the digital person
Ex Machina: Law, Technology, and Society
General Editors: Jack M. Balkin and Beth Simone Noveck

The Digital Person
Technology and Privacy in the Information Age
Daniel J. Solove
the
digital person

Technology and Privacy in the Information Age
daniel j. solove
In loving memory of

my grandma,

Jean
Contents

Acknowledgments ix

1 Introduction 1
   The Problems of Digital Dossiers 2
   Traditional Conceptions of Privacy 7
   Rethinking Privacy 8
   A Road Map for This Book 9

i computer databases

2 The Rise of the Digital Dossier 13
   A History of Public-Sector Databases 13
   A History of Private-Sector Databases 16
   Cyberspace and Personal Information 22

3 Kafka and Orwell: 27
   Reconceptualizing Information Privacy 27
   The Importance of Metaphor 27
   George Orwell’s Big Brother 29
Franz Kafka's Trial 36
Beyond the Secrecy Paradigm 42
The Aggregation Effect 44
Forms of Dehumanization:
   Databases and the Kafka Metaphor 47

4 The Problems of Information Privacy Law 56
   The Privacy Torts 57
   Constitutional Law 62
   Statutory Law 67
   The FTC and Unfair and Deceptive Practices 72
   A World of Radical Transparency:
      Freedom of Information Law 73
   The Law of Information Privacy and
      Its Shortcomings 74

5 The Limits of Market-Based Solutions 76
   Market-Based Solutions 76
   Misgivings of the Market 81
   The Value of Personal Information 87
   Too Much Paternalism? 90

6 Architecture and the Protection of Privacy 93
   Two Models for the Protection of Privacy 93
   Toward an Architecture for
      Privacy and the Private Sector 101
   Reconceptualizing Identity Theft 109
   Forging a New Architecture 119

ii public records

7 The Problem of Public Records 127
   Records from Birth to Death 127
The Impact of Technology
The Regulation of Public Records

8 Access and Aggregation:
Rethinking Privacy and Transparency
The Tension between Transparency and Privacy
Conceptualizing Privacy and Public Records
Transparency and Privacy:
  Reconciling the Tension
Public Records and the First Amendment

iii government access

9 Government Information Gathering
  Third Party Records and the Government
  Government–Private-Sector Information Flows
  The Orwellian Dangers
  The Kafkaesque Dangers
  Protecting Privacy with Architecture

10 The Fourth Amendment, Records, and Privacy
  The Architecture of the Fourth Amendment
  The Shifting Paradigms of
    Fourth Amendment Privacy
  The New Olmstead
  The Emerging Statutory Regime and Its Limits

11 Reconstructing the Architecture
  Scope: System of Records
  Structure: Mechanisms of Oversight
  Regulating Post-Collection Use of Data
  Developing an Architecture
12 Conclusion

Notes 229
Index 267
About the Author 283
It is often said that books are written in solitude, but that wasn’t true for this one. The ideas in this book were created in conversation with many wise friends and mentors. I owe them immense gratitude. Michael Sullivan has had an enormous influence on my thinking, and he has continually challenged me to strengthen my philosophical positions. Paul Schwartz has provided countless insights, and his work is foundational for the understanding of privacy law. Both Michael’s and Paul’s comments on the manuscript have been indispensable. I also must thank Judge Guido Calabresi, Naomi Lebowitz, Judge Stanley Sporkin, and Richard Weisberg, who have had a lasting impact on the way I think about law, literature, and life.

Charlie Sullivan deserves special thanks, although he disagrees with most of what I argue in this book. He has constantly forced me to better articulate and develop my positions. I may never convince him, but this book is much stronger for making the attempt.

So many other people are deserving of special mention, and if I were to thank them all to the extent they deserve, I would more than double the length of this book. Although I only list their names, my gratitude extends much further: Anita Allen, Jack Balkin, Carl Coleman, Howard Erichson, Timothy Glynn, Rachel Godsil, Eric Goldman, Chris Hoofnagle, Ted Janger, Jerry Kang, Orin Kerr, Raymond Ku, Erik Lillquist, Michael Risinger, Marc Rotenberg, Richard St. John, Chris Slobogin, Richard Sobel, Peter Swire, Elliot Turrini, and Benno Weisberg.
I greatly benefited from the comments I received when presenting my ideas, as well as portions of the manuscript, at conferences and symposia at Berkeley Law School, Cornell University, Emory Law School, Minnesota Law School, Seton Hall Law School, Stanford Law School, and Yale Law School.

My research assistants Peter Choy, Romana Kaleem, John Spaccarotella, and Eli Weiss provided excellent assistance throughout the writing of this book. Dean Pat Hobbs and Associate Dean Kathleen Boozang of Seton Hall Law School gave me generous support.

Don Gastwirth, my agent, shepherded me through the book publishing process with great enthusiasm and acumen. With unceasing attention, constant encouragement, and superb advice, he helped me find the perfect publisher. Deborah Gershenowitz at NYU Press believed in this project from the start and provided excellent editing.

Finally, I would like to thank my parents and grandparents. Their love, encouragement, and belief in me have made all the difference.

This book incorporates and builds upon some of my previously published work: Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 Stanford Law Review 1393 (2001); Access and Aggregation: Privacy, Public Records, and the Constitution, 86 Minnesota Law Review 1137 (2002); Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 Southern California Law Review 1083 (2002); and Identity Theft, Privacy, and the Architecture of Vulnerability, 54 Hastings Law Journal 1227 (2003). These articles are really part of a larger argument, which I am delighted that I can now present in its entirety. The articles are thoroughly revised, and parts of different articles are now intermingled with each other. The argument can now fully unfold and develop. Privacy issues continue to change at a rapid pace, and even though these articles were written not too long ago, they were in need of updating. The arguments originally made in these articles have been strengthened by many subsequent discussions about the ideas I proposed. I have been forced to think about many issues more carefully and with more nuance. My understanding of privacy is a work in progress, and it has evolved since I began writing about it. This book merely represents another resting place, not the final word.
Notes

Notes to Chapter 1


Notes to Chapter 2

3. See Regan, Legislating Privacy, 46.
4. Id., 46.
5. See id., 47.
23. Id., 57.
25. See id., 156.
27. Erik Larson, *The Naked Consumer: How Our Private Lives Become Public Commodities* 41 (1992). The connection between the Census Bureau and marketers remains a very close one. Presidents have frequently appointed former marketers to serve as the head of the Census Bureau. Since the 1970s, the Census Bureau has been run by a former director of marketing at General Motors, an executive at a political polling firm, a research manager for Sears, and a past president of the American Marketing Association. Id., 44. Companies have made special deals with the Census Bureau to ask certain questions and to perform tabulations of census data in ways that will be useful to marketers. Indeed, the Census Bureau has been accused of being too influenced by the needs and wants of corporate America. Id., 44–46.
30. See id., 300.
31. Id., 5.


34. Headden, “Junk Mail.”


37. See Hughes, Database Marketer, 365 (20 cents to 1 dollar per name); Headden, Junk Mail (3–20 cents per name).


44. Hughes, Database Marketer, 354.

45. See, e.g., Garfinkel, Database Nation, 137; Givens, Privacy Rights, 83.


47. Smith, Franklin’s Web Site, 314.


49. For example, Experian has information on 205 million Americans. See http://www.experian.com/corporate/factsheet.html.

50. See Givens, Privacy Rights, 83.


54. Id.

55. Id.


57. http://www.hippodirect.com/ListSubjectsN_1.asp?ISubject=37. For a terrific discussion of various databases such as the ones discussed in this section, see


68. Sterne, People Click, 255.


Notes to Chapter 3

1. See, e.g., Florida v. Riley, 488 U.S. 445, 466 (1989) (Brennan, J., dissenting) (quoting passage from 1984 to criticize the majority’s holding that viewing the defendant’s greenhouse from a low-flying helicopter wasn’t a search); United States v. Kyllo, 190 F.3d 1041, 1050 (9th Cir. 1999) rev’d 121 S. Ct. 2038 (Noonan, J., dissenting) (“The first reaction when one hears of the Agema 210 [thermal imaging device used to detect heat emissions from the home] is to think of George Orwell’s 1984.”); Lorenzana v. Superior Court, 511 P.2d 33, 41 (Cal. 1973) (en banc) (“Surely our state and federal Constitutions and the cases interpreting them foreclose a regression into an Orwellian society.”).


5. George Lakoff & Mark Johnson, Metaphors We Live By 145–46 (1980).

6. Id., 5.


8. Winter, Clearing, 65 (metaphor is a cognitive “process by which the mind projects a conceptual mapping from one knowledge domain to another”).


15. Id., 20.


19. Id., 201.


40. Id., 146.

41. Id., 199.

42. Id., 42–43.


46. Id. at 223.


49. Id., 1348, 1365.


58. See id., 435.


61. As legal scholar Arthur Miller observes, an “individual who is asked to provide a simple item of information for what he believes to be a single purpose may omit explanatory details that become crucial when his file is surveyed for unrelated purposes.” Miller, *Assault on Privacy*, 34.

62. W.H. Auden’s poem, “The Unknown Citizen” aptly describes this phenomenon. A person’s life is chronicled through the various records kept about him; we learn a lot about the person, but at the end of the poem, Auden demonstrates that the records reveal little about his happiness or quality of life. W.H. Auden, “The Unknown Citizen,” in *Collected Poems* 201 (Edward Mendelson ed., 1976).

64. *Brazil* (Universal Pictures 1985).
67. Hire Check, “Background Screening,” at http://www.hirecheck.com/ProductsAndServices/backgroundScreening.html (last viewed July 1, 2002).
73. See, e.g., Jane B. Baron, “Law, Literature, and the Problems of Interdisciplinarity,” 108 Yale L.J. 1059, 1061 n.9 (1999) (comparing Westlaw search of law reviews for terms “law and economics” and “law and literature” to measure comparative influence of each of these academic movements).
78. Smith, *Managing Privacy*, 123.
86. See In re Geocities, 1999 FTC LEXIS 17 (Feb. 5, 1999).
91. 10 U.S.C. § 654.
99. Id.

Notes to Chapter 4

7. Id., 195.
8. Id., 198, 205.
12. See Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 235 (Minn. 1998) (recognizing a common law tort action for invasion of privacy and noting that Minnesota had remained one of the few hold-outs).
14. See, e.g., Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 235 (Minn. 1998) (recognizing a common law tort action for invasion of privacy and noting that Minnesota had remained one of the few hold-outs).
18. Restatement (Second) of Torts § 652C (1976).
19. Restatement (Second) of Torts § 652C cmt. a (1976). According to legal scholar Jonathan Kahn, the “early association of appropriation claims with such intangible, non-commensurable attributes of the self as dignity and the integrity of one’s persona seems to have been lost, or at least misplaced, as property-based conceptions of the legal status of identity have come to the fore.”
20. Because their identities are lucrative for marketing purposes, celebrities often sue under this tort. For an interesting illustration, see Carson v. Here’s Johnny Portable Toilets, Inc., 698 F.2d 831 (6th Cir. 1983), where Johnny Carson successfully sued a portable toilet company that used the name “Here’s Johnny Portable Toilets.”
23. As legal scholar Bruce Sanford contends: “A stake-out by a group of unrelated reporters should be viewed as no more than the sum of its separate parts.”
29. U.S. Const. Amend. IV.
31. U.S. Const. Amend. V.
32. 116 U.S. 616 (1886).
33. Id., 630.
35. See Warden v. Hayden, 387 U.S. 294 (1967) (overturning the mere evidence rule in Boyd); Shapiro v. United States, 355 U.S. 1 (1948) (holding that the Fifth Amendment does not prohibit the government from requiring that a person produce her records).


