumers harmed by an entity’s unfair information practices. Several of the major information practice codes, including the seminal 1973 HEW Report, call for implementing legislation. The creation of private remedies would help create strong incentives for entities to adopt and implement fair information practices and ensure compensation for individuals harmed by misuse of their personal information. Important questions would need to be addressed in such legislation, e.g., the definition of unfair information practices; the availability of compensatory, liquidated and/or punitive damages; and the elements of any such cause of action.
c. Government Enforcement

Finally, government enforcement of fair information practices, by means of civil or criminal penalties, is a third means of enforcement. Fair information practice codes have called for some government enforcement, leaving open the question of the scope and extent of such powers. Whether enforcement is civil or criminal likely will depend on the nature of the data at issue and the violation committed.\(^\text{13}\)

The FTC continued to monitor and report to Congress on the progress (or lack thereof) of privacy protection for electronic commerce in its 1999 report \textit{Self-Regulation and Privacy Online}.\(^\text{14}\) As summarized by the FTC at the time:

\ldots The report describes the growth of electronic commerce, explains how Web sites collect information about consumers, explores consumers’ concerns about online privacy, and analyzes the state of online privacy self-regulation. The report states that “the Commission believes that legislation to address online privacy is not appropriate at this time. We also believe that industry faces some substantial challenges. Specifically, the present challenge is to educate those companies which still do not understand the importance of consumer privacy and to create incentives for further progress toward effective, widespread implementation.” It goes on to outline an agenda to address online privacy issues that includes a number of public workshops, task forces and an online survey, to reassess progress in Web sites’ implementation of fair information practices.

The report discusses the results of two studies of commercial Web sites conducted by Georgetown University Professor Mary Culnan, and the efforts of the Online Privacy Alliance, TRUSTe, BBBOnline, and others. “We continue to believe that effective self-regulation is the best way to protect consumer privacy on the Internet, and I am pleased that there has been real progress on the part of the online industry,” Chairman Pitofsky said. “Because of that progress, I do not believe legislation is necessary at this time. But this is not the occasion to declare victory. There is more to protecting consumer privacy than simply publishing notices on Web sites. We intend to monitor what we hope and expect will be continuing progress in development of privacy protection programs, as well as efforts to develop effective enforcement mechanisms. Responsible elements in the online business community have accomplished a great deal in a short time, but there is a considerable distance to go before consumers can feel secure from privacy invasions in their dealings on the Internet.”

In analyzing the state of online privacy self-regulation, the report emphasizes that “self-regulation is the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology.” Professor Culnan’s studies, the report

\(^\text{13}\) Id. at 7–11 (notes omitted).

points out, “suggest that the majority of the more frequently-visited Web sites are implementing the basic Notice principle by disclosing at least some of their information practices.” The report notes, however, that only a relatively small percentage of these sites are disclosing information practices that address all four substantive fair information practice principles: Notice, Choice, Access and Security. It also states that the privacy seal programs underway encompass only a small minority of all Web sites. “The self-regulatory programs described . . . reflect industry leaders’ substantial effort and commitment to fair information practices,” the report states.\(^\text{15}\)

By the next year, however, the FTC had changed its official stance on self-regulation, requesting that Congress enact general online privacy protection legislation:

. . . . Based on the past years of work addressing Internet privacy issues, including examination of prior surveys and workshops with consumers and industry, it is evident that online privacy continues to present an enormous public policy challenge. The Commission applauds the significant efforts of the private sector and commends industry leaders in developing self-regulatory initiatives. The 2000 Survey, however, demonstrates that industry efforts alone have not been sufficient. Because self-regulatory initiatives to date fall far short of broad-based implementation of effective self-regulatory programs, a majority of the Commission has concluded that such efforts alone cannot ensure that the online marketplace as a whole will emulate the standards adopted by industry leaders. While there will continue to be a major role for industry self-regulation in the future, a majority of the Commission recommends that Congress enact legislation that, in conjunction with continuing self-regulatory programs, will ensure adequate protection of consumer privacy online.

The proposed legislation would set forth a basic level of privacy protection for consumer-oriented commercial Web sites. Such legislation would establish basic standards of practice for the collection of information online, and provide an implementing agency with the authority to promulgate more detailed standards pursuant to the Administrative Procedure Act.

Consumer-oriented commercial Web sites that collect personal identifying information from or about consumers online would be required to comply with the four widely-accepted fair information practices:

(1) **Notice** — Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (e.g., directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.

(2) **Choice** — Web sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (e.g., to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).

(3) **Access** — Web sites would be required to offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information.

(4) **Security** — Web sites would be required to take reasonable steps to protect the security of the information they collect from consumers.

The Commission recognizes that the implementation of these practices may vary with the nature of the information collected and the uses to which it is put, as well as with technological developments. For this reason, a majority of the Commission recommends that any legislation be phrased in general terms and be technologically neutral. Thus, the definitions of fair information practices set forth in the statute should be broad enough to provide flexibility to the implementing agency in promulgating its rules or regulations.

Finally, the Commission notes that industry self-regulatory programs would continue to play an essential role under such a statutory structure, as they have in other contexts. The Commission hopes and expects that industry and consumers would participate actively in developing regulations under the new legislation and that industry would continue its self-regulatory initiatives. The Commission also recognizes that effective and widely-adopted seal programs could be an important component of that effort.

For all of these reasons, a majority of the Commission believes that its proposed legislation, in conjunction with self-regulation, will ensure important protections for consumer privacy at a critical time in the development of the online marketplace. Without such protections, electronic commerce will not reach its full potential and consumers will not gain the confidence they need in order to participate fully in the online marketplace . . . .

Notwithstanding the FTC’s request, however, Congress did not pass and has not to date passed overall information privacy legislation for electronic commerce, leaving privacy protection subject to self-regulation; that is, depending on companies to “do the right thing” with consumer information. What that entails, as per the FTC’s reports, has come to be known as a privacy policy.

---

IV. ANATOMY OF A PRIVACY POLICY: THE FAIR INFORMATION PRACTICE PRINCIPLES IN ACTION

The term “privacy policy” is actually somewhat confusing; it isn’t so much an establishment of a policy for the company but rather a disclosure of the existing information collection and use practices of the company. The practices themselves should track the Fair Information Practice Principles in order for the company to be self-regulating as described by the FTC,17 with particular attention required for the first of the principles notice and awareness:

a. Notice/Awareness: Spreading the (Accurate) Word

At the core of the FTC’s potential willingness to accept self-regulation over legislative mandates is the requirement that those from whom information is to be collected must be aware of the collection and the purposes to which the information will be put, including with whom else it may be shared. Such awareness may not be assumed, but requires notice of the practices to be at least available to the individual prior to the collection. The “privacy policy” placed on a Web site is the generally accepted form of such notice.

One aspect of making notice available is its presentation: how prominent and easy to obtain and read is the privacy policy? Is it linked from every page, just the home page, or some combination? Is the link obvious and properly labeled? Is it on a separate page, or a pop-up which might be blocked by some browser programs? Is the language clear or confusing legalese? Is it formatted for different sized devices? The more prominent, clear, and accessible the privacy policy is, the more likely it would pass muster with the FTC and other enforcement bodies.

Having a legible privacy policy, however, is far from the only or even most important aspect of notice. Where too many organizations err, and where the FTC and other enforcers have been very willing to exercise their authority, is in the requirement that the privacy policy above all be accurate. An inaccurate privacy policy, one which does not correctly describe the data collection and use practices of the site posting it, can yield liability for the siteowner, even if both what the policy describes and what the site is doing are both legal, because the inaccuracy means that the consumer was not actually given notice.

17 In February 2012, the Obama Administration released its “Consumer Privacy Bill of Rights,” which included an updated statement of the Fair Information Practice Principles encompassing:

- Individual control over what personal data organizations collect from them and how they use it
  - Transparency that allows consumers to easily understand information about privacy and security practices
  - Respect for the context in which consumers provide data
  - Security and responsibility in the way companies handle personal data
  - Access to personal data in usable format and an ability to correct errors
  - Reasonable limits on the personal data that companies collect and retain
  - Accountability as to how companies handle personal data.

Among the most common inaccuracies in privacy policies is some version of the following reassuring statement:

*We do not share your personal information with any third parties.*

This is essentially *never* true, if only because of how the Internet functions. There are so many third parties involved in connecting the sender and recipient of content (whether an e-mail message, a Web page, or something else), and so many other third parties specifically involved in the process of commerce, that some portion of the consumer’s personal information will inevitably be shared with one or more of those third parties. Again, this may not be illegal, and may even be what the consumer wants, but the privacy policy’s inaccurate statement can nevertheless expose the publisher of the policy to liability.

Consider the following illustration describing a hypothetical e-commerce site, CuteFuzzyBears.com:

As with many other such companies, CuteFuzzyBears does not maintain its own warehouse, but outsources the picking, packing, and shipping of its bears to another company, which maintains a relationship with a home delivery courier service. CuteFuzzyBears also contracts with a manufacturer in China to make and ship bears as needed; the warehouse maintains the inventory and reports low levels to CuteFuzzyBears, which then orders new merchandise to be sent directly to the warehouse. CuteFuzzyBears works with one vendor to process credit card information and a different one to manage the flow of funds from the card issuers (a typical situation). Finally, CuteFuzzyBears uses a Web development and hosting firm to create, operate,
maintain, and update its site.

In the illustration, a sender wishes to buy a teddy bear and have it sent as a gift to a friend. The sender accesses CuteFuzzyBears.com, skims through the available bears, and decides to order one. Thanks to a real-time inventory report from the outside warehouse, the site shows that the desired bear is in stock. The sender clicks to place an order, and is presented with a form in which to enter payment and delivery information, including the sender’s billing address and credit card data and the recipient’s name and address. The sender types in the data and presses “Submit,” after which he is shown a confirmation page with all the entered data. Once he confirms the information, he clicks once more to actually place the order.

Once the order is accepted, CuteFuzzyBears asks its credit card processor to pre-authorize the transaction; that is, to verify the account and billing information and ensure that there is sufficient credit available to pay for the bear once it’s ready to ship. The processor communicates with the issuing bank and, if the credit is available, places a temporary “pre-authorization hold” on that amount of credit to keep the purchaser from using it for more than one purchase. The processor reports back to CuteFuzzyBears that the credit is available, and CuteFuzzyBears notifies the warehouse to pick, pack, and ship that particular bear to the recipient’s address. The warehouse gets the shipment ready, hands it off to the courier, and transmits a tracking number to CuteFuzzyBears indicating that it has shipped. CuteFuzzyBears then notifies the credit card processor that it has earned payment, after which the processor communicates with the issuing bank and instructs it to transfer the payment amount through CuteFuzzyBears’ payment processing (or merchant account) company (this is called “settlement”). CuteFuzzyBears gets paid (minus processing fees and other possible charges), the bear gets delivered to the recipient, and when the credit card comes due for payment, the buyer, issuing bank, and the bank holding the buyer’s savings collaborate to pay the bill. (The dotted lines on the illustration to “VISA/MC/Amex” indicate the policies of the credit card brand owners that govern how issuing banks and customers may utilize the cards bearing their marks.)

