PRIVACY

THE LOST RIGHT

JON L. MILLS

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Oxford University Press, Inc., publishes works that further Oxford University's objective of excellence in research, scholarship, and education.

Oxford New York
Auckland Cape Town Dar es Salaam Hong Kong Karachi Kuala Lumpur Madrid Melbourne Mexico City Nairobi New Delhi Shanghai Taipei Toronto

With offices in
Argentina Austria Brazil Chile Czech Republic France Greece Guatemala Hungary Italy Japan Poland Portugal Singapore South Korea Switzerland Thailand Turkey Ukraine Vietnam

Published by Oxford University Press, Inc.
198 Madison Avenue, New York, New York 10016

Oxford is a registered trademark of Oxford University Press
Oxford University Press is a registered trademark of Oxford University Press, Inc.

Library of Congress Cataloging-in-Publication Data

Mills, Jon L.
Privacy: the lost right / Jon L. Mills.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-19-536735-5 (alk. paper)
1. Privacy, Right of—United States. I. Title.
KF1262.M55 2008
342.7308'58—dc22

2008016529

2 3 4 5 6 7 8 9

Printed in the United States of America on acid-free paper

Note to Readers
This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is based upon sources believed to be accurate and reliable and is intended to be current as of the time it was written. 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 person should be sought. Also, to confirm that the information has not been affected or changed by recent developments, traditional legal research techniques should be used, including checking primary sources where appropriate.

(Based on the Declaration of Principles jointly adopted by a Committee of the American Bar Association and a Committee of Publishers and Associations.)

CHAPTER I

Introduction

A Day in the Life

Lenny wakes up in the morning, gets dressed and goes online to visit a couple of Web sites, while cookies[1] and spyware[2] track her browsing habits and gather her consumer information. She then gets in her car, which has a global positioning system ("GPS") and drives to work, while a "black box" sends data about the vehicle back to the automobile manufacturer. As she drives to work, RFID[3] technology from her E-Z Pass relays her payment information and the location of the car as it passes through a toll station. During her drive to work, Lenny has a conversation on her cellular phone that may be intercepted and publicly disclosed on the radio.[4] She arrives

---

[1] Luke J. Albrecht, Note, *Online Marketing: The Use of Cookies and Remedies for Internet Users*, 36 SUFFOLK U. L. REV. 421 (2003) (discussing the use of cookies and the collection of data from Internet users).

[2] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004) (discussing a program that installs itself without your permission and can collect personal information).

[3] Radio Frequency Identification—implanted in merchandise, toll devices, pets, or people. *See* DANIEL J. SOLOVE, INFORMATION PRIVACY LAW 628–29 (2d ed. 2006).

[4] Further, technology can enable one to track a cell phone's location. "Cell phones can reveal very precise information about your location, and yet legal protections are very much up in the air." Ellen Nakashima, *Cell Phone Tracking Powers on Request*, WASH. POST, Nov. 23, 2007, at A01 (quoting Kevin Bankstone of Electronic Frontier Foundation).

at work and parks her car in a parking lot with camera surveillance. Once she is at her office desk, Lenny logs on to her computer and checks her e-mail, which is overseen by her employer.[5] In the afternoon, she visits a friend at a family-planning clinic and, unknown to her, her picture is taken and posted on a Web site by a "pro-life" group.[6] After work, Lenny and her colleagues are recorded going to a bar in a section of downtown where the city has recently installed a digital closed-circuit television ("CCTV") camera.[7] At the bar, Lenny buys a round of drinks with a credit card, and the transaction is monitored by her credit-card company, which then discloses Lenny's marketing information to a third party. After Lenny leaves the bar, a police detective picks up a piece of gum she left in an ashtray because Lenny generally fits the description of a murder suspect and the detective wants to check her DNA for a potential match.