37. Id., 743.


40. 410 U.S. 113 (1973).


42. Id., 601–02.

43. Id., 603.

44. 72 F.3d 1133 (3d Cir. 1995).

45. Id., 1139–40.


56. §§ 2710(b)(1), (c)(1).


60. 45 C.F.R. § 164.508(a).


62. § 6502(b)(1)(A).


65. 15 U.S.C. § 6802(a), (b).

66. See Smith, Franklin’s Web Site, at 327.


69. As Paul Schwartz observes, “personal information in the private sector is often unaccompanied by the presence of basic legal protections. Yet, private enterprises now control more powerful resources of information technology than ever before.” Paul M. Schwartz, “Privacy and Democracy in Cyberspace,” 52 Vand. L. Rev. 1609, 1633 (1999).


76. See, e.g., In re Liberty Financial Companies, No. 9823522, 1999 FTC LEXIS 99 (May 6, 1999) (operator of website falsely promised that personal data collected from children and teens would be kept anonymous); FTC v. ReverseAuction.com, Inc., No. 99-CV-32 (D.D.C. Jan. 6, 2000) (company improperly obtained personal information from eBay and used it to spam eBay customers); In re GeoCities, 1999 FTC LEXIS 17 (Feb. 5, 1999) (website falsely promised that it never provided information to others without customer permission).

77. See In the Matter of Microsoft Corp., No. 012-3240.

78. Schwartz, “Privacy and Democracy,” 1638. The relatively recent GLB Act provides a rare exception, for it requires financial institutions to develop “safeguards for personal information.” See 15 U.S.C. §§ 6801(b); 6805(b)(2). This is a rather general mandate, and the agency regulations do not provide much greater specificity. Ultimately, the strength of the GLB Act’s security protections will depend upon how they are enforced.


81. Id., 23.

82. Id., 23–24.

Notes to Chapter 5


I will advance a concept of privacy based on the individual’s control of information.

3. See Jessica Litman, “Information Privacy/Information Property,” 52 Stan. L. Rev. 1283, 1287 (2000) (“The proposal that has been generating the most buzz, recently, is the idea that privacy can be cast as a property right.”); Pamela Samuelson, “Privacy as Intellectual Property,” 52 Stan. L. Rev. 1125, 1132 (2000) (“In recent years, a number of economists and legal commentators have argued that the law ought now to grant individuals property rights in their personal data.”)


5. Westin, Privacy and Freedom, 324.


39. See id., 1101.
44. Id., 1662.
47. Id., 1126.
49. Of course, not all attempts to translate privacy into property rights will threaten the protection of privacy. For an example of a helpful use of property rights to protect privacy, see Janger, “Muddy Property.”

Notes to Chapter 6
3. Restatement (Second) of Torts § 652(I) comment (a).
4. 182 F.3d 1224, 1234–35 (10th Cir. 1999).
6. Fred Cate, Privacy in the Information Age 196 (1997).
7. Id., 131.
8. Id.


18. Id., 200.

19. Id., 207.


23. Moore v. Regents of the University of California, 793 P.2d 479 (Cal. 1990) (doctor has a fiduciary duty to disclose personal interests that could affect the doctor’s professional judgment).


25. As one court has aptly explained the relationship: “A fiduciary relationship is one founded on trust or confidence reposed by one person in the integrity and fidelity of another. Out of such a relation, the laws raise the rule that neither party may exert influence or pressure upon the other, take selfish advantage of his trust[, or deal with the subject matter of the trust in such a way as to benefit himself or prejudice the other except in the exercise of utmost good faith.” Mobile Oil Corp. v. Rubenfeld, 339 N.Y.S.2d 623, 632 (1972).


39. OECD Guidelines.


42. Id.


44. No. 022-3260 (July 30, 2003).

45. 15 U.S.C. §§ 6801(b); 6805(b)(2).

46. U.S. General Accounting Office (GAO), Report to the Honorable Sam Johnson House of Representatives, Identity Theft: Greater Awareness and Use of Existing Data Are Needed 23 (June 2002).

47. Id.


49. Id.


59. GAO Identity Theft Report, 1.
60. Id., 17–18.
68. 15 U.S.C. § 1681h(e), § 1681o, § 1681p.
71. Fred H. Cate, Privacy in Perspective 22 (2001).
73. Lee, “Fighting Back.”
74. GAO Identity Theft Report, 7.
79. For example, an identity thief purchased the SSNs of several top corporate executives from Internet database companies. The thief then used the SSNs to obtain more personal information about the victims. Benjamin Weiser, “Identity Theft, and These Were Big Identities,” N.Y. Times, May 29, 2002.
81. See 11 U.S.C. § 107(a) (Any “paper filed . . . and the docket of a bankruptcy court are public records and open to examination by an entity at a reasonable time without charge”).
86. Id., 108–14.
89. See id.
94. Cheever, “Ivy Rivalry.”
95. Vacca, Identity Theft, 54.
98. In her testimony before Congress, Beth Givens recommended that “[a]ll consumers should be able to receive one free copy of their credit report annually,” and noted that six states have enacted this measure into law. See Givens, “Identity Theft,” U.S. Senate Testimony.
101. Billions of pre-approved credit offers are made to consumers each year, and there is vigorous competition among creditors to find new customers. See Beth Givens, “Identity Theft,” U.S. Senate Testimony.

Notes to Chapter 7

4. See, e.g., id. § 103175.


10. See Lane, *Naked*, 274–75.


12. See, e.g., Cal. R. 243.1(c) (“Unless confidentiality is required by law, court records are presumed to be open”). Not all court records are public; in most states, adoption records, grand jury records, and juvenile criminal court records are not public. See, e.g., David S. Jackson, “Privacy and Ohio’s Public Records Act,” 26 Cap. U. L. Rev. 107, 120 (1997). Beyond pleadings and motions (which are, for the most part, always contained in the court file), other documents (such as exhibits) and transcripts may or may not be contained in the file. For example, typically a trial transcript will only be contained in the court file if an appeal is taken. The availability of other documents in the court file is controlled by local practice. Local practices vary greatly depending on limited storage capacities in clerks’ offices. Often, exhibits are kept by the parties.


16. In practice, juror information is rarely sought out except in high-profile cases.

17. If Social Security information is disclosed in court filings, confidentiality is lost. 20 C.F.R. § 401.180.


22. See Lane, *Naked*, 213.


26. See, e.g., Paul P. v. Verniero, 170 F.3d 396, 398 (3d. Cir. 1999); Russell v. Gregoire, 124 F.3d 1079, 1092 (9th Cir. 1997).


31. See Public Records Online, 8.

32. For example, KnowX.com states that it has amassed millions of public records, which are updated regularly. See http://www.knowx.com. Search Systems contains over 6,000 searchable public record databases. See http://www.pacinfo.com. Locateme.com permits its users to search public records such as driver registrations, voter registrations, and credit headers. See http://www.locateme.com.


40. See Cross, Right to Know, 26.


42. See Cross, Right to Know, 27; “Public Inspection,” 1108.

43. See Cross, Right to Know, 29.


45. See Key, “Common Law,” 668.

46. See Cross, Right to Know, 135–36.


54. See, e.g., Unabom Trial Media Coalition v. United States Dist. Court for E. Dist. of Cal., 183 F.3d 949, 951 (9th Cir. 1999).
55. See, e.g., Doe v. Frank, 951 F.2d 320, 323 (11th Cir. 1992) (“It is the exceptional case in which a plaintiff may proceed under a fictitious name”).
59. See Jason Lawrence Cagle, Note, “Protecting Privacy on the Front Page: Why Restrictions on Commercial Use of Law Enforcement Records Violate the First Amendment,” 52 Vand. L. Rev. 1421, 1422 n.2 (1999). While some states’ FOIAs replaced the common law, courts in some states have held that the state’s FOIA operates as an additional right of access to the common law. See id.
60. See Note, “Public Inspection,” 1107.
64. 5 U.S.C. § 552(f).
66. See, e.g., Del. Code Ann. tit. 29, § 10001 (stating that “it is vital that citizens have easy access to public records in order that the society remain free and democratic”); 5 Ill. Comp. Stat. Ann. 140/1 (1) (stating that the right to inspect public records “is necessary to enable the people to fulfill their duties of discussing public issues fully and freely”).
68. 5 U.S.C. §§ 552(b)(6); 552(b)(7)(C).
69. In contrast, companies seeking to protect trade secrets can initiate actions on their own to protect their information in what is known as a “reverse-FOIA” lawsuit. See Heather Harrison, Note, “Protecting Personal Information from Unauthorized Government Disclosures,” 22 Memphis St. U. L. Rev. 775, 783 (1992).
75. 5 U.S.C. § 552a.
76. Warth v. Dep’t of Justice, 595 F.2d 521, 522–23 (9th Cir. 1979).
77. 5 U.S.C. §§ 552a(b)(3).
80. See id.; Harrison, “Protecting Personal Information,” 787.
81. 5 U.S.C. § 552a(g)(4).
83. 838 F.2d 418, 425 (10th Cir. 1988).
94. 2 U.S.C. § 438(a)(4). Although the FEC occasionally uses decoy names to check to see if candidates are engaging in improper uses of the records, the FEC has not, according to critics, done much to investigate reports of abuse. See Chandrasekaran, “Information Pays.”

Notes to Chapter 8

2. Louis D. Brandeis, Other People’s Money 92 (1932).
3. Engrav v. Cragun, 769 F.2d 1224, 1228 (Mont. 1989); Houston Chronicle Publ’g Co. v. City of Houston, 531 S.W.2d 177, 186 (Tex. App. 1975); United States v. Hickey, 767 F.2d 705, 708 (10th Cir. 1985).
4. In re Cont’l Ill. Sec. Litig., 732 F.2d 1302, 1308 (7th Cir. 1984).
12. 608 P.2d 716 (Cal. 1980).
15. Id. § 652B cmt. c.
18. 87 F.3d 176, 179 (6th Cir. 1996); see also Doe v. City of New York, 15 F.3d 264, 268 (2d Cir. 1994) (“[A]n individual cannot expect to have a constitutionally protected privacy interest in matters of public record”).
19. 895 F.2d 188, 190–95 (4th Cir. 1990).
20. 124 F.3d 1079, 1094 (9th Cir. 1997).
21. 170 F.3d 396, 400–01, 405 (3d Cir. 1999). But see Doe v. Portiz, 662 A.2d 367, 411 (N.J. 1995) (following the conception from Reporters Committee when examining the constitutionality of Megan's Law and noting that “a privacy interest is implicated when the government assembles . . . diverse pieces of information into a single package and disseminates that package to the public, thereby ensuring that a person cannot assume anonymity”).
24. Mans v. Lebanon Sch. Bd., 290 A.2d 866, 868 (N.H. 1972) (quoting H.R. Rep. No. 1497, at 11 [1966]) (following the conception from Reporters Committee). See also Pottle v. Sch. Comm. of Braintree, 482 N.E.2d 813, 816–17 (Mass. 1985) (holding that payroll records containing names, salaries, overtime pay, and addresses of policemen and school employees were not private within the meaning of Massachusetts’s FOIA privacy exception because the information was not intimate).
28. Sykes, End of Privacy, 42–44.
29. Planned Parenthood v. Am. Coalition of Life Activists, 290 F.3d 1058 (9th Cir. 2002) (en banc).