In order to fulfill the order that the buyer wishes to place, CuteFuzzyBears must transmit personal information from the buyer to its Web host, the buyer’s ISP (on its way to the buyer), the credit card processing and payment firms, the issuing bank, and (if the buyer’s identity will be placed on the package) the warehouse and courier, not to mention the recipient. Even without purchases and shipments, the mere act of repeating back the information the buyer has provided passes that information through CuteFuzzyBears’ Web hosting company and the buyer’s ISP at a minimum. Each of those is a “third party” with which CuteFuzzyBears is “sharing” the buyer’s personal information, and this type of “sharing” is inevitable for any Web site operator, making those general “comforting” statements red flags of inaccuracy.

Other inaccuracies arise because many site owners (and even, regrettably, their attorneys) copy and paste language from a “good policy” published by another site for their own privacy statement. Unfortunately, unless by some miraculous coincidence the source site’s data collection and use practices are identical to those of the site copying the language, the policy will be at least somewhat incorrect in its description, and therefore will not be providing the required notice and enabling awareness.
One further source of inaccuracy (or at least incompleteness) is lack of knowledge on the part of the siteowner’s employees about the actual data practices of the company. Those responsible for drafting the policy, even if they do so from scratch, may not know all the ways personal information comes in, is utilized, and leaves the organization. For example, the policy may state that the company “only” collects personal information via a form on a Web site. That may well be one inbound channel, but if the company receives and logs telephone calls, e-mails, faxes or other communications from the customer, those represent additional ways the company collects information that must also be disclosed. The same goes for how data are used and shared; even if the company is not selling its customers’ personal information to marketers, it may be storing the data in a third-party, offsite backup facility (which is thus being “provided” with the information).

b. Choice/Consent: Getting Informed Permission

Assuming that the notice was accurate and effective in communicating the company’s data practices to the consumer, self-regulation next requires that the consumer agree to participate in the data collection and use. The agreement may not have to be explicit (i.e., a signature on a contract), but it should be possible for the consumer to consent, or choose not to, before the information is collected. Ideally, there should also be a method for the consumer to subsequently withdraw previously granted consent.

What happens, however, when the business wishes to change its information practices, especially if it intends to broaden its use or sharing beyond that to which consumers have already consented? In such circumstances, the company may prefer not to request permission for the new use from its existing customers, since the request may draw unwanted scrutiny to its plans and generate consumer discomfort or withdrawals of consent. One option is to segregate the data into “before” and “after” files, and only change the practices for the “after” customers. This, though, may reduce the value to the company of the new uses (for example, if it is looking to share its customer list with another marketer; segregation could substantially reduce the quantity of names and addresses being provided).

The other alternative would be to merely provide notice of the change, and offer consumers the opportunity to opt out of the added or changed uses of their personal information. This may, however, not be deemed sufficient by consumer protection agencies or the courts, as discovered by Amazon.com after it sought to change its information use practices in 2000:

May 24, 2001 Letter from FTC Bureau of Consumer Protection to Junkbusters Corp and Electronic Privacy Information Center

... On December 4, 2000, Junkbusters Corp. and the Electronic Privacy Information Center filed a joint petition requesting that the Federal Trade Commission (“FTC”) investigate whether Amazon.com (“Amazon”) deceived consumers in its representations about privacy and the circumstances under which Amazon might disclose information about its customers.
In reviewing the petition, FTC staff considered whether Amazon, under its revised privacy policy, changed its practices with respect to its collection and use of personal information in a way that was deceptive or unfair in violation of Section 5 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45. Based upon information we received from Amazon concerning its actual information disclosure practices, including correspondence attached to this letter as Exhibit A, staff believes that Amazon’s revised privacy policy does not materially conflict with representations Amazon made in its previous privacy policy and that it likely has not violated Section 5 of the FTC Act.

Amazon’s previous privacy policy stated that “Amazon.com does not sell, trade, or rent your personal information to others. We may choose to do so in the future with trustworthy third parties, but you can tell us not to by sending a blank e-mail message to never@amazon.com.” Exhibit B at 2. You are concerned that under its revised privacy policy, Amazon may now disclose personal information about consumers who previously selected “never.” Amazon has assured us that, despite the ambiguity of its revised policy on this issue, it will not disclose to third parties any personal information concerning consumers who previously selected “never.” Moreover, Amazon has informed the FTC that it has never sold, traded, or rented the personal information of any of its customers, even those customers who did not e-mail never@amazon.com, and it will not do so without notice to its customers and an opportunity for them to choose not to have their information shared. Exhibit A at 2–3.

Although Amazon’s revisions to its privacy policy are subject to various interpretations, Amazon’s letter describes its actual practices. It thus does not appear that Amazon has violated Section 5 of the FTC Act by making material changes in its previously disclosed information collection and disclosure policies. We would expect that in the event of a material change to its stated privacy practices, Amazon would provide adequate notice to customers as well as a mechanism to obtain consumers’ consent to the change with respect to information already collected from them. In addition, we of course would urge Amazon and others developing their privacy policies to make their policies clear and understandable to consumers.

We appreciate your bringing this matter to our attention. Petitions from groups such as yours are a helpful means of reviewing possible unfair or deceptive practices, and we hope you will continue to bring to our attention any practices that you believe may violate the FTC Act.18

A key point from this letter is the FTC’s view that in the event of a “material change” to a stated privacy policy, Amazon (or any other collector) would be required not only to provide “adequate notice” of the change, but to obtain “consumers’ consent to the change with respect to information already collected from them.” That is, if a business makes a material change (however that might be defined) to its practices, it must obtain an opt-in from customers whose information was previously collected before applying the change to those data. Otherwise, it could face enforcement for unfair or deceptive practices. For clients whose businesses, and privacy practices, may

---

evolve over time, it is essential that they are aware of this obligation.

Note as well that it is not merely changes in practices that might trigger this opt-in obligation, but to the statement of those practices contained in a privacy policy. To the extent that a company has published an *inaccurate* privacy policy, and seeks to correct it, the correction itself could be deemed a “material change” requiring affirmative consent from those from whom the company has previously collected personal information. This can offer significant challenges for businesses and their counsel seeking to improve their compliance with self-regulatory principles.

c. **Integrity/Security: Keeping Data Safe and Unaltered**

A business’ obligations regarding personally identifiable information collected from consumers are not solely connected with the use and sharing of those data. Companies are also required under the Fair Information Practice Principles to take steps to protect the security and integrity of the information. These are related but not identical concepts. Security represents the methods, both physical and electronic, to prevent unauthorized access to the data both during transmission and when stored. Integrity refers to the business’ obligation to protect the data from being edited, changed, damaged, or deleted other than by those permitted to do so. A company that fails to maintain either the security or integrity of the data entrusted to it could expose both itself and its customers to risks including identity theft, reputational damage, financial loss, and others.

As previously stated, there is as of yet no federal general privacy law for consumer information, nor is there an industry-neutral statutory obligation regarding either data security or integrity. This has not, however, prevented the FTC from taking action against companies for their failures to maintain security and integrity for consumer data, whether or not the companies’ privacy policies promised specific protection:

**BJ'S Wholesale Club Settles FTC Charges Agency Says Lax Security Compromised Thousands of Credit and Debit Cards**

BJ’s Wholesale Club, Inc. has agreed to settle Federal Trade Commission charges that its failure to take appropriate security measures to protect the sensitive information of thousands of its customers was an unfair practice that violated federal law. According to the FTC, this information was used by an unauthorized person or persons to make millions of dollars of fraudulent purchases. The settlement will require BJ’s to implement a comprehensive information security program and obtain audits by an independent third party security professional every other year for 20 years.

Natick, Massachusetts-based BJ’s operates 150 warehouse stores and 78 gas stations in 16 states in the Eastern United States. Approximately 8 million consumers are currently members, with net sales totaling about $6.6 billion in 2003.

19 There are, however, requirements connected with specific industries such as health and financial privacy. For more discussion of these, see Chapter 5 and Chapter 6 of this book respectively.
“Consumers must have the confidence that companies that possess their confidential information will handle it with due care and appropriately provide for its security,” said Deborah Platt Majoras, Chairman of the FTC. “This case demonstrates our intention to challenge companies that fail to protect adequately consumers' sensitive information.”

According to the FTC's complaint, BJ's uses a computer network to obtain bank authorization for credit and debit card purchases and to track inventory. For credit and debit card purchases at its stores, BJ's collects information, such as name, card number, and expiration date, from the magnetic stripe on the back of the cards. The information is sent from the computer network in the store to BJ's central datacenter computer network and from there through outside computer networks to the bank that issued the card.

The FTC charged that BJ's engaged in a number of practices which, taken together, did not provide reasonable security for sensitive customer information. Specifically, the agency alleges that BJ's:

- Failed to encrypt consumer information when it was transmitted or stored on computers in BJ's stores;
- Created unnecessary risks to the information by storing it for up to 30 days, in violation of bank security rules, even when it no longer needed the information;
- Stored the information in files that could be accessed using commonly known default user IDs and passwords;
- Failed to use readily available security measures to prevent unauthorized wireless connections to its networks; and
- Failed to use measures sufficient to detect unauthorized access to the networks or to conduct security investigations.

The FTC's complaint charges that the fraudulent purchases were made using counterfeit copies of credit and debit cards used at BJ's stores, and that the counterfeit cards contained the same personal information BJ's had collected from the magnetic stripes of the cards. After the fraud was discovered, banks cancelled and re-issued thousands of credit and debit cards, and consumers experienced inconvenience, worry, and time loss dealing with the affected cards. Since then, banks and credit unions have filed lawsuits against BJ's and pursued bank procedures seeking the return millions of dollars in fraudulent purchases and operating expenses. According to BJ’s SEC filings, as of May 2005, the amount of outstanding claims was approximately $13 million.

The FTC alleges that BJ’s failure to secure customers’ sensitive information was an unfair practice because it caused substantial injury that was not reasonably avoidable by consumers and not outweighed by offsetting benefits to consumers or competition. The settlement requires BJ’s to establish and maintain a comprehensive information security program that includes administrative, technical, and physical safeguards. The settlement also requires BJ’s to obtain an audit from a qualified, independent, third-party professional that its security program meets the standards
of the order, and to comply with standard book keeping and record keeping provisions.

The Commission vote to accept the proposed consent agreement was 5-0. The FTC will publish an announcement regarding the agreement in the Federal Register shortly. The agreement will be subject to public comment for 30 days, beginning today and continuing through July 16, 2005, after which the Commission will decide whether to make it final. Comments should be addressed to the FTC, Office of the Secretary, Room H-159, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. The FTC is requesting that any comment filed in paper form near the end of the public comment period be sent by courier or overnight service, if possible, because U.S. postal mail in the Washington area and at the Commission is subject to delay due to heightened security precautions.