The fictional societies in *Brave New World* and *1984* appalled readers with the specter of a dehumanized future world. Big Brother was omnipotent, privacy was scorned, and individuality was crushed. How do we stand today in the glare of instant communication, tabloid press, Internet intrusions,[8] data brokers, security cameras, and big government? Have individual freedoms been irretrievably altered by the omnipresent gaze of a modern-day panopticon?[9] What is left of individual privacy, and how

---

It was also recently revealed that there was a study conducted by Northeastern University which tracked the whereabouts of 100,000 people outside the United States through the use of their cell phones.Seth Borenstein, *Study secretly tracks cell phone users outside US*, Associated Press (June 4, 2008), available at http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2008/06/04/national/a100140D77.DTL (last visited June 11, 2008).

[5] Her employer may monitor the e-mails she sends or the Web sites she visits. Further, spyware implanted in her computer may allow outside parties to view her computer use, even the keystrokes. Kim Zetter, *Employers Crack Down on Personal Net Use*, PCWorld, Aug. 25, 2006, http://www.pcworld.com/article/id,126835-c,workplace/article.html (last visited May 9, 2008).

[6] *See* abortioncams.com (last visited June 22, 2008). *See also infra* note 354 for other examples of citizens posting pictures on the Internet.

[7] *See* Clive Norris & Gary Armstrong, The Maximum Surveillance Society: The Rise of CCTV (1999).

[8] For further discussion on the promise and problems of mass information on the Internet, see Tal Z. Zarsky, *Information Privacy in Virtual Worlds: Identifying Unique Concerns Beyond the Online and Offline Worlds*, 49 N.Y.L. Sch. L. Rev. 231 (2004).

[9] *See* Jeremy Bentham, The Panopticon Writings 29–95 (Miran Bozovic ed., Verso 1995) (suggesting the use of a panopticon design for a prison building, which aimed to create a prison atmosphere where prisoners could never know whether their actions were being monitored by guards at any given point in time). The mere possibility that a guard might be watching thus motivates inmates to regulate themselves as though

can it be saved? Is the protective ability of the law so far behind technology at this point that we cannot catch up? To understand privacy as it exists in this country today, we must answer a series of questions: what is privacy? what are the challenges to personal privacy in today's culture? what are our legal protections? and finally, how can we protect privacy better?

Individual identity is defined largely by the control of personal information and the exercise of personal autonomy. U.S. courts and writers refer to privacy in the most sacred of terms—as one of a person's most valued rights.[10] Indeed, privacy and personal autonomy are both cherished. We punish people by placing them in prison, thus taking away their autonomy and their ability to have private lives. We protect the right of citizens to live in a private home and carefully limit any intrusion into that home by either the government or other citizens. We usually allow people to choose which religious teachings to follow and which persons with whom to associate. However, in today's society, legal protections fail to match privacy's treasured status. Intrusions are allowed for a series of reasons: (1) protecting public security, welfare, and public health;[11] (2) upholding moral standards of society at a particular time;[12] (3) protecting other values such as access to public records and freedom of speech;[13] and (4) promoting commerce by allowing the gathering and wide dissemination of information.[14] The privacy right is hardly absolute. The importance of individual rights is balanced against the rights of the larger community. Amitai Etzioni devoted an entire book to describing the significance of honoring "communitarian theory" against modern concerns about individual privacy.[15] The book reminds us that we voluntarily give

---

someone was in fact observing their behavior. For a more thorough discussion of the panopticon effect, see *infra* Chapter III, § B-6.

[10] *See, e.g.*, Dalia v. United States, 441 U.S. 238, 250 n.9 (1979) ("[E]lectronic surveillance can be a threat to the 'cherished privacy of law-abiding citizens.'" (quoting United States v. U.S. Dist. Court, 407 U.S. 297, 312 (1972))); Quilici v. Village of Morton Grove, 695 F.2d 261, 280 (7th Cir. 1982) ("The right to privacy is one of the most cherished rights an American citizen has; the right to privacy sets America apart from totalitarian states in which the interests of the state prevail over individual rights.").

[11] *See, e.g.*, Sherr v. Northport-East Northport Union Free Sch. Dist., 672 F. Supp. 81 (E.D.N.Y. 1987) (holding that bogus and insincere religious beliefs are not grounds for exemption from New York's mandatory school inoculation program).

[12] *See, e.g.*, Loving v. Virginia, 388 U.S. 1 (1967). Miscegenation statutes of the past are one example of a prohibition that can only be based on a moral reason rather than other public purposes.