36. See id., 50–53.


42. See, e.g., U.S. Dep’t of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 772 (1989); see also Halloran v. Veterans Admin., 874 F.2d 315, 323 (5th Cir. 1989) (“[I]f disclosure of the requested information does not serve the purpose of informing the citizenry about the activities of their government, disclosure will not be warranted even though the public may nonetheless prefer, albeit for other reasons, that the information be released”).

43. 416 A.2d 244, 247–48 (D.C. 1980).

44. 194 F.3d 954, 960 (9th Cir. 1999).


52. See United States v. Criden, 675 F.2d 550, 557 (3d Cir. 1982); United States v. Chagra, 701 F.2d 354, 363 (5th Cir. 1983).
53. 733 F.2d 1059, 1070 (3d Cir. 1984) (internal quotations and citation omitted).
54. United States v. McVeigh, 119 F.3d 806, 811 (10th Cir. 1997); see also Littlejohn v. BIC Corp., 851 F.2d 673, 678 (3d Cir. 1988) (“Access means more than the ability to attend open court proceedings; it encompasses the right of the public to inspect and to copy judicial records.”); Associated Press v. United States Dist. Court, 705 F.2d 1143, 1145 (4th Cir. 1984) (“There is no reason to distinguish between pretrial proceedings and the documents filed in regard to them”). But see Lanphere & Urbaniak v. Colorado, 21 F.3d 1508, 1512 (10th Cir. 1994) (“[T]here is no general First Amendment right in the public to access criminal justice records”).
56. 988 F.2d 1344, 1354 (4th Cir. 1993).
58. After Whalen and Nixon, the Supreme Court has done little to develop the right of information privacy. A majority of the circuit courts have accepted the constitutional right to information privacy. See, e.g., In re Crawford, 194 F.3d 954, 958 (9th Cir. 1999); Walls v. City of Petersburg, 895 F.2d 188, 192 (4th Cir. 1990); Barry v. City of New York, 712 F.2d 1554, 1559 (2d Cir. 1983); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980); Plante v. Gonzalez, 575 F.2d 1119, 1132, 1134 (5th Cir. 1978). One circuit court has expressed “grave doubts” as to the existence of the right, stopping short of confronting the issue of whether the right existed. Am. Fed’n of Gov’t Employees v. Dep’t of Housing & Urban Dev., 118 F.3d 786, 788, 791–92 (D.C. Cir. 1997). For more background about the constitutional right to information privacy, see Elbert Lin, “Prioritizing Privacy: A Constitutional Response to the Internet,” 17 Berkeley Tech. L.J. 1085, 1124–28 (2002).
60. 443 U.S. 97, 103 (1979).

Notes to Chapter 9

3. See, e.g., Paul M. Schwartz, “Beyond Lessig’s Code for Internet Privacy: Cyber-
space Filters, Privacy-Control, and the Fair Information Practices,” 2000 Wisc. L.
Rev. 743, 770–71 (describing lack of employee privacy).
at 64.
6. This information was requested in employer questionnaires in American Fed-
eration of Government Employees v. HUD, 118 F.3d 786 (D.C. Cir. 1997) and Walls v.
City of Petersburg, 895 F.2d 188 (4th Cir. 1990).
7. See Sarah Schafer, “Searching for a Workable Fit; Employers Try Psychological
9. See John Markoff, “Pentagon Plans a Computer System That Would Peek at Per-
sonal Data of Americans,” N.Y. Times, Nov. 9, 2002.
12. See Cheryl Bolen, “Senate Withholds Data-Mining Funds until DOD Ad-
14. See id.
15. See id.
16. See Gregory Palast, “Florida’s Flawed ‘Voter-Cleansing’ Program,” Salon.com,
(Dec. 4, 2000).
17. See Robert O’Harrow, Jr., “U.S. Backs Florida’s New Counterterrorism Data-
bases: ‘Matrix’ Offers Law Agencies Faster Access to Americans’ Personal Records,”
Wash. Post, Aug. 6, 2003, at A1; Brief of Amici Curiae Electronic Privacy Informa-
tion Center (EPIC) and Legal Scholars and Technical Experts, in Hiibel v. Sixth Ju-
dicial District Court of Nevada, No. 03-5554 (U.S. Supreme Court, Dec. 13, 2003).
19. The Attorney General’s Guidelines on General Crimes, Racketeering Enter-
20. The Attorney General’s Guidelines on General Crimes, Racketeering Enter-
prise and Terrorism Enterprise Investigations § VI (May 30, 2002).
G1.
Nov. 26, 2001, at A2; Robert O’Harrow, Jr., “Financial Database to Screen Accounts:
A1.
39. See 31 C.F.R. § 103.22(1).
51. 401 U.S. 1 (1971).
52. Id., 6.
53. It is unclear how receptive the Court will be to this argument. The Court has held that mere information gathering about a group’s public activities did not harm First Amendment interests enough to give rise to standing. See Laird v. Tatum, 408 U.S. 1, 12–15 (1972).
65. See, e.g., Friedman, Crime and Punishment, 67.
71. See Regan, Legislating Privacy, 87.
74. See Regan, Legislating Privacy, 90.
82. See Gentry, Hoover, 76.
84. See Donner, Surveillance, 34; Gentry, Hoover, 79; Powers, Hoover, 68.
85. See Gentry, Hoover, 93.
86. See Powers, Hoover, 79–80.
87. See Gentry, Hoover, 98–99.
89. Id., 10.
91. See Schrecker, McCarthyism, 76–84.
93. See Schrecker, McCarthyism, 77.
95. Schrecker, McCarthyism, 76–84.
97. See David J. Garrow, The FBI and Martin Luther King, Jr. 165 (1980).
99. See, e.g., Diffie & Landau, Privacy on the Line, 140–42. It was not until 1975, nearly a decade after the wiretapping and three years after Hoover’s death, that Congress conducted an inquiry into the wiretapping of King through the famous Church Committee. See id., 178.
100. Garrow, Martin Luther King, 100–01.
101. Id., 126.
103. See id., 78. Hoover’s dislike of King may have also stemmed from racism. It is well-documented that Hoover was racist. See id., 153.
104. See id., 79–83.
105. See id., 151.
106. Id., 209.
Notes to Chapter 10

1. U.S. Const. amend. IV.
22. Id., 1771.
26. Although corporations are deemed “persons” under the Fourteenth Amendment, see Santa Clara County v. S. Pac. R.R., 118 U.S. 394, 394–95 (1886), they are not afforded Fourth Amendment rights. See California Bankers Ass’n v. Shultz, 416 U.S. 21, 65 (1974) (stating that “corporations can claim no equality with individuals in the enjoyment of a right to privacy”).
27. Stuntz, “Privacy’s Problem,” 1037.
28. Id.
30. See id.
34. Louis Fisher, “Congress and the Fourth Amendment,” 21 Ga. L. Rev. 107, 115 (1986) (“The spirit and letter of the fourth amendment counseled against the belief that Congress intended to authorize a ‘fishing expedition’ into private papers on the possibility that they might disclose a crime”).
35. U.S. Const. amend. IV.
38. Wasserstrom & Seidman, “Fourth Amendment,” 82.
49. See id., 848.
50. McDonald v. United States, 335 U.S. 451, 455–56 (1948). See also Steagald v. United States, 451 U.S. 204, 212 (1981) (warrants are necessary because law enforcement officials “may lack sufficient objectivity”); Coolidge v. New Hampshire, 403 U.S. 443, 450 (1971) (stating that “prosecutors and policemen simply cannot be asked to maintain the requisite neutrality with regard to their own investigations”); Johnson v. United States, 333 U.S. 10, 13–14 (1948) (stating that the Fourth Amendment ensures that inferences of potential culpability “be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime”).
53. 116 U.S. 616 (1886).
54. Id., 630.
55. See, e.g., Amar, Criminal Procedure, 22 (explaining that Boyd was part of the Lochner Court’s staunch protection of property); Alan Westin, Privacy and Freedom 339–41 (1967) (describing the conception of privacy in Boyd as “propertied privacy”).
56. 198 U.S. 45 (1905).
58. 96 U.S. 727, 733 (1877).
59. 141 U.S. 250, 252 (1891).
61. 277 U.S. 438 (1928).
62. Id., 464.
63. Id., 473 (Brandeis, J., dissenting) (internal quotations omitted).
64. Id.
65. Id., 473 (internal quotations omitted).
68. Id., 361 (Harlan, J., concurring).
71. See Nardone v. United States, 302 U.S. 379 (1937) (evidence directly obtained by wiretapping excluded from evidence); Nardone v. United States, 308 U.S. 338 (1939) (evidence obtained as the fruit of illegal wiretapping could not be used in court).
73. See Diffie & Landau, Privacy on the Line, 155–65.
74. See id., 161–62.
75. See id., 144.
76. Id., 173.
80. Id.
82. Id., 442.
83. 442 U.S. 735, 743 (1979).
85. Id., § I.C.1(b)(iv).
86. Olmstead, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).
92. Grand juries are still used in some states as well as in the federal system. See Degnan, “Obtaining Witnesses,” 229.
94. Stuntz, “Privacy’s Problem,” 1038.
99. Id. § 2518.
102. This conclusion is debatable, however, because telephone companies can also store telephone communications, and it is unlikely that the Court would go so far as to say that this fact eliminates any reasonable expectation of privacy in such communications.
104. Kerr, Searching and Seizing, § III.B.
105. Id., § III.D.1.
108. See, e.g., United States v. Hambrick, 55 F Supp.2d 504 (W.D. Va. 1999). For a compelling argument for why electronic surveillance statutes should have an

111. “Upon application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device. . . .” Id. § 3123 (a)(1).
112. United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995). See also Kerr, Searching and Seizing, §IV.B.
120. 47 U.S.C. § 551(b)(2).
125. Id. § 164.512(f)(2).
126. 45 C.F.R. § 160.102.