Copies of the complaint and consent agreement are available from the FTC's Web site at http://www.ftc.gov and also from the FTC's Consumer Response Center, Room 130, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint in English or Spanish (bilingual counselors are available to take complaints), or to get free information on any of 150 consumer topics, call toll-free, 1-877-FTC-HELP (1-877-382-4357), or use the complaint form at http://www.ftc.gov. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.20

ValueClick to Pay $2.9 Million to Settle FTC Charges

Online advertiser ValueClick, Inc., will pay a record $2.9 million to settle Federal Trade Commission charges that its advertising claims and e-mails were deceptive and violated federal law. The agency also charged that ValueClick and its subsidiaries, Hi-Speed Media and E-Babylon failed to secure consumers’ sensitive financial information, despite their claims to do so . . . .

The FTC . . . charged that ValueClick, Hi-Speed Media, and E-Babylon, misrepresented that they secured customers’ sensitive financial information consistent with industry standards. The FTC alleged the companies published online privacy policies claiming they encrypted customer information, but either failed to encrypt the information at all or used a non-standard and insecure form of encryption. The agency also charged that several of the companies’ e-commerce Web sites were vulnerable to SQL injection, a commonly known form of hacker attack, contrary to claims that the companies implemented reasonable security measures . . . .

The settlement . . . bars ValueClick, Hi-Speed Media, and E-Babylon from making

---

misrepresentations about the use of encryption or other electronic measures to protect consumers’ information, and about the extent to which they protect personal information. The order also requires the companies to establish and maintain a comprehensive security program, and obtain independent third-party assessments of their programs, for 20 years . . . .

d. Enforcement/Redress: Remedies for Wrongs

Self-regulation does not preclude the possibility of problems arising; in fact, the FIPP mandates that organizations collecting personal information provide some level of user remediation in the event of issues with their practices. As discussed above, consumers may and ideally will have access to internal (company-specific), private external (trade associations; alternative dispute resolution bodies) and governmental channels for both enforcement and redress. Businesses that are members of industry groups and associations should be particularly aware of any enforcement and other privacy-related mandates that may be imposed upon them as members, both in order to comply with the mandates and to be prepared for any group-driven enforcement they may face.

One more potential avenue of redress for consumers is through the activities of advocacy organizations such as the Electronic Privacy Information Center, the Electronic Frontier Foundation, and others. These groups monitor, inform, and actively litigate on behalf of digital privacy rights, often prompting FTC and other enforcement action through their initiatives.

V. OTHER FEDERAL LAWS INVOLVING CONSUMER PRIVACY

While there remains no general federal Internet privacy law, there are federal statutes and regulations that nevertheless impose specific consumer privacy-related obligations. One is the Video Privacy Protection Act. This statute was originally enacted following the use of Judge Robert Bork’s personal video rental records in the Senate confirmation hearing as part of the effort to derail his (ultimately unsuccessful)
nomination to the U.S. Supreme Court. The statute provides in relevant part:

(b) Video tape rental and sale records. — (1) A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d).

(2) A video tape service provider may disclose personally identifiable information concerning any consumer —

(A) to the consumer;
(B) to any person with the informed, written consent of the consumer given at the time the disclosure is sought;
(C) to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;
(D) to any person if the disclosure is solely of the names and addresses of consumers and if —

(i) the video tape service provider has provided the consumer with the opportunity, in a clear and conspicuous manner, to prohibit such disclosure; and
(ii) the disclosure does not identify the title, description, or subject matter of any video tapes or other audio visual material; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;
(E) to any person if the disclosure is incident to the ordinary course of business of the video tape service provider; or
(F) pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, if —

(i) the consumer is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and
(ii) the consumer is afforded the opportunity to appear and contest the claim of the person seeking the disclosure.

If an order is granted pursuant to subparagraph (C) or (F), the court shall impose appropriate safeguards against unauthorized disclosure.

(3) Court orders authorizing disclosure under subparagraph (C) shall issue only with prior notice to the consumer and only if the law enforcement
agency shows that there is probable cause to believe that the records or other information sought are relevant to a legitimate law enforcement inquiry. In the case of a State government authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the video tape service provider, may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on such provider.

(c) Civil action. — (1) Any person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court.

(2) The court may award —

(A) actual damages but not less than liquidated damages in an amount of $2,500;

(B) punitive damages;

(C) reasonable attorneys’ fees and other litigation costs reasonably incurred; and

(D) such other preliminary and equitable relief as the court determines to be appropriate.

(3) No action may be brought under this subsection unless such action is begun within 2 years from the date of the act complained of or the date of discovery.

(4) No liability shall result from lawful disclosure permitted by this section.

(d) Personally identifiable information. — Personally identifiable information obtained in any manner other than as provided in this section shall not be received in evidence in any trial, hearing, arbitration, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision of a State.29

Recent developments in technology, both in the method for delivering rented videos (DVDs and now downloadable and streaming video) and providing consent have posed challenges to the understanding and applicability of the Video Privacy Protection Act. On the delivery side, the definition of “video tape rental service” contained in the statute can still be read to encompass other media and delivery mechanisms:

the term “video tape service provider” means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subpara-

29 Id. Sections (b) through (d).
graph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure . . . .30

The requirement for “written consent,” however, may not include current online methods for consumer consent, whether directly provided to the rental/streaming site or via a partnership with another site such as Facebook. A bill introduced in the 112th Congress31 sought to broaden the permissible methods of consent accordingly:

Section 2710(b)(2) of title 18, United States Code, is amended by striking subparagraph (B) and inserting the following:

‘(B) to any person with the informed, written consent (including through an electronic means using the Internet) in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer given at one or both of the following times —

‘(i) the time the disclosure is sought; and

‘(ii) in advance for a set period of time or until consent is withdrawn by such consumer;’32

Companies must also consider privacy-related obligations coming from other areas of law. One notable example arises in federal bankruptcy law, addressing the possibility that personal information could be found among the assets that may be sold to help repay creditors in a bankruptcy. Depending on the details of the proposed sale, it could violate the terms of a privacy policy under which the information was originally collected. In such a circumstance, the court-appointed trustee must follow additional procedures to address privacy concerns:

§ 332. Consumer privacy ombudsman

(a) If a hearing is required under section 363(b)(1)(B),33 the court shall order the United States trustee to appoint, not later than 7 days before the

30 Id. § 2710(a)(4) (2006).
32 See supra note 54.
33 11 U.S.C. § 363(b) states:

(b)(1) The trustee, after notice and a hearing, may use, sell, or lease, other than in the ordinary course of business, property of the estate, except that if the debtor in connection with offering a product or a service discloses to an individual a policy prohibiting the transfer of personally identifiable information about individuals to persons that are not affiliated with the debtor and if such policy is in effect on the date of the commencement of the case, then the trustee may not sell or lease personally identifiable information to any person unless —

(A) such sale or such lease is consistent with such policy; or

(B) after appointment of a consumer privacy ombudsman in accordance with section 332, and after notice and a hearing, the court approves such sale or such lease —

(i) giving due consideration to the facts, circumstances, and conditions of such sale or such lease; and

(ii) finding that no showing was made that such sale or such lease would violate applicable nonbankruptcy law.
commencement of the hearing, 1 disinterested person (other than the United States trustee) to serve as the consumer privacy ombudsman in the case and shall require that notice of such hearing be timely given to such ombudsman.

(b) The consumer privacy ombudsman may appear and be heard at such hearing and shall provide to the court information to assist the court in its consideration of the facts, circumstances, and conditions of the proposed sale or lease of personally identifiable information under section 363(b)(1)(B). Such information may include presentation of —

(1) the debtor’s privacy policy;

(2) the potential losses or gains of privacy to consumers if such sale or such lease is approved by the court;

(3) the potential costs or benefits to consumers if such sale or such lease is approved by the court; and

(4) the potential alternatives that would mitigate potential privacy losses or potential costs to consumers.

(c) A consumer privacy ombudsman shall not disclose any personally identifiable information obtained by the ombudsman under this title.

Section 332 was added to the federal bankruptcy law in 2005 in response to cases such as that of Toysmart, in which an Internet retailer undergoing an involuntary liquidation sought to sell its customer lists as part of the bankruptcy proceedings. The FTC objected, based upon the language of Toysmart’s privacy policy:

Through its Web site, Toysmart collects detailed personal information about its visitors, including name, address, billing information, shopping preferences, and family profiles, which include the names and birthdates of children. Since September 1999, Toysmart has posted a privacy policy which states that information collected from customers will never be shared with third parties.

That policy states that:

Personal information, voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party.

The policy continues:

When you register with toysmart.com, you can rest assured that your information will never be shared with a third party.

Toysmart subsequently settled with the FTC over many of these privacy policy issues.

(although COPPA-related children’s privacy claims were not included in the settlement):

[126x547]. . . . Under the settlement agreement, Toysmart will file an order . . . in Bankruptcy Court (“Bankruptcy Order”), prohibiting Toysmart from selling the customer list as a stand-alone asset. The settlement only allows a sale of such lists as a package which includes the entire Web site, and only to a “Qualified Buyer” — an entity that is in a related market and that expressly agrees to be Toysmart’s successor-in-interest as to the customer information.

The Qualified Buyer must abide by the terms of the Toysmart privacy statement. If the buyer wishes to make changes to that policy, it must follow certain procedures to protect consumers. It may not change how the information previously collected by Toysmart is used, unless it provides notice to consumers and obtains their affirmative consent (“opt-in”) to the new uses.

In the event that the Bankruptcy Court does not approve the sale of the customer information to a Qualified Buyer or a plan of reorganization within the next year, Toysmart must delete or destroy all customer information. In the interim, Toysmart is obligated to abide by its privacy statement.