[13] The right to free speech justifies multiple private intrusions.

[14] *See* discussion *infra* Chapter III, § B-5(b).

[15] Amitai Etzioni, The Limits of Privacy (1999).

up some individual rights to protect our community from child molesters and terrorists.

What does privacy mean? The word's etymology is from *privation* and *deprivation*—two decidedly negative concepts.[16] But the words we normally associate with privacy are independence, freedom, autonomy, liberty, individuality, dignity, seclusion, and the absence of intrusion. All of these are treasured concepts. However, we should be conscious that just because something is protected by "privacy" does not automatically mean that it is good and universally supported. Privacy can shield bad acts. Feminist writers and others note that privacy was used to cloak abuses by husbands in "disciplining" their wives.[17] So privacy can be, and has been, used to cover up abuses.

There is a continuing struggle to define privacy. Some suggest that it is not worth the struggle, because privacy cannot be understood as a unified concept. Privacy is hardly a one-dimensional concept and is probably more akin to the "bundle of rights" we talk about when legally conceptualizing property rights. These property rights include the ability to own, transfer, and exclude people from property. Privacy rights include the right to exclude others, make choices, and exercise personal liberties.[18] It is worthwhile to look at this entire bundle at one time.

Just as difficult as defining the term "privacy" is reaching agreement on the origins of privacy as a legal concept. The legal status of privacy is grounded in ancient natural-law principles of individual freedom and liberty. These principles were articulated by philosophers from Aristotle to Cicero to Thomas Aquinas. Evaluation of privacy law must begin with these higher precepts. The principles of imposing limitations on the government and the sanctity of individuals are further described in the writings of John Stuart Mill, John Locke, and Thomas Hobbes. For example, Mill said, "The only part of the conduct of anyone for which he is amenable to society is that which concerns others. In that part which merely concerns himself, his independence is, of right, absolute."[19] Sir William

---

[16] RICHARD A. GLENN, THE RIGHT TO PRIVACY: RIGHTS AND LIBERTIES UNDER THE LAW 3 (2003).

[17] The protection of a husband's ability to "discipline" his wife has been rightly critiqued by contemporary feminist writers. *See* SOLOVE, *supra* note 3, at 69–73; *see also* Reva B. Siegel, *"The Rule of Love": Wife Beating as Prerogative and Privacy*, 105 YALE L.J. 2117 (1996).

[18] *See* the "Four Spheres of Privacy" chart at page 6 and the accompanying text.

[19] JOHN STUART MILL, *On Liberty* 96 in UTILITARIANISM, LIBERTY, AND REPRESENTATIVE GOVERNMENT, American ed., E.P. Dutton and Co., Inc. (1951); *see also* GLENN, *supra* note 16, at 19.

Blackstone, as the first recorder of the common law, emphasized the importance of private property and the prerogatives of a family's privacy.[20]

Privacy thus has many theoretical progenitors. Even in early America, the combination of rights protecting the home, the person, and personal information provided a basis for protecting individual liberty.[21] Those protections are based on the evolution of common-law protections. Even before the landmark—and revered—article by Samuel D. Warren and Louis D. Brandeis,[22] Thomas Cooley made an attempt to define privacy as "a right of complete immunity: to be let alone."[23] And the Michigan Supreme Court recognized the right when deciding that a young unmarried man could be excluded from a room during childbirth because "[t]he plaintiff had a legal right to privacy of her apartment at such a time and the law secures to her this right by requiring others to observe it."[24]

The article by Warren and Brandeis galvanized this disparate history. It is fair to say that they named privacy but did not invent it. The 1890 article expressed deep concern about the advent of photography, new technologies, an intrusive society, and an invasive press as dangers to individual privacy.[25] In fact, Warren may have been personally offended by press coverage of his daughter's wedding.[26] In 1905, the first American court identified "privacy" as a freestanding right.[27] In 1928, Brandeis, sitting as a Supreme Court justice, dissented in *Olmstead v. United States*, a case dealing with surveillance, arguing that the right to privacy is inherent in the U.S. Constitution.[28] Brandeis's view would become law when *Katz v. United States* overturned *Olmstead*, echoing his earlier dissent.[29] Likewise, in *Mapp v. Ohio*, an important decision regarding the exclusionary rule under the Fourth Amendment, the Court again returned to

---

[20] 2 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAW OF ENGLAND 1–15 (1766).