Notes to Chapter II
3. See Inness, Intimacy, 78 (intimate matters draw “their value and meaning from the agent’s love, care, or liking”).
4. See Smith v. Maryland, 442 U.S. 735, 740–41 n.5 (1979) (noting that “where an individual’s subjective expectations had been ‘conditioned’ by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was”).
5. See Current Opinions of the Judicial Council of the American Medical Ass’n Canon 5.05 (1984) (observing that “the information disclosed to a physician during the course of the relationship between the physician and patient is confidential to the greatest possible degree”).
8. See, e.g., Cal. Health & Safety Code § 199.21 (prohibiting disclosure of HIV test results); N.Y. Pub. Health L. § 17 (prohibiting disclosure of minors’ medical records pertaining to sexually transmitted diseases and abortion).
9. See Weissenberger, Evidence, 190.
14. Mechanisms of restriction are also embodied in evidentiary privileges. These privileges protect particular relationships, such as those between attorney and client, physicians and patients, and others. Privileges are needed to ensure that our conversations with our lawyers and doctors remain candid.
15. U.S. Const. amend V.
17. 255 U.S. 298, 309 (1921).
22. Id., 571.

Notes to Chapter 12
3. Id.
10. Id., at 50–51. This law, which protects against prying into another’s mail, is still valid today. See 42 U.S.C. § 1702.
11. 96 U.S. 727, 733 (1877).
12. See Regan, Legislating Privacy, 47; see also David J. Seipp, Right to Privacy, 43–50 (1978).
Abortion doctors, 147
Abortion rights, 65
Accessibility of information, 161, 213
Acxiom, Inc., 171
Acxiom.com, 3–4
Administrative states, 189–190, 191
Advertising, 43
Affiliate sharing, 70–71
Aggregation effect: defined, 44; digital biographies, 44–47; Kafka metaphor for invasion of privacy, 149; restrictions on government information collection, 215; threats to privacy, 161; tort law, 95; value of personal information, 87–88
Airline passengers, 171, 182
Allen, Anita, 70
Amar, Akhil, 192
Amazon.com, 23–24, 92, 172–173
America Online (AOL), 54, 80
Amsterdam, Anthony, 215
Andrews v. Veterans Administration, 136–137
Anonymity, 176–177, 252n21
Anonymous speech, 176–177
Appropriation, 60, 61, 89, 238n19, 238n20
Architecture: architectural solutions for architectural problems, 100; architectures of control, 99; architectures of vulnerability, 99; criminal law compared to, 100; Fourth Amendment’s, 188–209; identity theft, 115–123; implementation of, 98; information systems, 98; Katyal on, 98; meaning, 97–98; Panopticon’s, 98–99; privacy protections, 186; psychological and social effect, 98; separation of powers as, 194; Social Security numbers (SSNs), 116; Wright on, 98. See also architecture for governing government information collection
Architecture conception of privacy, 93–123; common good, 186; enforcement, 107–109; Fair Information Practices, 104–105, 107; fiduciary relationship as model, 102–104; harmfulness of current architecture, 119; harms addressed, 107–108; individual rights, 186; inequalities in knowledge, 102; information collection, 121; invasion conception compared to, 100–101, 186; need for federal agency to regulate collection and use of personal information, 108–109; networking by institutions, 101–102; opening new accounts, 122; participation in uses of personal information, 105–106, 113, 118, 120, 149, 223; recognition of harm within design and structure, 101; relationship between individuals and information collectors, 101–105; responsibility for uses of personal information, 120, 121; restrictions on use of data, 106–107; varying methods of personal identification, 121–122
Architecture for governing government information collection, 210–222; control goal, 211, 219; development of, 222; exclusionary rule, 221; goals, 211, 215; mandated destruction of data, 222; mechanisms for controlling government information collection, 217–221; minimization, 211, 219; no control option for controlling government information collection, 217; oversight mechanisms for controlling government information collection, 218–221; particularization, 211, 219; post-collection use of data, 221–222; probable cause, 220; restriction mechanisms for controlling government information collection, 218, 264n14; scope, 211–217; social relationships, 213–216; special court orders, 220–221, 222; subpoenas, 219–220; system of records, 211–217, 221; third party data sources, 215–216, 221; type of information vs. third party possessing it, 213, 215; volunteering data vs. accessing information, 212; warrants, 219–220

Architectures of control, 99
Architectures of vulnerability, 99, 115, 119
Aristotle, Inc., 20
Arrest records, 128–129, 141, 145, 158
Ashcroft, John, 171
Assault on Privacy, The (Miller), 147
Ayres, Ian, 77

Background checks, 21, 47, 121, 171

Baird v. State Bar, 176
Balkin, Jack, 28, 151
Bank records: confidentiality, 263n123; Douglas on, 174–175; Right to Financial Privacy Act, 206; as source of government information, 166; tracking of, 21; United States v. Miller, 200–201
Bank Secrecy Act (1970), 174
Bankruptcy, 83, 117, 129–130, 246n81
Bargaining power, 82–85, 88, 90
Bennet, Colin, 33, 71
Bentham, Jeremy, 30
Big Brother, 29–36; architectures of control, 99; Brave New World compared to, 40; cashless marketplace, 233n22; citations by Supreme Court, 233n3; computer databases, 33–34; computers, 31; digital dossiers, 7, 35; DoubleClick on, 43; drug testing, 233n3; government, 7; government data protection boards, 233n22; government information collection, 175–177; as metaphor for invasion of privacy, 7–8, 27, 29–36; power, 40; privacy, 31, 43; private-sector databases, 32; public understanding of, 28; surveillance, 34–35; telescreens’ role, 29–31; Trial compared to, 38; Wrong on, 30
Birth date, 121
Birth records, 127
Bork, Robert, 69
Boys, 25–26
Boyd v. United States, 63–64, 195–196, 197, 218
Boyer, Amy Lynn, 54
Brandes, Louis, 141, 175, 197–198, 201. See also Right to Privacy (Warren and Brandes)
Brave New World (Huxley), 40, 191
Brazil (film), 46
Brin, David: Transparent Society, 73
Briscoe v. Reader’s Digest Ass’n, 144
Britain: surveillance in, 99
Bureaucracy: accountability, 53–55, 149; databases, 39; decision-making, 39; existence of generalized harm, 96; harms caused by, 175; human dignity, 39; Kafka’s Trial, 9, 38; law enforcement, 179; laws governing relationships with, 91–92; occurrence of specific abuses, 96; personal information, 9, 39; potential for abuse of personal information, 152; power, 39–41, 91; powerlessness, 9, 48; Schwartz on, 38–39; Weber on, 38–39
Businesses: access to public records, 156; Census Bureau connections, 230n27; collection of personal information, 227; commercial use of public records, 156; Fourth Amendment, 260n26; freedom of information laws, 151–152; government requests for data, 172, 206; information collection, 227; informing people about their personal information, 120; percent using direct marketing, 19; personal relationship with, 100; potential for abuse of personal information, 152; power of, 148; responsibility for identity theft, 118–119; responsibility for personal information, 120; reverse-FOIA lawsuits, 250n69; Social Security number as identifier, 154; threats to privacy, 32; trade secrets,
bankruptcy sales, 83; Big Brother metaphor, 33–34; of campaign donors, 20; categorization of people, 19, 22; conformity, 33, 34; credit histories, 21; defamation, 60; demographic information, 18; false light, 60; intrusion upon seclusion, 59; new bank accounts, 21; number maintained by federal government, 15; of people obtaining new jobs, 15, 148, 170; personal information in, 3; powerlessness, 41, 47–48; privacy of information in, 43, 44; problem with, 89–90, 91; prohibitions on disseminating information, 122; psychographic information, 18–19; public disclosure, 59; as public places, 59; of recent movers, 22; Schwartz on, 33; Social Security numbers (SSNs), 14–15; of supermarket sales, 20; targeted/database marketing, 18; tort law, 61–62; of voters, 20. See also databases; digital dossiers

Computer matching, 181

Computerization, 14, 15

Computers, 14, 23–26, 31, 42, 48–49

Conde Nast Publications, Inc., 52–53

Confidentiality: application to companies, 244n30; bank records, 263n23; evidentiary privileges, 214, 264n14; implied obligations, 77; patient-physician relationship, 103, 263n22, 263n123; public records, 157; Social Security information, 248n17

Conformity, 33, 34

Consent, 51–52, 84–86, 97, 106, 154

Constitution. See constitutional law; United States Constitution

Constitutional law, 56, 62–67, 75, 157. See also United States Constitution

Contraceptives, 64, 65

Contract law, 56, 77, 81–82, 196

Contracts, 82–83, 90–91

Contractual default rules for ownership of personal information, 77, 78–79, 85, 88, 90

Conviction records, 130, 145

Cookies (on hard drives), 24, 68–69

Corporations. See businesses

Court orders, 203

Court records: access to, 131–132, 141, 156, 248n12; Cox Broadcasting Corp. v. Cohn, 157; data in, 129–130; Publicker Industries, Inc. v. Cohen, 155–156; sealing, 134; true information in, 157