After the Bankruptcy Order is approved, the FTC will also file a stipulated consent agreement and final order before the U.S. District Court, Massachusetts (“District Court Order”), enjoining the unlawful practices alleged in the Complaint, prohibiting Toysmart from making any false or misleading statements about the disclosure of personal information to third parties, and prohibiting Toysmart from disclosing, selling, or offering for sale to any third party any customer information, except as provided for in the Bankruptcy Order.36

VI. STATE CONSUMER PRIVACY LAWS: LOCAL LEGISLATION, WIDE-RANGING IMPACT

Even as the federal government has declined to enact general legislation mandating the publication and form of digital privacy disclosures, states have stepped up to do so. While the jurisdiction of state law is limited to a state’s borders by the so-called negative or dormant Commerce Clause of the U.S. Constitution, which understands as exclusive Congress “[p]ower . . . to regulate [c]ommerce with foreign [n]ations, and among the several [s]tates, and with the Indian [t]ribes . . . .,”37 the essentially borderless nature of the Internet, and the intertwined nature of modern business, mean that almost any state’s enforcement power may potentially stretch to a company located in another state.38

38 The cross-border nature of the Internet, and its potential extension of state law enforcement beyond the state’s borders, can be seen in the growth of so-called “Amazon tax” legislation in a number of states,
One significant example of a state privacy law with interstate influence is California's Online Privacy Protection Act of 2003, which specifically mandates disclosure of online data collection and use practices affecting California residents:

**Cal. Bus. & Prof. Code § 22575. Commercial Web site operators; posting of privacy policy; violation of subdivision for failure to post policy; policy requirements**

(a) An 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, or in the case of an operator of an online service, make that policy available in accordance with paragraph (5) of subdivision (b) of Section 22577. An operator shall be in violation of this subdivision only if the operator fails to post its policy within 30 days after being notified of noncompliance.

starting with New York. Following the U.S. Supreme Court's guidance in *Quill Corp. v. North Dakota*, 504 U.S. 298 (1992) and related cases, states have been limited under the Commerce Clause in their power to levy sales taxes to those transactions where the seller maintains a “substantial nexus,” a significant presence, in the state. This presence has been understood to include elements such as physical offices and/or employees, including sales personnel, based in the state. In recent years, given the resurgence of mail order online sales as a major stream of commerce (and the resulting loss of easily collectible sales taxes from the local retailers whose potential customers may be shopping online instead), states are attempting to extend the definition of “nexus” to include some Internet-based sales. One popular method of doing so is via a focus on the commission-based referral methods known as “affiliate programs,” through which independent Web site publishers can refer potential customers to an online retailer through unique Web links, and receive commissions if the referrals result in sales. See, e.g., *Affiliate Marketing Definition*. Employment of this new approach has been met with both applause and criticism. While some have argued that the approach is fair and increases state tax revenue, others have raised concerns about the potential for abuse and the potential for states to gain unfair competitive advantage. As a result, the courts have been called upon to weigh the benefits of the new approach against the potential for abuse and the potential for states to gain unfair competitive advantage. The courts have struck a balance, recognizing the potential for abuse but also recognizing the potential for the approach to increase state tax revenue and provide benefits to consumers. See, e.g., *New York Affiliate Tax Complicates Affiliate Marketing Programs — Mobile Marketer — Columns* (Aug. 18, 2008), http://www.mobilemarketer.com/cms/opinion/columns/1547.html (last visited May 7, 2012); Jonathan I. Ezor, *Split Decision in Appeal of NY “Amazon Tax” Case | New York Advertising Attorneys Blog* (Nov. 5, 2010), http://www.advertisinglawblog.com/2010/11/split-decision-in-appeal-of-ny-amazon-tax-case.shtml (last visited May 7, 2012).


40 § 22577(b) states,

(b) The term “conspicuously post” with respect to a privacy policy shall include posting the privacy policy through any of the following:

(1) A Web page on which the actual privacy policy is posted if the Web page is the homepage or first significant page after entering the Web site.

(2) An icon that hyperlinks to a Web page on which the actual privacy policy is posted, if the icon is located on the homepage or the first significant page after entering the Web site, and if the icon contains the word “privacy.” The icon shall also use a color that contrasts with the background color of the Web page or is otherwise distinguishable.
(b) The privacy policy required by subdivision (a) shall do all of the following:

(1) Identify the categories of personally identifiable information that the operator collects through the Web site or online service about individual consumers who use or visit its commercial Web site or online service and the categories of third-party persons or entities with whom the operator may share that personally identifiable information.

(2) If the operator maintains a process for an individual consumer who uses or visits its commercial Web site or online service to review and request changes to any of his or her personally identifiable information that is collected through the Web site or online service, provide a description of that process.

(3) Describe the process by which the operator notifies consumers who use or visit its commercial Web site or online service of material changes to the operator's privacy policy for that Web site or online service.

(4) Identify its effective date.

California further protects its citizens' data privacy rights through its so-called "Shine the Light" law, most notably its mandated notice of consumer access to information about data sharing with marketers:

**Excerpt from Cal. Civ. Code § 1798.83: Personal Information; Disclosure to Direct Marketers**

(a) . . . . [I]f a business has an established business relationship with a customer and has within the immediately preceding calendar year disclosed personal information that corresponds to any of the categories of personal information set forth in paragraph (6) of subdivision (e) to third parties, and if the business knows or

---

(3) A text link that hyperlinks to a Web page on which the actual privacy policy is posted, if the text link is located on the homepage or first significant page after entering the Web site, and if the text link does one of the following:

(A) Includes the word “privacy.”

(B) Is written in capital letters equal to or greater in size than the surrounding text.

(C) Is written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language.

(4) Any other functional hyperlink that is so displayed that a reasonable person would notice it.

(5) In the case of an online service, any other reasonably accessible means of making the privacy policy available for consumers of the online service.

---

The categories include:

(i) Name and address.

(ii) Electronic mail address.

(iii) Age or date of birth.

(iv) Names of children.

(v) Electronic mail or other addresses of children.

(vi) Number of children.

(vii) The age or gender of children.

(viii) Height.
reasonably should know that the third parties used the personal information for the third parties’ direct marketing purposes, that business shall, after the receipt of a written or electronic mail request, or, if the business chooses to receive requests by toll-free telephone or facsimile numbers, a telephone or facsimile request from the customer, provide all of the following information to the customer free of charge:

(1) In writing or by electronic mail, a list of the categories set forth in paragraph (6) of subdivision (e) that correspond to the personal information disclosed by the business to third parties for the third parties’ direct marketing purposes during the immediately preceding calendar year.

(2) In writing or by electronic mail, the names and addresses of all of the third parties that received personal information from the business for the third parties’ direct marketing purposes during the preceding calendar year and, if the nature of the third parties’ business cannot reasonably be determined from the third parties’ name, examples of the products or services marketed, if known to the business, sufficient to give the customer a reasonable indication of the nature of the third parties’ business.

(b)(1) A business required to comply with this section shall designate a mailing address, electronic mail address, or, if the business chooses to receive requests by telephone or facsimile, a toll-free telephone or facsimile number, to which customers may deliver requests pursuant to subdivision (a). A business required to comply with this section shall, at its election, do at least one of the following:

(A) Notify all agents and managers who directly supervise employees who regularly have contact with customers of the designated addresses or numbers or the means to obtain those addresses or numbers and instruct those employees that customers who inquire about the business’s privacy practices or the business’s compliance with this section shall be informed of the designated addresses or numbers or the means to obtain the addresses or numbers.

(ix) Weight.
(x) Race.
(xi) Religion.
(xii) Occupation.
(xiii) Telephone number.
(xiv) Education.
(xv) Political party affiliation.
(xvi) Medical condition.
(xvii) Drugs, therapies, or medical products or equipment used.
(xviii) The kind of product the customer purchased, leased, or rented.
(xix) Real property purchased, leased, or rented.
(xx) The kind of service provided.
(xxi) Social security number.
(xxii) Bank account number.
(xxiii) Credit card number.
(xxiv) Debit card number.
(xxv) Bank or investment account, debit card, or credit card balance.
(xxvi) Payment history.
(xxvii) Information pertaining to the customer’s creditworthiness, assets, income, or liabilities.

(B) Add to the home page of its Web site a link either to a page titled “Your Privacy Rights” or add the words “Your Privacy Rights” to the home page’s link to the business’s privacy policy. If the business elects to add the words “Your Privacy Rights” to the link to the business’s privacy policy, the words “Your Privacy Rights” shall be in the same style and size as the link to the business’s privacy policy. If the business does not display a link to its privacy policy on the home page of its Web site, or does not have a privacy policy, the words “Your Privacy Rights” shall be written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language. The first page of the link shall describe a customer’s rights pursuant to this section and shall provide the designated mailing address, e-mail address, as required, or toll-free telephone number or facsimile number, as appropriate. If the business elects to add the words “Your California Privacy Rights” to the home page’s link to the business’s privacy policy in a manner that complies with this subdivision, and the first page of the link describes a customer’s rights pursuant to this section, and provides the designated mailing address, electronic mailing address, as required, or toll-free telephone or facsimile number, as appropriate, the business need not respond to requests that are not received at one of the designated addresses or numbers.

(C) Make the designated addresses or numbers, or means to obtain the designated addresses or numbers, readily available upon request of a customer at every place of business in California where the business or its agents regularly have contact with customers.

The response to a request pursuant to this section received at one of the designated addresses or numbers shall be provided within 30 days. Requests received by the business at other than one of the designated addresses or numbers shall be provided within a reasonable period, in light of the circumstances related to how the request was received, but not to exceed 150 days from the date received. 42

Note that while the definition of “Customer” used here is limited to California residents, 43 the word “business” in this section includes companies both within and outside the state:

“Business” means a 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. The term includes an entity that disposes of records. 44

43 “ ‘Customer’ means an individual who is a resident of California who provides personal information to a business during the creation of, or throughout the duration of, an established business relationship if the business relationship is primarily for personal, family, or household purposes.” Cal. Civ. Code § 1798.83(e)(1) (2006).
44 Id. § 1798.80(a).
As one measurement of the actual impact of California’s statute on companies located beyond its borders, a Google search for the phrase “Your California Privacy Rights,” one of the required headings for the marketing disclosure, yields literally millions of results, including the privacy policies for explicitly non-California businesses such as WTVY, a television station in Dothan, AL whose parent company, Gray Television, Inc., is based in Albany, GA.

Another state which has enacted its own privacy policy-related statute is Pennsylvania. In contrast to the affirmative disclosure obligation imposed by California, Pennsylvania includes within its definition of “deceptive or fraudulent business practices” a situation in which a person “knowingly makes a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public.” Such a provision clarifies and potentially expands the liability for inaccurate privacy policy statements beyond general consumer protection concerns into the realm of criminal law.

VII. CONCLUSION: BEST PRACTICES START WITH ACCURATE DISCLOSURE

Given that, in the realm of consumer privacy law, the overarching principle is informed consent, best practices in connection with consumer information must incorporate a mechanism for obtaining this consent. In order to do this, though, the company must itself be informed not only about relevant law where applicable, but also the complete path and scope of consumer data it may be collecting, using and sharing. This is not always a simple process, since organizations both large and small, may have different business units each of which has some knowledge of the company’s information practices. Unfortunately, those professionals who are made responsible for drafting and promulgating a company’s privacy policy are often not fully aware of their colleagues within the organization (or, if the policy is being drafted by outside counsel all of personnel within the client organization) who “touch” consumer data. It’s therefore critical both for effective policy drafting and in preparation for defending any enforcement action claiming any improper information use that the people in charge of creating the consumer information document known as a privacy policy collect the relevant information about company process in an organized, detailed fashion.