[21] *See* GLENN, *supra* note 16, at 47.

[22] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[23] GLENN, *supra* note 16, at 50 (noting that as early as the 1880s, Thomas Cooley was attempting to define privacy).

[24] DeMay v. Roberts, 9 N.W. 146, 149 (Mich. 1881).

[25] Warren & Brandeis, *supra* note 22 (asserting that individuals should have full protection of person and property).

[26] *See* GLENN, *supra* note 16, at 45. However, recent scholarship indicates that Warren's daughter could only have been as old as seven at the time of the publication and was not married until fifteen years later. *See* J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY 20 (2d ed. 2007).

[27] *See* Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905).

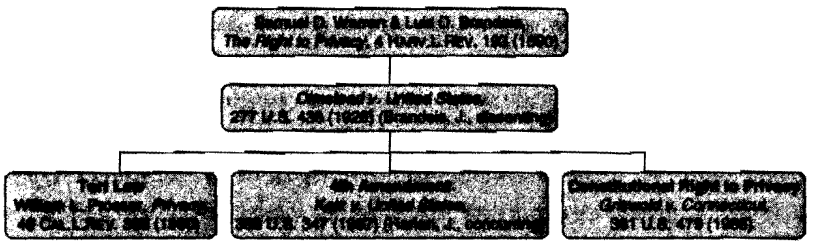
[28] Olmstead v. United States, 277 U.S. 438, 473–76 (1928) (Brandeis, J., dissenting).

[29] Katz v. United States, 389 U.S. 347, 350–51 (1967).

Brandeis's ideas to support the finding that evidence obtained through unconstitutional means may not be used against a defendant.[30]

By the 1960s, legal protections derived from Warren and Brandeis had developed in three areas: the privacy torts, as articulated by William L. Prosser[31] and the *Restatement (Second) of Torts*; the search-and-seizure Fourth Amendment jurisprudence developed in *Katz v. United States*; and the now well-known "penumbral" rights identified in *Griswold v. Connecticut*. The Court in *Griswold* again cited Brandeis's dissent in *Olmstead*, including the phrase "the right to be let alone." In *Griswold*, Justice William O. Douglas recognized that privacy was not a new concept when he said ". . . the right of privacy which presses for recognition here is a legitimate one. . . . We deal with a right of privacy older than the Bill of Rights. . . ."[32]

Family Tree for Privacy in Contemporary U.S. Law



Though these areas of the law are different, each draws from the same well. The once seemingly novel idea that a "right to privacy" existed in the Constitution found footholds at various times through similar reasoning in Fourth Amendment jurisprudence, privacy torts, and constitutional penumbral rights.[33]

Today, the law protects privacy through a mixture of constitutional law, tort law, property law, and statutory law. Some of these legal protections are ancient and settled, whereas others are more modern and tend to be less effective. Constitutional law protecting personal autonomy in areas such as marriage, procreation, and child rearing is well developed, offering significant, though sometimes unpredictable, protection. However,

---

[30] Mapp v. Ohio, 367 U.S. 643 (1961).

[31] Prosser was something of a critic of privacy as it was articulated by Warren and Brandeis. He did not favor expansion. He did categorize privacy into four torts. *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

[32] Griswold v. Connecticut, 381 U.S. 479, 485–86 (1965).

[33] *See* discussion *infra* Chapter III, § A-1.

the same cannot be said for constitutional law's effectiveness in the area of intrusions relating to personal information, by either private or governmental sources. For these types of intrusions, constitutional law provides a lower standard of protection. Furthermore, because the First Amendment specifically fosters individual expression by protecting most forms of speech, in some cases it can be a significant obstacle to an individual's *privacy interests*. Because individual privacy is impaired through the constitutional protection enjoyed by the media when disclosing private information, the First Amendment serves a critical dual role in privacy analysis. It provides both a basis for the "penumbra" protecting privacy and a justification for press and other free-speech intrusions.[34]