Cox Broadcasting Corp. v. Cohn, 145, 157, 159
Crawlers, 25–26
Credit cards, 110–111, 122–123, 166, 247n101
Credit reporting: Cate on, 80; Citibank, 118; complaints about, 51, 236n79; credit histories, 21; dispute resolution, 121; Equifax, 21, 112; Experian, 21, 112; Fair and Accurate Credit Transactions Act, 113; Fair Credit Reporting Act (FCRA), 67–68, 84, 112–113, 206; fraud alerts, 113; identity theft, 109, 112; inaccuracies in personal information, 121; information flow, 80; information highway, 233n12; LoPucki on, 117–118; major reporting agencies, 21; obtaining information about oneself, 112, 113, 119, 120–121, 247n98; opt-in systems, 120–121; pervasiveness, 21; privacy protections, 117; release of government data to, 136; Remsburg v. Docusearch, Inc., 54; sale of credit reports for criminal uses, 55; as source of government information, 167; sudden changes in behavior, 121; Trans Union Corp., 21, 112; TRW, Inc. v. Andrews, 112–113
Criminal justice system, 153–154, 155–156, 248n16, 249n44
Criminal law, 95, 100
Culture of Surveillance (Staples), 31
Customers, “angel” vs. “demon,” 50
Dash, Samuel, 200
Data aggregation, 170
Data collection. See information collection
Data mining, 41, 171
Data warehousing, 42
Database industry, 19
Database marketing. See targeted/database marketing
Databases, 38, 39, 208–209. See also computer databases; digital dossiers
Dataveillance, 33
DCSiooo (Carnivore), 172
Decentralized consumerism, 32
Defamation, 60
Degnan, Ronald, 202
Democracy, 175–176
Demographic information, 18
Department of Defense, 5–6
Department of Health, Education, and Welfare (HEW), 15, 104
Dewey, John, 6
Digital biographies, 44–47, 146, 168
Digital dossiers, 13–26; becoming digital biographies, 168; Big Brother, 7, 35; Census data, 13–14; defined, 1–2; Flaherty on, 32; government access to, 10; identity theft, 110, 115; inaccuracies in, 46–47; information brokers, 153; information privacy law, 75; invasion conception of privacy, 8; Kafka metaphor for invasion of privacy, 72; Kang on, 32–33; law’s contribution to creating, 227; owners’ goals, 7; personal information in, 7; pervasiveness of data, 49; powerlessness, 149; private-sector databases, 16–21; problems with, 2–7, 75, 95, 223, 226; public-sector databases, 13–16; reductive nature, 44–47; restrictions on government information collection, 215; social structure, 148; threats to privacy, 222; Trial and, 36, 37; use restrictions, 150; uses, 3, 9; vulnerability, 149
Digital person defined, 1
Digital rights management (DRM), 25
Direct marketing, 17, 19, 80
Direct Marketing Association (DMA), 84, 91
Discipline and Punish (Foucault), 30
Disclosure. See freedom of information laws (FOIAs); public disclosure
Discount cards, 52
Divorce records, 130
Doe v. Southeastern Pennsylvania Transportation Authority (SEPTA), 66–67
Domestic surveillance, 180
Donnelly Marketing Information Services, 18, 20
DoubleClick, 24–25, 43, 68–69
Driver’s Privacy Protection Act (DPPA, 1994), 138, 147, 154
Drug testing, 233n3
Dunhill International, 22
Dunhill v. Director, District of Columbia Department of Transportation, 151
Dürenmatt, Friedrich, 42
Duyer v. American Express Co., 61, 89
Earnings data, 14
Eastman Kodak Company, 57
Eavesdropping, 198
EBay, 173
Elections, 20, 137–138, 170
Electronic Communications Privacy Act (ECPA), 68, 204–205, 205–206, 208
Electronic surveillance, 68, 199–200, 204
Email, 204–205
Employee records, 166
End of Privacy (Whitaker), 32
Equifax, 21, 112
Etzioni, Amitai, 224
European Community Directive on Data Protection (European Union), 106–107
European Union, 67, 106–107
Evidence, 189, 199, 218, 261n71
Evidentiary privileges, 56, 264n14
Ex Parte Jackson, 196, 225
Exclusionary rule: architecture for governing government information collection, 221; Cable Communications Policy Act, 207; civil damages, 259n15; evidence, 189; Fourth Amendment, 189, 210; Holmes on, 189; information obtained in violation of, 205; Loewy on, 189; Pen Register Act, 206; remedies provided by, 219; Stored Communications Act, 205; Wiretap Act, 204
Experian, 21, 70, 112, 118, 231n49
Fair and Accurate Credit Transactions Act (FACTA, 2003), 113, 120
Fair Credit Reporting Act (FCRA, 1970), 67–68, 84, 112–113, 206
Fair Information Practices, 104–105, 107, 120, 152–153
False light, 60
Family court proceedings, 130
Family Educational Rights and Privacy Act (FERPA, 1974), 68
FBI: access to student records, 171; Carnivore (DCS1000), 172; domestic surveillance, 180; formation of, 178–179; Hoover’s leadership, 178; information collection by, 169; internment of Japanese Americans, 182; McCarthyism, 183–184; predecessor, 183; purchase of private-sector databases, 169; rap sheets, 143–144; surveillance of King, 185, 199, 258n93; surveillance practices, 74, 171; United States Department of Justice v. Reporters Committee for Freedom of the Press, 143–144; USA PATRIOT Act (2001), 174; wiretapping by, 185, 199
Federal Communications Act (1934), 199, 203
Federal Election Campaign Act (FECA), 137–138, 251n94
Federal Trade Commission (FTC): complaints about credit reporting, 51, 236n79; complaints from single customers, 112; on identity theft, 111–112, 114; limitations, 73, 108; privacy policies, 72, 240n74; In re
Guess.com, Inc., 108; in regulating collection and use of personal information, 108; unfair and deceptive practices, 72–73; U.S. West, Inc. v. Communications Commission, 95–96
Fiduciary relationship, 102–104, 244n25
Fifth Amendment, 63–64, 188, 195–197, 218, 264n14
Financial records, 64, 206–207, 239n68, 240n78
First Amendment, 62–63, 155–161, 176–177, 220, 256n53
Flaherty, David, 32
Florida: access to public records, 137; results of 2000 presidential election, 170
Florida Star v. B.J.F, 157, 159
Florida v. Riley, 200
Focus USA, 22
Ford, Gerald, 147
Ford Motor Credit Company, 118
Forsher v. Bugliosi, 144
Foucault, Michel: Discipline and Punish, 30; on the Panopticon, 30–31, 98–99; surveillance and internalization of social norms, 35
Fourth Amendment, 188–209; applicability, 188–189, 195–200; architecture of, 188–209; bodily intrusions, 196–197; Boyd v. United States, 195–196, 197; businesses, 260n26; electronic surveillance, 199–200; enforcement, 189; exclusionary rule, 189, 210; government as equal of everybody else, 215; government’s ability to glean information about one’s associations, 176, 256n53; inferences of potential culpability, 261n50; inviolability of the person, 196–197; opening mail, 225; per se warrant rule, 189; physical intrusion conception of invasion of privacy, 196–198; privacy, 63–64, 190–191, 195–200; privacy protections, 186, 189–192; probable cause, 174, 189, 202, 203, 207; prohibitions on compelling disclosures, 191–192; reasonable expectation of privacy test, 198, 200–202; replacement by privacy policies, 209; search and seizure, 188–189, 192–193, 196–197, 220; secrecy paradigm, 64, 190, 198–202; statutory regime surrounding, 202–209, 222; stored communications, 204, 262n102; subpoenas, 195–196, 200–201; Supreme Court’s conceptualization of privacy, 190–191, 195–202, 215, 222; Supreme Court’s interpretation,
Fourth Amendment (Continued)
227; Terry v. Ohio, 189; third party doctrine, 201–202, 207–208; third party records, 10; type of information vs. third party possessing it, 208, 213, 215; warrant requirement, 189, 192–195, 202, 219; wiretapping, 197, 203; Zurcher v. The Stanford Daily, 220
Frankfurter, Felix, 183
Franklin, Benjamin, 225
Freedom of association, 63, 176, 177
Freedom of Information Act (FOIA, 1966), 134–135, 136
Freedom of information laws (FOIAs): access to public records, 253n42; commercial users, 150, 151–152; exemptions, 135–136, 143–144, 146; federal, 134–135; information collection, 151–152; invasion of privacy, 135; Massachusetts, 252n24; reverse-FOIA lawsuits, 250n69; state laws, 135–136, 150–151, 250n59; Wald on, 150
Freedom of speech, 157–161
Frequent shopper programs, 52
FTC. See Federal Trade Commission (FTC)
Gandy, Oscar, 32, 82, 181
Garrow, David, 185, 186
Gartner, Inc., 111
Gellman, Robert, 136
General Electric, 51
General Motors, 16–17
General warrants, 193
GeoCities, 53
Georgia: access to public records, 137
GeoVoter software, 20
Gerety, Tom, 212
Gertner, Robert, 77
Global Regulatory Information Database (GRID), 21
Globe Newspaper Co. v. Superior Court, 155
Goldman, Eric, 80–81
Goldman v. United States, 198
Gormley, Ken, 56
Gossip, 57, 74
Gostin, Lawrence, 81–82
Government: in 1984 (Orwell’s novel), 29; access to digital dossiers, 10; Big Brother and, 7; control of, 193–194; duty to provide public information, 158; as equal of everybody else, 215; illumination of government functioning, 150, 152, 156; personal information, 152; personal relationship with, 100; power of, 148; responsibility for identity theft, 118–119; sanctioning disclosure of information made public, 158–159; transparency, 141, 151–152; use restriction laws, 159–160. See also government information collection; public records; United States government
Government data protection boards, 233n22
Government information collection, 165–187; abuses of, 186–187; anonymity, 176–177; automated investigations, 180–182; Baird v. State Bar, 176; Big Brother, 175–177; changing purposes and uses of information, 184–185; compelling disclosure of memberships, 176; computer matching by agencies, 181; control of, 211; democracy, 175–176; effects of September 11 attacks, 5; by FBI, 169; freedom of association, 176, 177; harms caused by, 175–186, 179; information from private-sector databases, 168–175; by interviewing, 212, 215; by IRS, 169; Kafka metaphor for invasion of privacy, 177–186; lapses, 179–180; leaks, 179–180; mechanisms for controlling, 217–221; minimization of, 211, 219; New Deal, 14; opening mail, 225; overreaction in times of crisis, 182–184; particularization of, 211, 219; particularized suspicion in, 174, 181; powerlessness, 178; probable cause, 174; procedural requirements for obtaining information, 202–203; profiling, 180–182; requests for private-sector data, 170, 172, 206; restrictions on, 211–217, 218, 219; self-determination, 175–176; sharing of records between agencies, 180–181, 221–222; state and local governments, 229n2(ch.2); third parties sources, 165–168, 187, 202–209, 215–216, 221; threats to privacy, 202; totalitarianism, 175; vulnerability, 178, 179–180; Whalen v. Roe, 157. See also architecture for governing government information collection
Gramm-Leach-Bliley Act (GLB, 1999), 70, 108, 239n68, 240n78
Great Universal Stores, 70
Greiding v. Davis, 156
GRID (Global Regulatory Information Database), 21
Griswold v. Connecticut, 64, 65
Guess.com, Inc., 108
Hamilton, Alexander, 225
Harlan, John Marshall, 198
Harm without victimization, 119
Health Insurance Portability and Accountability Act (HIPAA), 69–70, 208
Henry, Patrick, 193
Hippo Direct, 22–23
HireCheck, 47
HIV, 66–67
Hollerith, Herman, 14
Holmes, Oliver Wendell, 141, 189, 199
Hoofnagle, Chris, 236n79
Hoover, J. Edgar, 178, 183–184, 184–185, 199
Hospitals, 154
Human dignity, 39
Human judgment, 34, 48–49
Huxley, Aldous: Brave New World, 40, 191

IBM, 14
Identity systems, 147–148, 173
Identity theft, 109–123; architecture and, 115–123; architectures of vulnerability, 99, 115; calculating damages from, 107; Cate on, 114; combating, 119–123; convictions for, 111; credit card fraud, 110–111; credit reporting, 109, 112; culprits, 118–119; defined, 109; digital dossiers, 110, 115; disclosure of public records, 146; eradication of, 123; examples, 109; Fair Credit Reporting Act (FCRA), 112–113; Federal Trade Commission on, 111–112, 114; growth of, 110; harms caused by, 110, 119; identifying existence of, 111–112, 121; Identity Theft and Identity Theft and Assumption Deterrence Act (1998), 111; invasion conception of privacy, 111–115, 123; as a manufactured product, 119; opening new accounts, 122; participation in uses of personal information, 118, 120; passwords as identifier, 121, 122; personal responsibility for avoiding it, 114–115; prosecution of, 111; questions about oneself as identifier, 121–122; responsibility for, 118–119; root causes, 119–120; sale of credit reports for use in, 55; significance of the term, 115; Social Security numbers (SSNs), 115–118, 146, 246n79; traditional legal view of, 115; varying methods of personal identification, 121–122; victims of, 111, 112; vulnerability to, 116

Immigration Reform and Control Act (1986), 148
In re Crawford, 151
In re DoubleClick, Inc. Privacy Litigation, 68–69