One useful tool in this process is a questionnaire. A properly drafted questionnaire will list the full range of relevant issues for privacy policies encompassing not only the type and channels of collection for consumer information but also general corporate details that may be of relevance in both the disclosure and in identifying and managing privacy risks. For example, the location of any out of state or foreign offices in which

company employees or strategic partners may exist is extremely relevant for consumer privacy management given the broad range of diverse often contradictory privacy laws and regulations to which a multijurisdictional organization may be subject. Understanding the off-line process as to how consumers connect with the company (e.g., through faxes, telephone calls, postal letters, etc.) will inform the policy’s disclosure of consumer information collection. Knowing of other business units, whose operations may nominally be separate from that for which the policy is being drafted, will help the professional crafting the policy to determine if there are more sensitive areas of law that could, in the future, become relevant if information will be shared with those other business units. Finally, asking about the organization’s membership and trade associations and any existing enforcement (whether privacy related or not) may raise questions about consent orders, self-enforcement policies, and other matters with which the IT professionals within the organization may not be immediately familiar.

Another benefit of a question-based process for drafting consumer disclosure is that it enables research. An attorney discussing privacy policies with a client may ask all of the right questions, but that particular individual may not have all of the answers immediately at hand. With a questionnaire, though, all of the relevant personnel within the company can be given a chance to do all of the relevant research to track down a more complete set of answers to the questions. The questionnaire will further sensitize those in the company who answer it to the kinds of potential pitfalls that arise in the context of consumer privacy, such as those described in this chapter.

Once the questionnaire has been fully answered, any uncertainties addressed and the drafter made aware of the current practices of the organization with regard to consumer information, the process can go much more smoothly. However, there are both strategic and risk-related considerations that arise in the choice of language and provision in the privacy policy itself beyond merely accurate reflection of the company’s practices. One is flexibility. A well considered privacy policy will not merely disclose the company’s current data uses, but will provide sufficient flexibility so that some future uses, which may not yet be contemplated by the company, will fall within the privacy policy without the language having to be revised.
Chapter 3

SOCIAL MEDIA PRIVACY: NOT (NECESSARILY) AN OXYMORON

Social media (and the similar term “social networks”) are not a new concept either in the analog or digital world. At their heart, social media are many where members of a community can express themselves, and respond to others’ statements, whether one at a time or as part of a group. Subway trains and overpasses covered with different taggers’ graffiti and the stereotypical public bathroom wall are (perhaps extreme) examples of offline social media. Party lines (telephone lines shared by more than one household, before individual lines became available and affordable), single-line college dorm suites, and pay-per-minute “chat lines” (often with sexually explicit conversations) were social media as well, using the telephone wires as their conduit. While television production and distribution costs made social television unfeasible (most individuals did not and could not build their own television stations), the lower cost and greater accessibility of radio meant that communities could develop using that medium: ham operators would chat worldwide via voice or even Morse code, while citizen band radios became popular for conversations among both truck drivers and others in the 1970s and early 1980s.

On the Internet, social media have formed a major part of the framework since the earliest days. Network users could send each other short text messages via UNIX “write” or “talk” commands,¹ Usenet hosted message boards on thousands of different topics, Internet Relay Chat (“IRC”) servers across the Internet enabled real-time, multi-user chat, and Internet-based multi-user dungeons (“MUDs”) combined text-based virtual “worlds” with live interaction among players through the characters whose actions they controlled (known as avatars). Similar socially driven programs ran on private dial-up bulletin board systems (BBSes) and proprietary online systems like GEnie, Prodigy, and CompuServe. These communities, while at times incredibly vibrant and ongoing, were accessed by a tiny fraction of society, mainly technologists, hobbyists, and those in university communities which provided Internet access to some or all students.

Beginning in the early-to-mid ‘90s, and especially since the turn of the millennium, Internet-based social networks have expanded in numbers and market penetration. As the skills needed to access social networks lessened, and the user base diversified, hundreds of millions of people around the world have become regular users of social networks from the earlier MySpace to Facebook, Twitter, LinkedIn and many more. In doing so, they have joined a culture of relationships and sharing that raises

significant and diverse privacy issues, in terms of what information is shared, by whom, with whom, and how it can be accessed. Some of these issues are under control of the person to whom the information pertains, but most may not be. Service providers, other users, and third parties may have control, and resulting legal obligations, with regard to the personal and behavioral information relating to social media services, in addition to the other laws and regulations that generally cover digitally stored private information.

I. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT: THE KEY FEDERAL STATUTE

The Electronic Communications Privacy Act (“ECPA”) is the major federal statute which determines whether and how social media posts and data about them may be shared, at least to the extent that the issue involves something that falls under one of the statutory definition of electronic communications to which the statute applies:

“electronic communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include —

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds . . . .

Assuming it does, the next question to be answered is whether the requesting party, the disclosing party, or both are considered governmental actors: police or other law enforcement officials, public education facilities, government agencies, etc. If so, the provisions of ECPA that apply to governmental acts apply. Otherwise, one looks to those requirements and restrictions for private entities and individuals.

Two more key distinctions under ECPA are (1) whether the information being collected and sought is from the content or other portions of the communications, and (2) whether the disclosure is of communications as they are being sent or of stored communications after the fact. Depending on the answer to these two questions, different portions of ECPA may apply:

---

Further, ECPA distinguishes between two types of service providers: an electronic communications service ("ECS") and a remote computing service ("RCS"). Each has its own unique requirements and restrictions in terms of what information it may disclose, under what circumstances, to whom, and the documentation required to authorize the disclosure.

II. SOCIAL MEDIA SHARING: THE FOUR WS

Perhaps the most surprising element of social media from a privacy perspective is the sheer scope of how much and what types of information can be obtained from and about users. It may be helpful to frame the discussion via a concept borrowed from journalism: the five Ws and an H. Reporters are trained to answer six crucial questions in a story: "who," "what," "where," "when," "why," and "how." While "why" and "how" are not specifically privacy-related, the other four W questions are precisely on point.

a. Who: Identity, Anonymity and Pseudonymity Online

From the earliest days of online communities, users were given a choice that they rarely had in most off-line, real-world contexts: whether to use their real identities, remain anonymous, or take the middle ground of creating and using a pseudonym. Certainly, anonymity was actually possible in real-world interactions, but it required hiding one's face and voice; so did taking on a pseudonym. While fiction was full of successful anonymous or pseudonymous interactions (e.g., the superhero's "secret identity" or Alexander Dumas' "Man in the Iron Mask"), there were few real life situations where an individual could not be quickly and easily identified. By contrast, online communities very quickly provided identifiers that could be different from one's real name. E-mail addresses or network logins could technologically use words other than the user's identity, with limits only in available characters or the policy of the network owners. As networks offered more sophisticated, software-based games, chat

---

6 "[E]lectronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications." Id. § 2510(12).
7 "[T]he term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).
rooms, and message boards, the opportunities to create or hide one's true name expanded. At a whim, or perhaps for more nefarious reasons, a user could utilize a different name, age, gender, or even species, limited only by the programming of the particular software being run and/or rules and policies created by the community itself.

Excerpt from “A Rape in Cyberspace” by Julian Dibbell

The facts begin (as they often do) with a time and a place. The time was a Monday night in March, and the place, as I’ve said, was the living room — which, due largely to the centrality of its location and to a certain warmth of decor, is so invariably packed with chitchatters as to be roughly synonymous among LambdaMOOers with a party. So strong, indeed, is the sense of convivial common ground invested in the living room that a cruel mind could hardly imagine a better place in which to stage a violation of LambdaMOO’s communal spirit. And there was cruelty enough lurking in the appearance Mr. Bungle presented to the virtual world — he was at the time a fat, oleaginous, Bisquick-faced clown dressed in cum-stained harlequin garb and girdled with a mistletoe-and-hemlock belt whose buckle bore the quaint inscription KISS ME UNDER THIS, BITCH! But whether cruelty motivated his choice of crime scene is not among the established facts of the case. It is a fact only that he did choose the living room.

The remaining facts tell us a bit more about the inner world of Mr. Bungle, though only perhaps that it wasn’t a very cozy place. They tell us that he commenced his assault entirely unprovoked, at or about 10 p.m. Pacific Standard Time. That he began by using his voodoo doll to force one of the room’s occupants to sexually service him in a variety of more or less conventional ways. That this victim was exu, a Haitian trickster spirit of indeterminate gender, brown-skinned and wearing an expensive pearl gray suit, top hat, and dark glasses. That exu heaped vicious imprecations on him all the while and that he was soon ejected bodily from the room. That he hid himself away then in his private chambers somewhere on the mansion grounds and continued the attacks without interruption, since the voodoo doll worked just as well at a distance as in proximity. That he turned his attentions now to Moondreamer, a rather pointedly nondescript female character, tall, stout, and brown-haired, forcing her into unwanted liaisons with other individuals present in the room, among them exu, Kropotkin (the well-known radical), and Snugberry (the squirrel). That his actions grew progressively violent. That he made exu eat his/her own pubic hair. That he caused Moondreamer to violate herself with a piece of kitchen cutlery. That his distant laughter echoed evilly in the living room with every successive outrage. That he could not be stopped until at last someone summoned Iggy, a wise and trusted old-timer who brought with him a gun of near wizardly powers, a gun that didn’t kill but enveloped its targets in a cage impermeable even to a voodoo doll’s powers. That Iggy fired this gun at Mr. Bungle, thwarting the doll at last and silencing the evil, distant laughter.

These particulars, as I said, are unambiguous. But they are far from simple, for the simple reason that every set of facts in virtual reality (or VR, as the locals abbreviate it) is shadowed by a second, complicating set: the “real-life” facts. And while a certain
tension invariably buzzes in the gap between the hard, prosaic RL facts and their more fluid, dreamy VR counterparts, the dissonance in the Bungle case is striking. No hideous clowns or trickster spirits appear in the RL version of the incident, no voodoo dolls or wizard guns, indeed no rape at all as any RL court of law has yet defined it. The actors in the drama were university students for the most part, and they sat rather undramatically before computer screens the entire time, their only actions a spidery flitting of fingers across standard QWERTY keyboards. No bodies touched. Whatever physical interaction occurred consisted of a mingling of electronic signals sent from sites spread out between New York City and Melbourne, Australia. Those signals met in LambdaMOO, certainly, just as the hideous clown and the living room party did, but what was LambdaMOO after all? Not an enchanted mansion or anything of the sort — just a middlingly complex database, maintained for experimental purposes inside a Xerox Corporation research computer in Palo Alto and open to public access via the Internet.