In re Guess.com, Inc., 108
Inalienability (“immutable”) rules, 77, 79, 91, 241n15
Incorporeal injuries, 197
Indoctrination, 40
Inequalities in knowledge, 86–87, 97, 102, 103, 106
Inequalities in power, 91, 103
Infomediaries, 241n10
Information, 48–49, 74, 143
Information Age hermits, 217
Information brokers, 153, 241n10
Information collection: in architecture conception of privacy, 121; as a benefit to subscribers, 52; bots/crawlers/spiders, 25–26; businesses, 227; Conde Nast Publications, Inc., 52–53; consent to, 51–52; curtailment of, 92; discount cards, 52;DoubleClick, 24–25; freedom of information laws, 151–152; frequent shopper programs, 52; by General Electric, 51; Internet, 23–24; marketing, 34; Motion Picture Association of America, 25–26; need for federal agency to regulate collection and use of personal information, 108–109; powerlessness, 51; problem with, 149; Recording Industry Association of America, 25–26; relationship between individuals and information collectors, 101–105; spamming, 26; spyware, 25; in United States, 51; warranty registration cards, 52; web bugs, 25. See also government information collection

Information flow: business-to-business, 13–123; business-to-government, 165–228; credit reporting, 80; effects of September 11 attacks, 5; enforcement problems, 95; freedom of speech, 157–161; government-to-business, 127–161; inequalities in, 91; Kafka metaphor for invasion of privacy, 91–92; lack of awareness of, 75; privacy problem caused by public records, 149; support for developing information gathering technologies, 173–174; systemic problems, 96; tort law, 58–59; types, 3

Information highway, 233n12

Information privacy law: circuit courts, 254n38; collective actions, 75, 95; digital dossiers, 56, 75; Doe v. Southeastern Pennsylvania Transportation Authority (SEPTA), 66–67; effectiveness of, 223; Gormley on, 56; infringements of, 75;
Information privacy law (Continued) relationships with bureaucracy, 91–92; right to information privacy, 157, 254n58; right to privacy, 75; secrecy paradigm, 143; shortcomings, 74–75; technology and, 74, 197–198, 201; types of law contained in, 56; Whalen v. Roe, 65–66, 156–157, 254n58. See also privacy law
Information systems, 98
Inhibition, 34
Inness, Julie, 212
Intellectual exploration, 25
Internet: anonymous speech, 177; bots/crawlers/spiders, 25–26; cattleyard on, 24; Children’s Online Privacy Protection Act, 70, 71; clickstream data, 24; cookies, 24; digital rights management (DRM), 25; information collection methods, 23–24; investment in privacy, 81; persistence of data on, 26; personal information on, 22; personalized home pages, 168; public records, 117, 132; regulation of, 99; Schwartz on, 32; as source of government information, 167–168; spamming, 26; spyware, 25; surveillance on, 32; targeted marketing, 23; telescreens and, 31, 32; web bugs, 25; websurfing, 23–24. See also ISPs (Internet service providers)
Interviewing, 212, 215
Intimacy, 212
Intrusion upon seclusion, 59, 62, 144–145, 238n23
Invasion conception of privacy, 93–97; architecture conception compared to, 100–101, 186; defined, 8; digital dossiers, 8; effectiveness, 95; identity theft, 111–115, 123; individual remedies in, 100; limitations, 100–101; a personal right, 94, 97; primary remedy, 93, 100; privacy protections, 94; problem with, 146; reactive nature, 94; tort action for damages, 93; as traditional view of privacy, 2, 8
Invasion of privacy: American Express Co., Dwyer v., 89; Big Brother metaphor, 7–8; criminal law, 95; defined, 8; digital dossiers, 8; freedom of information laws, 135; Kafka metaphor, 8–9; physical incursion conception, 196–198; tort law, 57–62, 94
Inviolability of the person, 196–197
IP addresses, 205–206
IRS, 169
ISPs (Internet service providers), 167, 172, 177, 201, 204–205
Jacoby, Stephen, 52
James, Henry: Portrait of a Lady, 45
Janger, Ted, 225
JetBlue Airlines, 171
Johnson, Lyndon, 199
Johnson, Mark, 28
Junk mail, 231n33
Jurors, 153–154, 248n16
Justice Department, 169, 262n84
Juvenile offenders’ names, 157–158
Kafka, Franz: Trial, 8–9, 36–42, 55, 67, 191; where Orwell meets, 42
Kafka metaphor for invasion of privacy: aggregation effect, 149; aptness of, 8–9, 36–42, 55, 226; architectures of vulnerability, 99; defined, 81; digital dossiers, 72; government information collection, 177–186; information flow, 91–92; powerlessness, 96; transparency, 151
Kahn, Jonathan, 238n19
Kang, Jerry, 32–33, 78–79, 241n15
Karas, Stan, 44–45
Karst, Kenneth, 48
Katz, Neal, 98, 100, 119
Katz v. United States, 198
Kentucky: access to public records, 137
Kerr, Orin, 262n84
King, Martin Luther, Jr., 180, 185, 199, 258n99
Knowledge and power, 74
Lakoff, George, 28
Landlords, 167
Law: common law, 131–134; construction of privacy, 224–228; contribution to creation of digital dossiers, 227; ideological drift in, 151; loss of privacy, 224–225; privacy protection and, 224, 228; property law, 56; technology, 224. See also constitutional law; contract law; criminal law; information privacy law; Megan’s Laws; privacy law; tort law
Law enforcement: bureaucratization, 179; Communication Assistance for Law Enforcement Act (1974), 174; particularization, 211; pressures to succeed, 179; restrictions on government information collection, 211–212; rise of, 178–179;
third parties in, 212; third party records in, 166–167, 176; warrants, 194
Lessig, Lawrence, 79, 98, 99
Lexis-Nexis, 80
Liberty, 175
Literature, 28
Litman, Jessica, 244n30
“Little Brothers,” 32, 234n25
Lochner era, 196–198
Lochner v. New York, 196
Loewy, Arnold, 189
LoPucki, Lynn,
Lochner v. New York, 196
Los Angeles Police Department v. United Reporting Publishing Co., 158, 160
Lotus Corporation, 80
Louisiana: access to public records, 137
Lyon, David, 32

Madison, James, 141, 193–194
Mail, 196, 204–205, 225, 231n33
Mail order catalogs, 17
Mailing lists, 19, 22–23, 84
Market-based solutions to privacy problems, 76–92; aggregation effect, 87–88; bargaining power, 82–85; contract law, 81–82; contractual default rules for ownership of personal information, 77–79; customization of privacy preferences, 85–86; deficiencies in, 81–87; future uses of personal information, 88; individual choice, 90–91; inequalities in knowledge, 86–87; Lessig on, 79; personal information, 91; property rights, 76–79, 88–90; self-regulation, 79–81, 82, 91; value of personal information, 87–90
Marketing, 19; categorization of people, 19, 22; Census Bureau connections, 230n27; cluster marketing, 18–19; information collection, 34; junk mail, 231n33; mail order catalogs, 17; mailing lists, 19; mass marketing, 16; mass media, 17; motives in requesting public records, 151; psychographic information, 18–19. See also direct marketing; targeted/database marketing; telemarketing
Markets, 87, 91, 92, 216
Mass media, 17
Massachusetts: freedom of information laws, 232n24; “street lists,” 128
MATRIX (Multi-State Anti-Terrorism Information Exchange), 170
McCarthy, Joseph R., 183–184
McNealy, Scott, 224
McVeigh, Tim, 54
McVeigh v. Cohen, 54
Medical information: cancellation of bank loans to cancer patients, 55; disclosure by physicians, 214; disclosure of sex lives of psychotherapy patients, 54–55; Doe v. Southeastern Pennsylvania Transportation Authority (SEPTA), 66–67; Health Insurance Portability and Accountability Act, 69–70; third party doctrine, 207–208; Whalen v. Roe, 65–66
Medical Information Bureau, 20
Megan’s Laws, 130, 145, 252n21
Melvin v. Reid, 144
Mere evidence rule, 218
Metaphors, 27–28
Metromail Corporation, 18, 53, 70
Microsoft, 72–73, 108
Miller, Arthur: The Assault on Privacy, 147
Mother’s maiden name, 121, 131
Motion Picture Association of America (MPAA), 25–26
Motor vehicle records, 138
Movers, recent, 22
Mowshowitz, Abbe,
MSN network, 172
Multi-State Anti-Terrorism Information Exchange (MATRIX), 170
Murder, 54, 147
Murphy, Richard, 78

NAACP v. Alabama, 156
Names and addresses, disclosure of, 146
NASA, 41
National Demographics and Lifestyles Company, 52
National identity systems, 147, 148, 173
Nazi Germany, 148, 182
New Deal, 14
New employees, 15, 148, 170, 174
Newspapers, 57, 81, 225–226
1984 (Orwell), 7, 74, 91, 231n1, 232n2. See also Big Brother
Nissenbaum, Helen, 44
Nixon, Richard, 185, 199
Nixon v. Warner Communications, Inc., 133, 254n58
Nock, Steven, 21
Nondisclosure, 64
Northwest Airlines, 171