To be more precise about it, LambdaMOO was a MUD. Or to be yet more precise, it was a subspecies of MUD known as a MOO, which is short for “MUD, Object-Oriented.” All of which means that it was a kind of database especially designed to give users the vivid impression of moving through a physical space that in reality exists only as words filed away on a hard drive. When users dial into LambdaMOO, for instance, the program immediately presents them with a brief textual description of one of the rooms of the database’s fictional mansion (the coat closet, say). If the user wants to leave this room, she can enter a command to move in a particular direction and the database will replace the original description with a new one corresponding to the room located in the direction she chose. When the new description scrolls across the user’s screen it lists not only the fixed features of the room but all its contents at that moment — including things (tools, toys, weapons) and other users (each represented as a “character” over which the user has sole control).

As far as the database program is concerned, all of these entities — rooms, things, characters — are just different subprograms that the program allows to interact according to rules very roughly mimicking the laws of the physical world. Characters may not leave a room in a given direction, for instance, unless the room subprogram contains an “exit” at that compass point. And if a character “says” or “does” something (as directed by its user-owner via the say or the emote command), then only the users whose characters are also located in that room will see the output describing the statement or action. Aside from such basic constraints, however, LambdaMOOers are allowed a broad freedom to create — they can describe their characters any way they like, they can make rooms of their own and decorate them to taste, and they can build new objects almost at will. The combination of all this busy user activity with the hard physics of the database can certainly induce a lucid illusion of presence — but when all is said and done the only thing you really see when you visit LambdaMOO is a kind of slow-crawling script, lines of dialogue and stage direction creeping steadily up your computer screen . . . .

From a practical perspective, the anonymity or pseudonymity of a particular user can be limited by a number of factors. First, of course, is whether the user (accurately) discloses her true identity within the online community, either intentionally or otherwise. As was pointed out earlier in the book, identity can be effectively disclosed through combination of facts that individually do not serve as identifiers. Even if the user member never explicitly mentions her name, address, or other typical pieces of personally identifiable information, others within the community can “put the pieces together” and figure out the user’s actual identity.

Human nature can also play a part in de-anonymizing social media users. Often, a user may use the same word or phrase, by itself or in connection with a meaningful number such as an age or birth date, as his user name for multiple communities or services. If so, the fact that the user hid his identity on one message board may be meaningless, if a quick search of his “pseudonym” turns up another site or service where his personal identity is more easily found. The more unique the chosen identifier, especially in combination with other information provided by the user, the greater the chance of such discovery, as occurred when the Wikileaks mass information release was traced to intelligence specialist Bradley Manning, born in 1987, who used the online name “Bradass87” while discussing his occupation and position:

**Excerpt from “Afghanistan War Logs: Story Behind Biggest Leak in Intelligence History”**

... On 21 May, a Californian computer hacker called Adrian Lamo was contacted by somebody with the online name Bradass87 who started to swap instant messages with him. He was immediately extraordinarily open: “hi . . . how are you? . . . im an army intelligence analyst, deployed to eastern bagdad . . . if you had unprecedented access to classified networks, 14 hours a day, 7 days a week for 8+ months, what would you do?”

For five days, Bradass87 opened his heart to Lamo ... On 26 May, at US Forward Operating Base Hammer, 25 miles outside Baghdad, a 22-year-old intelligence analyst named Bradley Manning was arrested, shipped across the border to Kuwait and locked up in a military prison ...

Whatever other users may discover about an anonymous or pseudonymous user, though, identifying information is almost certainly known by (and potentially obtainable from) various service providers, at least from a technical perspective. First, to the extent the particular social medium requires registration before use, the user may have had to provide a verifiable real identity and/or payment information to the service host. Even if the service provider did not require pre-registration, or was given false

---

9 See discussion at Chapter One, note 20.

information, one piece of data is embedded in every communication sent via the
Internet, including through social networking communities: the IP address of the
sender. The service host can associate a unique IP address with every message, and
that IP address will in turn be assigned to a unique individual or account at that
particular date and time by the ISP or network owner from whose blocks of addresses
that specific one comes. While an IP address cannot by itself identify a person, it can
be traced to an account, a device, or other unique location to which a limited number
of people may have access.

At times, the IP address’ use and ownership is publicly accessible: in August 2007,
Wired Magazine wrote of tracing the IP address used to excise negative information
about Diebold voting machines from a Wikipedia article to an IP address registered to
Diebold itself.11 In that instance, the IP address itself was shown on Wikipedia, and its
ownership was searchable via the Arin.net Web site. Similar methods, along with a
broader analysis of geography and similar word choices, helped bloggers identify the
so-called “Fake Steve Jobs” as reported by The New York Times the same month.12
While technologies do exist to enable IP address hiding, spoofing and other conceal-
ment techniques,13 the vast majority of Internet users connect without such methods
and via traceable IP addresses.

When social media or other communications, or the information about by whom and
when they were sent, are not publicly viewable, however, relevant statutory and case
law along with internal policies may determine whether and how the service providers
with the information may share it.

Beyond the formal legal prohibitions and requirements for disclosure, the service
provider’s own internal and published policies will have an impact. Internally, the
service provider must initially decide whether it will be collecting, and verifying, user
information; such a decision will be driven both by relevant law and the interests of the
desired membership and the provider itself. In some contexts, a service provider may
be required to collect and archive user information and communications because of its
industry or the type of discussions that occur.14 In others, as with COPPA,15 the
service provider may be discouraged from collecting user identity information because
of the substantial requirements for such collection.

Other concerns such as marketing and reputation come into play as well in the
establishment of a service provider’s internal policies. Some services require users to
publicly utilize their actual names, and may even verify them, to provide accountability
and retain a decorum in the discussions.16 Others will verify only some users, such as

11 John Borland, See Who’s Editing Wikipedia - Diebold, the CIA, a Campaign, W IRED (Aug. 14, 2007),
2007/08/05/the-trial-of-fake-steve-jobs/ (last visited May 7, 2012).
14 See, e.g., 17 CFR § 240.17a-4(b)(4) (SEC retention requirements for broker-dealers).
15 See discussion on COPPA in Chapter 4: The Special Case of Children.
16 Google’s Google Plus service requires that members use real rather than fanciful names: “To help fight
spam and prevent fake profiles, use the name your friends, family or co-workers usually call you. For
celebrities, to reduce the risk that imposters may take famous names and fool other users. Intermediaries like auction, payment, and dating sites may enable public pseudonymity, but will retain and utilize verified personal information to facilitate and improve the reliability of the desired transaction or introductions.

By contrast, there are service providers which seek to enable anonymity for their users, for a variety of reasons including but not limited to:

- Providing a forum for unpopular or dissident political discussions;
- Performing or supporting illegal activity;
- Granting access to socially sensitive content (e.g., sexually explicit discussions or materials); and
- Otherwise giving those who fear reprisal or danger from disclosing their identities a tool for communicating without risking doing so.

If providers wish to offer true anonymity, they must consider both technical and legal issues. Technically, even if the provider does not itself request or retain other identifying information, it may still be logging IP addresses which can be obtained and utilized by authorities or others to identify the otherwise anonymous service users, as occurred in 1995 to the well-known and relied-upon anon.pen.et.fi automated remailer:

EXCERPTED FROM THE CUTTING EDGE: The Helsinki Incident and the Right to Anonymity BY DANIEL AKST

... Anon.pen.et.fi is basically a computer in Helsinki, Finland, whose purpose is to allow e-mail users all over the world to send anonymous messages, both to individuals as private e-mail and to Internet newsgroups, as the Net's 10,000-plus discussion forums are known. You message anon.pen.et.fi and it strips off your identity, substituting a code number. Responses at your anon.pen.et.fi address get routed back to you. There are many “anonymous remailers” like anon.pen.et.fi, but probably none is as stable or widely used. Its operator, a selfless computer networking specialist named Johan (Julf) Helsingius, supports the server to the tune of $1,000 a month and has developed a reputation for integrity. Helsingius has rules: He won't disclose the name behind an anonymous ID, but every message explains how to send him complaints. Abuse anon.pen.et.fi and you'll probably find yourself locked out of the system. During previous incidents in which he was pressured to disclose the identity of a user, Helsingius stood firm. Then the inevitable happened: He was faced with a search warrant served by Finnish police ...
As the anon.penet.fi incident shows, a social network or other service may be legally obligated to disclose personal information it retains, whether or not it promises anonymity. This highlights a second potential area of legal exposure: the promise itself. Just as sites generally may be held liable under consumer protection laws for unkept promises or other misstatements in their privacy policies, a service that promises unlimited anonymity but is required to disclose could face civil exposure from its no-longer anonymous members. In this context, as with privacy policies generally, it’s important to include exceptions to any commitment to protect identities. Alternatively, the service may choose not to preserve logs of IP addresses (assuming it is otherwise not legally required to do so), so that it cannot disclose them because it does not actually have them. While this does enhance its ability to detect identities, it removes the service’s ability to identify and seek redress from users who abuse or damage the service itself. Further, while the service may decline to keep logs, its real-time connections could be tapped to obtain IP addresses as the communications are made.

b. What: Content as Disclosure

The informality of social media, along with potentially confusing settings from various social media services regarding who can or cannot see a particular user’s postings, can result in content being posted that is at best embarrassing, and at worst may violate legal obligations such as confidentiality requirements, whether contractual or arising out of a particular industry’s requirements.19

From an inbound information collection perspective, companies that are covered by statutory or regulatory obligations discussed elsewhere in this volume (for example, COPPA for information collection from children, HIPAA for health-related businesses, and the various requirements for financial service providers) may not be exempt from those rules merely because the channel through which they are collecting personal information is a social network rather than their own Web sites or other internal resources. Similarly, if the organization is prohibited from or faces restrictions on its disclosing of personal information, those restrictions may or will include disclosure via social media. Unfortunately, customers who are not covered by the same restrictions may be able to tweet or post about the company, even falsehoods that might damage the company’s reputation, with the only available response being a costly and uncertain defamation lawsuit.

Some industries and professions face formal confidentiality obligations beyond those arising of privacy regulations. Attorneys, for example, are required by the ethical rules of the state(s) in which they are admitted to practice to maintain client confidences,20 which is as true of social media posts as casual conversations in elevators and other public places:

Note that the obligation for attorneys goes beyond information that may be generally thought of as personal identifiable information or even confidential information, to encompass all “information relating to the representation of a client.”

---

19 See, e.g., discussions of health privacy in Chapter 5; financial privacy in Chapter 6; and the ethical obligations of confidentiality for attorneys in Chapter 11.

20 See discussion of attorney confidentiality obligations at Chapter 11, note 1.
This broad requirement can be breached not only through express revelations, but through implicit ones as well. For example, a corporate attorney from New York City who checks in on Foursquare at a hotel in Bentonville, Arkansas (well-known as the home of Walmart’s corporate headquarters) could effectively be disclosing that her client has some business or other relationship with Walmart, even if that information is not otherwise public. Consider as well the actual litigator who tweeted that he was in a settlement meeting at his opponent’s office. While this might seem a casual message rather than an ethical breach, this is not so clear. Although the attorney did not name either the case or the opposing attorney, and regardless of the fact that the existence of settlement discussions is inadmissible, a juror from the case who was following that attorney (as many non-sequestered jurors are now in the habit of doing) would be made aware that settlements were being discussed (or might believe so, even though the attorney could have been discussing settling a different case) and could share that information with other jurors or otherwise allow it to impact on the verdict.