OECD (Organization for Economic Coop-
eration and Development), 105, 106
Ohio: Public Records Act, 135
Olmstead v. United States, 197–199
Omnibus Crime Control and Safe Streets Act (1968), 203–204
Opt-out systems, 70–71, 83–84, 84, 105–106
Organization for Economic Cooperation and Development (OECD), 105, 106
Orwell, George: 1984, 7, 74, 191, 231n1, 231n2 (see also Big Brother); where Kafka meets, 42; Wrong on, 30
P-TRAK Personal Locator, 80
Palmer, A. Mitchell, 183
Palmer Raids ("Red Scare"), 183
Panopticon, 30–31, 32, 98–99
Particularization, 211, 219
Passwords, 116, 121, 122, 127
Patient-physician relationship, 102, 103, 214, 263n122, 263n123
Paul P. v. Verniero, 145
Payroll records, 252n24
Pen Register Act, 204, 205–206
Pen registers, 201, 205
Pennsylvania: Right to Know Act, 135
Per se warrant rule, 189, 219
Personal information: affiliate sharing of, 70; “angel” is “demon” customers, 50; black-and-white view of, 143, 159; bureaucracy, 9, 39; in census data, 13–14; compensation for, 89; curtailing collection of, 92; disclosure of, 43, 106; discrepancies in, 122–123; explanatory details, 235n61; forced disclosure of, 156; future uses of, 88; in government bureaucracies, 178; government functioning, 152: as identifier, 121; illumination of government functioning, 150, 152, 158; inaccuracies in, 121; incremental release of, 87–88; on the Internet, 22; market-based solutions to privacy problems, 91; national database of, 147; need for federal agency to regulate collection and use of personal information, 108–109; opportunity to assert privacy interest, 138; participation in uses of, 105–106, 113, 118, 120, 149, 223; personal control of, 43, 76–77, 106; potential for abusing, 152; in private sector, 240n69; private sector handling of, 117, 148; processing of, 105; prohibitions on disseminating, 122; property rights to, 76–79, 87, 241n3; In re Guess.com, Inc., 108; relinquishment of full title to, 88, 90; responsibility for, 120; sales of, 53–55; security practices, 108, 121; trade in, 90; use restriction laws, 71, 152–154; value of, 87–90. See also contractual default rules for ownership of personal information
Personal Responsibility and Work Opportunity Reconciliation Act (1996), 174
Philadelphia Police Department (PPD), 180
Phone numbers, 64, 80, 166, 201
Photographs, 57, 81, 225–226
Physical incursion conception of invasion of privacy, 196–198
Pointdexter, John, 168, 169
Police: coercion and violence by, 190, 191; interviewing by, 215; the most efficient, 141; national police, 221; objectivity of, 261n50; Philadelphia Police Department (PPD), 180; professionalization of, 178; public disclosure of payroll records, 146; warrants, 261n50
Political contributions, 137–138
Portrait of a Lady (James), 45
Posner, Richard, 28, 78
Pound, Roscoe, 183, 237n14
Power: Big Brother, 40; bureaucracy, 39–41, 91; of businesses, 148; effectiveness of individual remedies, 97, 100, 107; of government, 148; inequalities in information transfers, 91; information and, 74; in Kafka’s Trial, 40–41, 191; knowledge and, 74; social relationships, 216; system of records, 216. See also bargaining power
Powerlessness: architectures of vulnerability, 99; bureaucracy, 9, 48; computer databases, 41, 47–48; digital dossiers, 149; government information collection, 178; harms created by, 108; inequalities in knowledge, 97; information collection, 51; Kafka metaphor for invasion of privacy, 96; privacy and, 49–50, 51
Powers, Richard, 184
PPD (Philadelphia Police Department), 180
Princeton University, 118
Privacy: accessibility of information, 161, 213; active elimination of, 225; Big Brother and, 31, 43; bodily intrusions, 196–197; Cohen on, 176; collection/use of personal information, 6, 148; computerization, 15; constitutive privacy, 175–176; construction of, 224–228; contextual nature, 212–213; control of use of information, 143, 148; death of, 73, 224, 227; definition of, 212; desire for, 91, 96;
disclosure of personal information, 43;
financial records, 64, 206–207; First Amendment, 62–63, 155–161; Fourth Amendment, 63–64, 190–191, 195–200; freedom of association, 63; "going price" of, 80; importance to people, 82; incorporeal injuries, 197; Information Age hermits, 217; infringements of, 44; institutional interests in, 191; intimacy and, 212; lack of, 176; loss of, 224–225; McNealy on, 224; natural occurrence of, 224; police coercion and violence, 190, 191; powerlessness and, 49–50, 51; preferences, 82, 85–86; as a property right, 88–90, 243n49; protections provided by, 48; in public, 44; reasonable expectation of, 198, 200–202; risk and, 213–214; Rosen on, 48; Schwartz on, 97, 175–176; secrecy paradigm, 8, 42–44, 64; social and legal structure, 97–101; social relationships, 213–216; state protections, 62; stated concerns compared to behavior, 80–81, 82, 96–97; Supreme Court’s conceptualization of, 190–191, 195–202, 215, 222; term not in U.S. Constitution, 62; threats to, 32, 161, 197–198, 201, 202, 222, 224, 225–226; transparency, 140–143, 150–154; use restriction laws, 150; ways of understanding, 7; in well-functioning markets, 87; Westin on, 76; zero privacy, 224. See also architecture conception of privacy; invasion conception of privacy; right to privacy
Privacy Act (1974): amendments proposed by author, 154; Andrews v. Veterans Administration, 136–137; applicability, 136; Freedom of Information Act, 136; limitations, 68, 136–137, 154, 221–222; provisions, 136; "routine use" exception, 136, 154, 181; sharing of records between government agencies, 180–181; Social Security numbers, 116; system of records, 214
Privacy law: historical context, 101; personal relationships with business and government, 100; right of access to public records, 155; Right to Privacy (Warren and Brandeis), 57–59, 93–94, 100–101, 225–226. See also information privacy law
Privacy policies: Amazon.com’s, 172–173; Bennet on, 71; changes in, 83; contracts compared to, 82–83; difficulties with, 82; EBay’s, 173; enforcement mecha-
isms, 83; feasibility of personal customization, 86; Federal Trade Commission (FTC), 72, 240n74; incentives for adopting, 91; lack of interest in, 82; Lessig on, 79; model statement, 173; as replacement for Fourth Amendment, 209; similarities among, 86; Smith on, 53; “trustmark” for, 173; violations of, 72–73, 108
Privacy preferences, 82, 85–86
Privacy Protection Act (1980), 220
Privacy protections: architecture conception of privacy, 97–123; Boyd v. United States, 63–64, 197; competition in the marketplace, 82; credit reporting agencies, 117; European Union vs. U.S., 67, 106–107; Fair Information Practices, 104–105; Fourth Amendment, 186, 189–192; inequalities in knowledge, 86–87; in invasion conception of privacy, 94, 97; isolated infractions, 123, 148, 161; law and, 224, 228; markets and, 91, 92, 216; minimum floor for, 138–139, 154; nondisclosure, 64; OECD guidelines, 105, 106; paper records, 139; participation in uses of personal information, 123, 223; personal relationships with business and government, 100; Privacy Protection Act (1980), 220; private sector handling of personal information, 117, 148; property rights, 100, 243n49; public records, 139; records not protected at all, 208–209; requirements for viable protection, 101; social design, 226; social structure, 148; state laws compared to federal laws, 113; through architecture, 186; type of information vs. third party possessing it, 208
Private-sector databases, 16–21; Big Brother, 32; ChoicePoint’s, 169–170; government data protection boards, 233n22; government purchase of data from, 168–175; government requests for data from, 170, 172; as “Little Brothers,” 32, 234n25; mass marketing, 16; public records, 127, 131, 149; as salable assets, 19; targeted/database marketing, 16–19
Probable cause: architecture for governing government information collection, 226; Fourth Amendment, 189, 207; government information collection, 174; relevance vs., 203; warrants, 202
Profiling, 5–6, 168–169, 171, 180–182, 236n74
Property law, 56
Property rights: alienability of property, 87; bargaining power, 85; consent, 85; in defective markets, 90; initial entitlements, 78; to personal information, 76–79; 241n3; privacy as one, 88–90, 243n49; privacy protections, 100, 243n49; Westin on, 77

Property tax assessment records, 128

Prosser, William, 58

Protective orders, 133–134

Psychographic information, 18–19

Psychotherapy patients, 55

Public disclosure: abortion doctors, 147; accessibility of information, 161; Andrews v. Veterans Administration, 136–137; black-and-white view, 143, 159; Briscoe v. Reader’s Digest Ass’n, 144; computer databases, 59; Cox Broadcasting Corp. v. Cohn, 145, 157; defined, 59; disclosure of information by physicians, 214; Forsher v. Bugliosi, 144; juvenile offenders’ names, 157–158; Melvin v. Reid, 144; motives of requesters of public records, 151; NAACP v. Alabama, 156; names and addresses, 146; Paul P. v. Verniero, 145; police payroll records, 146; prohibitions on compelling, 191–192; protective orders, 133–134; rape victim’s name, 157–158; redaction before, 152–153; Restatement of, 144; “routine use” exception in Privacy Act (1974), 136, 154; Russell v. Grecoire, 145; sanctioning disclosure of public information, 158; Scheetz v. Morning Call, Inc., 145; Social Security numbers, 151, 156; specifying purpose for, 152–153; teacher salaries, 146; Walls v. City of Petersburg, 145

Public office, 142

Public records, 127–139; access to (see public records, access to); arrest records, 128–129, 141, 145; bankruptcy records, 129–130, 246n81; birth records, 127; California, 137; Colorado, 137; commercial use of, 156; common law, 132–134; compilations of, 131, 154, 249n32; confidentiality, 157; conviction records, 130, 145; data in, 127–131, 132; digitalization of, 131–132; disclosure of, 143–150; divorce records, 130; Dunhill v. Director, District of Columbia Department of Transportation, 151; family court proceedings, 130; Florida, 137; Georgia, 137; government power, 148; information brokers, 153; on the Internet, 117, 132; Kentucky, 137; laws governing, 132–139; limits on disclosure, 137–139; Louisiana, 137; Massachusetts, 128, 252n24; Megan’s Laws, 130, 145, 252n21; motives of requesters of, 151; motor vehicle records, 138; Nixon v. Warner Communications, Inc., 133, 254n58; number of federal government databases, 15; Ohio, 135; Pennsylvania, 135; political contributions, 137–138; Privacy Act (1974), 68, 136–137; privacy problem caused by, 149; privacy protections, 139; private-sector databases, 127, 131, 149; property tax assessment records, 128; protective orders, 133–134; public disclosure, 137–139; public-sector databases, 13–16; redaction before disclosure, 152–153; Reno v. Condon, 138; restricting contents of, 153; sales of data from, 154; secrecy paradigm, 143; security, 157; sex offender records, 130, 145; state records, 16, 138–139; “street lists,” 128; threats to privacy, 161; trends affecting, 127; true information in, 157–158; use restriction laws, 132–139, 152–161; vital records, 128; voting records, 128, 137; worker’s compensation records, 128. See also court records; freedom of information laws (FOILs); government

Public records, access to, 140–161; businesses, 156; commercial speech, 158; conditional access, 158–160; court records, 155–156; Cox Broadcasting Corp. v. Cohn, 157, 159; criminal trials, 155; First Amendment, 155–160; Florida Star v. B.J.F., 158–159; Globe Newspaper Co. v. Superior Court, 155; illumination of government functioning, 150, 152, 156; judicial records, 249n44; juvenile offenders’ names, 157–158; Los Angeles Police Department v. United Reporting Publishing Co., 158; membership lists, 156; NAACP v. Alabama, 156; pre-access vs. post-access restrictions, 158–159; public domain, 4–5, 127; public records law, 132–134; Publicker Industries, Inc. v. Cohen, 155–156; purpose for, 150–151; restrictions on, 137–138, 152, 158–160, 227; Richmond Newspapers, Inc. v. Virginia, 155; technology, 13; vulnerability, 146

Publicker Industries, Inc. v. Cohen, 155–156

R. L. Polk & Co., 18

Rape victims, 134, 157–158
RDC (Regulatory DataCorp), 21
RealNetworks, Inc., 53
Reasonable expectation of privacy: architecture for governing government information collection, 213; Fourth Amendment, 198, 200–202; Harlan on, 198; ISPs, 201; privacy, 198, 200–202; secrecy paradigm, 200–202; Smith v. Maryland, 64, 263n4
Recording Industry Association of America (RIAA), 25–26
Redaction before disclosure, 152–153
Regan, Priscilla, 181
Regulatory DataCorp (RDC), 21
Reidenberg, Joel, 71, 84–85, 98, 99, 105
Remsburg v. Docusearch, Inc., 54
Reno v. Docussearch, Inc., 54
Reno v. Condon, 138
Reputations, 21
Richmond Newspapers, Inc. v. Virginia, 155
Right to Financial Privacy Act (RFPA, 1978), 206
Right to privacy: Cate on, 94; constitutional law, 62, 64–67, 75; enforcement, 97; a personal right, 94; Right to Privacy (Warren and Brandeis), 57–59; tort law, 94; warrants, 195; Whalen v. Roe, 156–157
Right to Privacy (Warren and Brandeis): incoporeal injuries, 197; photography, 57, 81, 225–226; Pound on, 237n14; privacy law, 57–59, 93–94, 100–101, 225–226; technology, 57, 74, 225–226
Roe v. Wade, 65
Rosen, Jeffrey, 48
Rotenberg, Marc, 104, 105, 106
RR Donnelley, 18
Russell v. Gregoire, 145
Rwanda: national identification system, 148
Safire, William, 169, 199
Samuelson, Pamela, 87, 182
Sanford, Bruce, 238n23
Scheetz v. Morning Call, Inc., 145
Schools, 154
Schrecker, Ellen, 183
Schwartz, Paul, on: bureaucracy, 38–39; computer databases, 33; consent and websites, 85; constitutive privacy, 175–176; digital surveillance, 32; Fair Information Practices, 105; Federal Trade Commission privacy policies, 73;
Gramm-Leach-Bliley Act, 70–71; personal information in the private sector, 240n69; privacy, 97; privacy preferences, 82; state data protection laws, 137
Secrecy paradigm: abandonment of, 161; court cases, 143–145; defined, 8, 42; definition of privacy, 212; Fourth Amendment, 64, 190, 198–202; harms addressed, 43; information privacy law, 143; public records, 143; reasonable expectation of privacy, 200–202; Supreme Court’s conceptualization of privacy, 190, 198–202; surveillance and, 8, 42–44; third party doctrine, 201–202
Secret Service, 174
Seidman, Louis Michael, 189
SeisInt, Inc., 170
Self-censorship, 33, 34, 35
Self-determination, 175–176
Self-incrimination, 63–64, 188, 218
Separation of powers, 193–194
September 11 attacks, 5, 170, 173
Sex offender records, 130, 145
Shaeffer, Rebecca, 147
Shibley v. Time, Inc., 61
Simitis, Spiros, 97, 181–182
Sixth Amendment, 188
Slobogin, Christopher, 214
Smith, H. Jeff, 49, 53
Smith v. Daily Mail, 157–158
Smith v. Maryland, 64, 201, 210, 217, 263n4
Sobel, Richard, 148
Social conditioning in Brave New World, 40
Social control, 32
Social design, 226
Social relationships, 213–216
Social Security Administration, 14
Social Security numbers (SSNs): architecture and, 116; availability of, 146, 148; confidentiality, 248n17; disclosure of, 151, 156; Greiding v. Davis, 156; as identifier, 115–116, 121, 154, 169; identity theft, 115–118, 146, 246n79; as linking mechanism, 14–15; as magic key, 116; in murder of Boyer, 54; in murder of Shaeffer, 147; as passwords, 116; Princeton University’s use of, 118; Privacy Act (1974), 116; private-sector usage, 154;
Social Security numbers (Continued)

In re Crawford, 151; redacting before disclosing public records, 153; refusal to disclose, 116; sale and disclosure of, 117; voter registration, 156

Social structure, 148

Social transactions, 142

Southeastern Pennsylvania Transportation Authority (SEPTA), Doe v., 66–67

Sovenn, Jeff, 84, 106

Spyware, 26

Spiders (on the Web), 25–26

Spyware, 25

SSNs. See Social Security numbers (SSNs)

Staples, William: Culture of Surveillance, 31

Statutory law, 56, 67–72, 202–209, 210, 222

Steiker, Carol, 221

Stored communications, 204–205, 262n102

Stored Communications Act, 204–205

“Street lists,” 128

Student records, 68, 171

Stuntz, William, on: Boyd v. United States, 64, 218; institutional interests in privacy, 191; post-collection use of data, 221; privacy in administrative states, 189–190, 191; subpoenas, 202–203; warrants, 194

Subpoenas: architecture for governing government information collection, 219–220; Boyd v. United States, 195–196

Degnan on, 202; grand jury subpoenas, 202–203; issuance of, 202; problems with, 203; quashing, 203, 220; as replacement for warrants, 209; Stuntz on, 202–2–3; United States v. Miller, 200–201; warrants, 202–203, 220

Sundby, Scott, 190, 192

Sunlight, 141

Supermarket sales, 20

Surveillance: Big Brother and, 34–35; in Britain, 99; Communication Assistance for Law Enforcement Act (1974), 174; computers, 42; conformity, 34; dataveillance and, 33; domestic surveillance, 180; eavesdropping, 198; Electronic Communications Privacy Act, 68; electronic surveillance, 199–200; FBI practices, 74, 171; Foucault’s analysis, 35; human judgment and, 34; inhibition, 34; internalization of social norms, 35; on the Internet, 32; non-taboo information, 35, 43; secrecy paradigm and, 8, 42–44; self-censorship and, 33, 34, 35; of welfare recipients, 41–42. See also electronic surveillance; wiretapping

Swire, Peter, 84

System of records, 211–217, 221

Talley v. California, 176–177

Targeted/database marketing: appropriation and, 61; computer databases, 18; General Motors, 16–17; Internet, 23; panopticism of, 32; percent U.S. companies using, 19; purpose, 16

Teacher salaries, 146

Technology: access to public records, 131; law and, 224; Right to Privacy (Warren and Brandeis), 57, 74, 225–226; support for developing information gathering technologies, 173–174; threats to privacy, 197–198, 201, 224, 225–226

Telemarketing, 19, 69

Telephone companies, 262n102

Telephone Consumer Protection Act (TCPA, 1991), 69

Telescreens, 29–30, 30–31, 32

Terrorism Information Awareness. See Total Information Awareness (later Terrorism Information Awareness)

Terry v. Ohio, 189


Third party doctrine, 201–202, 207–208

Thumbprints, 166

Torch Concepts, 171

Tort law, 57–62; aggregation effect, 95; computer databases, 61–62; disclosure of information by physicians, 214; false light, 60; flow of personal information, 58–59; information flow, 58–59; information privacy law, 56; intrusion upon seclusion, 59, 62, 144–145, 238n23; invasion conception of privacy, 93; invasion of privacy in, 94; Prosser on privacy torts, 58; right to privacy, 94. See also appropriation; confidentiality; public disclosure

Total Information Awareness (later Terrorism Information Awareness): closeness to, 175; funding for, 169; logo, 169; motto, 169; Poindexter and, 168; profiling, 5–6, 168–169; renaming, 169; sponsor, 5

Totalitarianism, 175

Trade secrets, 250n69
Trans Union Corp., 21, 112
Transparency: confidence, 151; defined, 140; enabling information collection, 142; functions, 140–142; government, 141; Kafka metaphor for invasion of privacy, 151; privacy, 140–143, 150–154; public officials, 142; social transactions, 142; use restriction laws, 150; from window on government to window on individuals, 151–152
Transparent Society (Brin), 73
Trash, privacy of, 200
Travel agent records, 166
Trial (Kafka), 8–9, 36–42, 55, 67, 191. See also Kafka metaphor for invasion of privacy
Truste.com, 173
Trustee relationship, 102
TRW, Inc. v. Andrews, 112–113

Unfair and deceptive practices, 72–73
Union Pacific Railway Company v. Botsford, 196–197
United States: information collection in, 51
United States Army, 180
United States Constitution, 62, 157, 254n58. See also constitutional law; Fifth Amendment; First Amendment; Fourth Amendment; Sixth Amendment
United States Department of Defense, 5–6
United States Department of Health, Education, and Welfare (HEW), 15, 104
United States Department of Justice, 169, 262n84
United States Department of Justice v. Reporters Committee for Freedom of the Press, 143–144
United States government, 41, 67, 147, 171. See also government information collection
United States Secret Service, 174
United States Supreme Court: 1984 citations, 232n1, 232n2; Big Brother citations, 233n3, 233n12; conceptualization of privacy, 190–191, 195–202, 215, 222; Information Age hermits, 217; Lochner era, 196–198
United States v. Miller, 64, 200–201, 210, 217
“Unknown Citizen” (Auden), 235n62
U.S. West, Inc. v. Communications Commission, 95–96
USA PATRIOT Act (2001), 174, 205–206
Use restriction laws: commercial speech, 159–160; consent, 154; defense of, 159–160; digital dossiers, 150; distinction between pre- and post-access restrictions, 158–159; First Amendment, 155–161; Los Angeles Police Department v. United Reporting Publishing Co., 160; personal information, 71, 152–154; privacy, 150; public records, 132–139, 152–161; transparency, 150
Veterans Administration, Andrews v., 136–137
Victimization, 119
Video Privacy Protection Act (VPPA, 1988), 69, 207
Vital records, 128
Volokh, Eugene, 96
Voter registration, 156
Voters, 20, 142
Voting records, 128
Vulnerability: access to public records, 146; calculating damages from being made vulnerable, 107–108; digital biography, 146; digital dossiers, 149; government information collection, 178, 179–180; harms created by, 108; to identity theft, 116; technology and, 101. See also architectures of vulnerability

Wald, Patricia, 150
Walls v. City of Petersburg, 145
Warrants: Amar on, 192; architecture for governing government information collection, 219–220; evidence obtained using, 218, 261n71; general warrants, 193; government’s procedure for obtaining information, 202; law enforcement, 194; per se warrant rule, 189; police, 261n50; Privacy Protection Act (1980), 220; probable cause, 202; replacement by subpoenas, 209; requirement for, 189, 192–195, 202; right to privacy, 195; Stuntz on, 194; subpoenas, 202–203, 220; writs of assistance, 193
Warranty registration cards, 52
Warren, Samuel, 197. See also Right to Privacy (Warren and Brandeis)
Washington, George
Waterston, Silas, 189
Waterston, Silas, 189
Web bugs, 25
Weber, Max, 38–39
Websurfing, 23–24
Welfare recipients, 41–42
Westin, Alan, 76, 77
Whalen v. Roe, 65–66, 156–157, 254n58
Whitaker, Reg: End of Privacy, 32
Wiland Services, 3
Winter, Steven, 27–28
Wiretap Act, 204
Wiretapping: Brandeis on, 201; evidence from, 199, 261171; by FBI, 185, 199; Federal Communications Act (1934), 199, 203; Fourth Amendment, 197, 203; Holmes on, 199; Hoover on, 199; by Johnson, 199; of King, 185, 258n99; by Nixon, 199; Olmstead v. United States, 197–199; state wiretapping, 200; Title III, Omnibus Crime Control and Safe Streets Act (1968), 203–204
Witnesses, 153–154
Wood, Gordon, 194
Worker’s compensation records, 128
Wright, Frank Lloyd, 98
Writs of assistance, 193
Wrong, Dennis, 30
Yale University, 118
Yellow journalism, 57
Youens, Liam, 54
Zurcher v. The Stanford Daily, 220
About the Author

Daniel J. Solove is Associate Professor of Law at the George Washington University Law School. Previously, he taught at Seton Hall Law School. He is the author (with Marc Rotenberg) of Information Privacy Law. Professor Solove received his J.D. from Yale Law School.