A further privacy-related legal issue for businesses is the confidentiality obligations they may face based upon their contractual relationships. Companies can all too easily violate a non-disclosure provision or agreement regarding a business relationship or even the name of the contracting parties through an injudicious tweet or blog posting, especially if the employee who tweets is not aware of the obligation in the first place. When Apple was preparing to launch its first-generation iPad in February 2010, it showed pre-release units to technology journalists under strict non-disclosure obligations. A deputy managing editor for The Wall Street Journal tweeted during such a meeting that he was using the iPad; the tweet later was deleted, but was later reported by BusinessWeek. At times, social media can facilitate unauthorized disclosure even when the posting doesn’t contain any obvious information, confidential or otherwise, solely due to how various technologies function. In one instance, a well-known technology blogger inadvertently leaked the not-yet-public 5 megapixel camera resolution of the pre-release Palm Pre 2 smartphone he was apparently given to test, when he posted his photo of an old stereo system via the photo-sharing service img.ly. While the contents and caption of the photo (“Vintage from the 90s. I’m old.”) were unremarkable, the photo’s digital file contained standardized EXIF (Exchangeable Image File Format) information clearly indicated that it had a resolution of 2576 x 1928 pixels (that is, 5 megapixels) and that it was taken with a “Palm Pre.” Since no then-available Palm Pre phone had a 5 megapixel camera, the blogger had inadvertently disclosed a specification upgrade that the company itself had not yet confirmed, merely by posting a photo to a social media service.

Even if the revelation of information does not violate laws or contracts, it can still be detrimental to the business, whether due to embarrassment or loss of competitive

21 See, e.g., Fed R. Evid. 408.
advantage.

*From “A Twitter Code of Conduct” by Douglas MacMillan*

During a recent tour of interactive ad agency Toquigny’s Austin (Tex.) headquarters, Chief Executive Yvonne Toquigny was confronted by her guest, an executive from a large energy company who was a potential client. The visitor had recently learned that Toquigny was wooing one of his company’s competitors — by seeing a message that one of Toquigny’s employees had posted to Twitter “It took me by surprise,” says Toquigny. “I realized that we needed to be more cautious about what we throw out there in to the universe . . .”

Twitter can be a great business tool. But as use of the Web site for 140-character messages spreads to workplaces around the world, companies are also discovering the risks. Now, instead of just worrying about a dubious blog post or an embarrassing photo of the boss being posted to Facebook, employers have to contend with staffers shooting off frequent blasts of personal insight into a public and traceable sphere. “The concept of [workers] posting inappropriate material that could be harmful has been around for a while, but Twitter accelerates the problem because of its immediacy and volume,” says Mark Rasch, a former head of the U.S. Justice Dept.’s computer crime unit who now consults with companies on creating policies to address employees’ use of technology.

To prevent sensitive information leaks, blemishes on a reputation, and other potential liabilities of a Twittering workforce, companies are drafting new employee codes of conduct and educating workers about what they should and shouldn’t say on the site. The basic rule: Don’t be stupid . . .

c. When: Time as a Key Element of Identity

While an IP address may be a unique identifier, it may also be shared among numerous users either sequentially or simultaneously. Either way, in order to specifically identify a user, the investigator will require the *exact* date and time of each relevant communication; that is, to answer the question of when.

This is due to two technical factors. The first is that, because IP addresses in their current format (consisting of four sets of three digits between 0 and 255, separated by periods; e.g., 192.168.1.1) are a large but finite resource, they can be allocated in both dynamic as well as static methods. In a dynamic IP environment, the network operator or service provider maintains a set of IP addresses it controls. As a new user signs into the network or service, the user is assigned an available IP address from the set, and whenever the user signs off the network, that IP address becomes...


available for reuse either by the same or another user upon signon to the network. A dynamic IP address environment is similar to the way telephone numbers are assigned within a particular area code or other geographic region: new customers may be given telephone numbers that could have been used by previous customers who have moved or otherwise discontinued service. In the telephone system, numbers may be kept inactive for some period between assignments to reduce the chance of newer customers receiving calls properly dialed but intended for the previous assignee of the number. For dynamic IP addresses, however, very little time is required between assignments, since the infrastructure of the Internet is not designed to assume that IP addresses will remain fixed, and each communication will include a “lookup” to obtain the latest IP address for the intended recipient.

The second technical matter has to do with how networks route communications. Modern local area networks (“LANs”) will likely utilize the same type of IP address-based communications as the broader Internet. The difference, however, is that while every device communicating with the Internet must have an IP address that is unique throughout the world, locally connected devices will be issued internal IP addresses that must only be unique within the local network, but could be identical to those assigned to any number of devices connected to other local networks, just as numerous corporate telephone systems could use the same set of numbers for their internal extensions without conflicting with each other.

In order for internal networked computers to communicate with the Internet, however, the network must provide a router, a device which will redirect Internet-bound communications from internal machines out to the Internet, and then receive and distribute any replies back to the internal machines to which the replies are being sent. In order for this to work properly, the router will be assigned a single public IP address, which will be associated with every communication and request from every user coming from that router’s internal network, just as the caller ID from callers within a corporation may be reported as the main number of the corporation, since the internal corporate telephone system routes outbound calls from its local extensions through its available public lines.

As with dynamic IP addresses, an exact date and time is needed in order to identify the particular user from which a communication utilizing a router’s public IP address has come. With those data, the network’s administrator may be able to trace the communication back to the specific internal network user who connected to the Internet through the router at that moment. Given how many internal users may be sharing the router, however, this identification can be more difficult than simply associating a dynamic IP address with its then-current assignee. Without the time information, though, it can be almost impossible absent additional evidence to identify a user behind a shared router’s public IP address.

Even if one has the date and time a particular IP address was used, that will not necessarily lead to positive identification. First, one must be sure that the clocks of the sending and receiving networks are identical; if not, it is vital to correct for any discrepancies, since failing to do so could likely lead to inaccurate identification. Second, even when the network operator is provided with the correct information, it could report back inaccurate identification, leading to embarrassment or worse.
From “Faulty IP address data leads to Shaq attack on innocent family”

Anyone who follows the slate of lawsuits against music fans is cognizant of the crucial role that IP addresses play in attempts to cow suspected file sharers. But as we have seen time and time again, IP addresses are not consistently reliable means of identifying users. Law enforcement officials and a family in Gretna, Virginia and learned that lesson the hard way after their home was searched by a law enforcement team that included Miami Heat center Shaquille O’Neal, according to a law enforcement official.

The spectre of an angry, uniform-wearing Shaq, let alone an entire team of deputies and federal marshalls would be enough to turn one’s knees to jelly. That’s the sight apparently witnessed by farmer A.J. Nuckols, his schoolteacher wife, and three children last month when their home was raided and their computers, DVD, video tapes, and other belongings were confiscated after they were connected to an IP address reportedly used to access child pornography on the Internet.

It turned out to be a case of mistaken identity. Nine days after the raid, an investigator told Nuckols that “the wrong IP address had been identified” and that he and his family would not be charged in the investigation . . . .

One more caveat about obtaining identity via social media: at best, the unique identifiers used (IP addresses, account names, etc.) can be connected to an account or specific computer or device rather than the specific person using the device or operating the device. Further investigation may be necessary to definitively match the IP address to the human utilizing it, as in legal proceedings with particular evidentiary standards or burdens of proof.

d. Where: Location-Based Information

For most of the history of networked communications, geography was both irrelevant (as long as there was a wire or a signal) and difficult to determine, especially when the communicator wished to hide her location. In the analog world, while the central offices would likely know and could potentially report the physical location of wired telephone lines, each participant in the call might not automatically know where the other caller was located, beyond general information from the telephone number. For example, the old Hotel Pennsylvania in New York City had the telephone number “Pennsylvania 6-5000,” memorialized by the Glenn Miller Orchestra in a song; the “Pennsylvania” in the number (later updated to PE6-5000 and currently in use with the Manhattan 212 area code by the hotel as 212-736-5000) was the telephone exchange of that part of Manhattan, named for the nearby

---


Pennsylvania Railroad Station. Anyone calling Pennsylvania 6-5000, or any number beginning with Pennsylvania, would know the other party was likely in the region of Pennsylvania Station on the West Side of midtown Manhattan. Telephone exchanges (and, once the number of phones in use exceeded the available quantity of telephone numbers, area codes appended to the exchanges) continued to provide rough geographic data about caller location at least until call forwarding and mobile telephones disconnected the caller from a particular place. Today, little can be definitively determined about the physical location of a caller from the telephone number the caller uses; even the country may be unknowable.

With computer networks, the issue of geographical location became even more irrelevant, at least at first. The TCP/IP protocol on which all Internet communication is carried was designed to be tolerant of breaks in the network, by routing messages (actually, by breaking messages into packets of information that would be reassembled at their final destination to once again represent the complete message) via any available connection, no matter the geographical location. While a particular connection might not be the most direct from a physical perspective (i.e., the shortest length of wire), it could be the one that happened to have the least congestion and therefore most availability at the moment a packet needed to be sent. While the initial wires that carried Internet traffic were mainly within the United States (as part of the original ARPAnet), as the network spread and other countries’ internal networks were interconnected through multiple paths, national borders turned porous to network traffic. It was only those countries whose international telecommunications services were routed through a single, controllable connection where Internet traffic could generally be “stopped at the border.” As for the transmitted information itself, it was identified only by a numerical IP address, which theoretically could be assigned to any computer without regard to its physical location; while domain names often included geographic designations (e.g., .uk as a “country code” for systems based in the United Kingdom), IP addresses did not. There were no equivalents of international calling codes, or postal codes, assigned to computers.

As a result, social media services would generally have no inherent knowledge of their members’ geographical location, unless the members provided the information to the services either voluntarily or as a condition for gaining access to the service itself. The most frequent situation in which a service provider would have information about a member’s location (or at least mailing address) was when the service required payment in some way, or the member required or requested physical materials to be sent from the service. Payments made by check or credit card would connect a location to the member account, as would mailing instructions or any correspondence sent by the member to the service for whatever reason.

Paid services, therefore, would need to consider how they would protect the location information as part of their overall privacy policies, where free services had less need to do so (except when the information was volunteered by the member).

---


They could also, however, face potential liability based upon their imputed knowledge of their members’ locations, especially when those locations’ laws were violated by the activities of the service.

From “Virtual Community Standards”

. . . . [I]n the law-enforcement community and in the mainstream press, the prospect of online obscenity is still an eye-grabber. . . . This factor does much to explain the hoopla surrounding the obscenity prosecution of Robert and Carleen Thomas of Milpitas, CA. At first glance, the case may seem little different from the average obscenity prosecution. Sure, there’s a computer bulletin-board system (BBS) involved, but there’s nothing new about prosecuting pornography distributors in conservative states like Tennessee, is there?

Except that this BBS wasn’t in Tennessee. It was in California. But that didn’t stop Tennessee prosecutors from going after it . . . .

More recently, a technology called “geolocation” has made it substantially easier for social media service providers to know (or at least have a strong likelihood of knowing) where a particular user might be. One method of geolocation involves the creation and maintenance of a database matching IP addresses to physical locations based upon a variety of source information (domain name records, ISP and corporate office addresses, and others); once the databases are compiled, they can be queried by website and social media service owners each time a user connects to the service. This can enable the service to provide location-specific content (e.g., advertising for local businesses) or, alternatively, block content which the service may not legally provide in the location in which the user is believed to be. Even when the accuracy of the databases may not be complete, the service provider may nevertheless make decisions about the information they provide.

From “Geo-Location Technologies and Other Means of Placing Borders on the ‘Borderless’ Internet”

If a website operator can know the location of those who access the website, he/she can, due to the reactive nature of Web servers, control what material is presented, and indeed, accessible to each access-seeker: In addition to business advantages, such as targeted advertisement, a structure allowing for geo-identification has the advantage of providing the website operator with the means to comply with local regulations . . . .

A website operator with the ability to determine the geographical location of those who access his/her website would be in a good position to avoid minimum contact being established between him/her and undesirable locations. . . . As long as states apply conflict of laws rules that focus on the location of the effect rather than on the location where the defendant acted, there is a need for website operators to take steps

to limit the geographical spread of their content . . . .

While the currency and accuracy of geolocation databases may vary depending on their source materials and collection methodologies, the expansion of global positioning system ("GPS") technology in cellphones, smartphones, laptops, and other devices enables social networks and other Web sites to receive extremely accurate location information for each user. In fact, a growing number of social media services are either based directly upon or have added supplemental features arising out of GPS-enabled location reporting.

Along with the enhanced scope and accuracy of knowledge of users’ location, social media services are facing increased legal exposure as well, particularly on the privacy front. First, they must disclose whether they know the user’s location and how they use that information, within their general privacy policy. As with all such disclosures, failing to do so, or failing to be accurate in the disclosure, can open up a site to

---


34 As stated in the Executive Summary of the official standard document for the U.S. government’s Global Positioning System,

The U.S. Global Positioning System (GPS) Standard Positioning Service (SPS) consists of space-based positioning, navigation, and timing (PNT) signals delivered free of direct user fees for peaceful civil, commercial, and scientific uses worldwide. This SPS Performance Standard (SPS PS) specifies the levels of SPS performance in terms of broadcast signal parameters and GPS constellation design. The U.S. Government is committed to meeting and exceeding the minimum levels of service specified in this SPS PS and this commitment is codified in U.S. Law (10 U.S.C. 2281(b)).

Since GPS initial operational capability (IOC) in 1993, actual GPS performance has continuously met and exceeded minimum performance levels specified in the SPS PS and users can generally expect improved performance over the minimum levels described here. For example, with current (2007) Signal-in-Space (SIS) accuracy, well designed GPS receivers have been achieving horizontal accuracy of 3 meters or better and vertical accuracy of 5 meters or better 95% of the time. A number of U.S. agencies continually monitor actual GPS SPS performance, including the Federal Aviation Administration (FAA) which publishes quarterly Performance Analysis Reports at its National Satellite Test Bed (NSTB) web site (http://www.faa.gov). Interested readers are encouraged to refer to this and other sources for updated GPS performance.


36 When the social media service Facebook added Facebook Places in August 2010, product manager Michael Eyal Sharon introduced the feature via a blog posting:

If you’re like me, when you find a place you really like, you want to tell your friends you’re there. Maybe it’s a new restaurant, a beautiful hiking trail or an amazing live show.

Starting today, you can immediately tell people about that favorite spot with Facebook Places. You can share where you are and the friends you’re with in real time from your mobile device.

Checking In with Friends

Ever gone to a show only to find out afterward that your friends were there too? With Places, you can discover moments when you and your friends are at the same place at the same time . . .

consumer protection actions.

Next, social media services may be subject to subpoenas and other formal process from law enforcement officials and litigants with regard to the location of particular individuals. This information can be relevant in the context of investigating crimes (whether to find an accused perpetrator or to verify or establish an alibi), in divorce cases (e.g. tracking the location of a spouse accused of having an affair), and in essentially every other situation where the physical whereabouts of an individual social media user may be relevant.

One key question is what type of legal process is required to obtain location information. ECPA distinguishes between content and non-content information, for both in-process and stored communications. Both those seeking the information and those being asked to provide it must be sure that the proper process is used, in order to avoid exposure for improper access or disclosure. While one might assume that location information is non-content and generally subject to lesser requirements and standards for disclosure, this may not be true. Consider that some social networks are based upon sharing location information; for those services, the location could be defined as content whose disclosure would be governed by the more stringent requirements within ECPA, especially for monitoring non-published current and previous “check-ins” or other location reports by users.

One further potential area of exposure, whether legal or otherwise, arises from the consequences of enabling location sharing and disclosure. If, for example, a user is robbed or injured as a result of reporting her location via a social media service, the service itself could theoretically find itself the subject of a liability lawsuit. Even without legal action, though, such incidents could substantially harm the reputation and business prospects of a social media service:

**From “Please Rob Me: The Risks of Online Oversharing”**

*Think before you tweet. You might not be aware of how much information you’re revealing.*

That’s the message from the founders of Please Rob Me, a website launched on Tuesday that illustrates just how easy it is to rob people blind on the basis of the information they’re posting on the Web. The site uses streams of data from Foursquare, an increasingly popular location-based social network that is based on a game-like premise. Players use smart phones or laptops to “check in” to a location, recording their position on a map for friends using the service to see. The more often you check in, the better your chances of being declared the mayor of a particular location, be it a restaurant, bar, office or even your own home.

The problem comes when users also post these locations to Twitter, says Boy van Amstel, one of the founders of Please Rob Me. Then the information becomes publicly available, making it theoretically possible for a robber (or anyone else) to keep tabs on when you say you’re in your home or not.

37 See discussion of ECPA at Chapter 3:1.
“We saw people checking in at their home addresses, or even worse, those of their friends and family,” van Amstel says. “Which we just thought was very wrong.”

Van Amstel is no expert hacker, and Please Rob Me isn’t a complicated website; it’s simply a dressed-up page of Twitter search results that monitors the latest posts of users sharing their locations via Foursquare. And there are a lot of results — thousands of people willingly broadcast when they’re not at home (it’s rarer for users to post to Foursquare when they return). A select, misguided few broadcast their address or those of unknowing and disapproving friends or family. This makes the site more useful at proving a point than an actual tool for robbers to exploit . . .

* * *

From “Facebook ‘Friend’ Suspected in Burglary”

Everyone you consider a “friend” on Facebook, may not have the friendliest intentions. That was the hard lesson homeowners in New Albany, Ind., believe they learned after their home was ransacked by two men.

Keri McMullen and Kurt Pendleton left a status update on Facebook Saturday night that said they wouldn’t be home because they were going to a concert in nearby Louisville at 8 p.m.

At 8:42 p.m., two burglars entered their house, using a screwdriver to force open a back door. However, luckily for McMullen and Pendleton, they had recently installed a surveillance system in their home. The cameras caught the entire episode on tape.

The video shows the two men going through McMullen’s purse, stealing electronics — more than $10,000 worth — including a plasma television right off the wall. The burglars are then seen driving away with a laundry basket filled with the stolen goods.

After posting images of the suspects on Facebook, McMullen realized one of them had “friended” her about six months ago. She says he grew up across the street from her and hasn’t seen him in more than 20 years . . .

III. CONCLUSION: SOCIAL MEDIA PRIVACY: SIGNIFICANT CHALLENGES AND BEST PRACTICES

As the number and adoption of social media services increase, organizations and their advisors must consider how issues of privacy law and policy impact on how they and their affiliates use social media. For companies that host social media services, the primary legal challenges involve customer behavior and personal information (that is, the Four Ws discussed above). Whether the service is focused upon common user characteristics or locations (e.g. location-based services such as Foursquare, or topic-driven communities based upon occupations or hobbies), the company must

---


decide what kind and quantity of information it will be collecting, as it designs both its software and its marketing materials. It must further identify necessary (and potential future) uses of the information it collects, as well as with whom and how it may (or must) share the data. The preceding is true of all companies collecting personal information; what makes a social network different is that it is expected to share the information in some ways, and that its business requires users to provide more information than they otherwise might to a third-party vendor. Once those parameters are determined, the service must ensure that all of its disclosures are accurate, and that it has procedures for circumstances in which it may be legally compelled to produce otherwise private user information.

Social networks must also consider the culture they wish to create among their users, or that may arise organically from the most frequent users of the service amongst themselves, when deciding what kind and how much information they will collect and share. When Google launched its Buzz social network in February 2010, its integration with other Google services and poorly structured privacy controls resulted in new users sharing more their Buzz use than they had intended to with their Gmail contacts and others. This in turn led to rapid condemnation by users and journalists, congressional inquiries, and FTC legal action, and Buzz was quickly discontinued by Google. By contrast, Google’s follow-up effort Google Plus was much easier to control with regard to privacy issues, and has met with substantially more positive reactions.

Even when disclosure may be technically accurate and data collection within legal parameters, social media services may still face legal and reputational challenges as to their privacy practices. Facebook, for example, is explicit in its terms of service and signup procedures that children under 13 are not permitted to use the service, in order to avoid compliance issues under COPPA and likely to minimize other unwanted situations such as pedophiles “friending” underaged Facebook users. Nevertheless, a May 2011 survey published by Consumer Reports found that 75 million Facebook users were under the age of 13, exposing it to potential liability.

For the companies that are using social media in their operations, or whose employees (whether identified or identifiable as coming from the company) are doing so personally, it is crucial to establish and communicate clear guidelines as to both the acceptable uses of social media for business purposes, and the risks of improper use. If there are specific laws or regulations that apply to the company because of its industry, the guidelines must be consistent with those as well. Businesses should keep

---

40 See, e.g., discussion of LambdaMOO at Chapter 3, note 8.
44 For more on COPPA, see Chapter 4.
in mind, though, that while they prohibit unauthorized or inappropriate social media use by employees in the workplace, they can likely not prevent such use; unless the company’s offices are in a cellular deadzone, employees whose internal networks block connection to social media services can simply access them on their cellphones, smartphones, or other mobile devices. Instead of relying on firewalls, organizations should use education and policy to reduce their risks of privacy and related breaches through social media use.

NOTE: FOR MORE INFORMATION AND ORDERING DETAILS, GO TO HTTP://EZOR.ORG/PRIVACYBOOK