Tort law seeks to prevent the intrusiveness associated with unauthorized disclosure of personal information.[35] But tort protections are inadequate for the realities of modern life. Tort law fails to protect against the disclosure of personal information or to provide an adequate remedy to the victim once that information is disclosed. One reason for this result is the law's pervasive requirement in privacy cases, both information-related and autonomy-related, that an individual have a "reasonable expectation" of privacy in order to be eligible for any remedy.[36] Obviously, the law cannot provide redress for every perceived intrusion against the privacy of some oversensitive person. However, the reasonable expectation of privacy recognized by the law does not keep pace with the varying types of information disclosure afforded by rapidly advancing technologies, such as the Internet, digitally recorded closed-circuit television, and mobile communication devices. As a result, data that was once within the reasonable expectation of personal and private information has become readily available and easily disseminated—without a legal structure in place to protect the individual whose privacy has been invaded.

In comparison with the unclear and flimsy remedies associated with protecting information, the rights associated with protecting personal, real, and intellectual property and the rights protecting personal physical space are well developed and well established in most modern systems of law.

---

[34] *See* discussion *infra* Chapter IV.

[35] *See* Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 295 n.11 (1983) ("The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."(quoting Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890)).

[36] *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

This book explores why personal information is less protected than personal autonomy and suggests theories of how protections could be improved. In particular, it explores how modern courts can and should expand tort remedies to comport with reality, how property theories offer an avenue for protecting personal information, and how governments might expand existing statutory privacy protection.[37]

The examples of actual cases in the next chapter help illustrate the importance and prevalence of privacy issues in our contemporary lives.

[37] *See* Warren & Brandeis, *supra* note 22, at 205.

CHAPTER II

A Perspective on the Reality of Privacy Issues Today

The loss of privacy is more than just an academic question. The complexity of today's society constantly generates both major and minor invasions of an individual's privacy rights. The following are real-life examples that will be referenced in various places in this book when the issues they illustrate are discussed. Some of these examples will also be examined in more depth in Chapter VI, where I will discuss the outcomes of the cases and how various reforms might improve such outcomes.

Twenty invasions:

1. After a series of savage murders of college students, the press seeks access to autopsy and crime-scene photographs.
2. The producers of the movie *The Perfect Storm* intentionally and inaccurately depict boat captain Billy Tyne as an unsuccessful and careless captain who took risks that cost his crew their lives. They market the film as a true story.
3. Two individuals talk on a cell phone about a labor dispute in Philadelphia. Their call is monitored and later broadcast on the radio.
4. A St. Patrick's Day parade committee in Boston denies a gay group their request to participate in the parade.
5. A woman writes an Internet blog revealing personal, embarrassing, and offensive details about a lover.

6. Terri Schiavo is found to be in a persistent vegetative state. A court finds that her intent was to be removed from life support in these circumstances. The legislature passes a statute requiring life support to be reattached.
7. An Internet Web site solicits salacious comments about individuals and promises anonymity to the writer.
8. Ms. Toni Ann Diaz is elected the first female president of her community-college student body in Oakland, California. The newspaper publishes the fact that she had previously undergone a sex-change operation.
9. During a child-custody dispute an estranged husband surreptitiously videotapes, through the open window of her house, his wife having sex with another woman.
10. The *New York Times* seeks NASA records of the audiotape of the crew's voices recorded during the Challenger crash.
11. The company that produces the video series *Girls Gone Wild* films a woman exposing herself in a public square and uses her image in nationwide advertising for the video.
12. The newsletter of the organization Jews for Jesus recounts the conversion of a Mrs. Rapp to Jesus. She says it never happened.
13. The Texas legislature passes a statute criminalizing homosexual behavior.
14. A Maryland database of medical records compiled for cost-containment purposes is sold to bankers who use the list to call in loans to patients with terminal cancer.
15. A school board requires random drug and alcohol testing of all students if they are going to participate in the school band.
16. The City of Miami Beach requires all applicants for city jobs to disclose whether they have smoked tobacco in the last year.
17. An unknown person in Berlin pretends to be an actress on a dating Web site. That person posts suggestive remarks and discloses the actress's home address and phone number.
18. A physician uses a patient's spleen cells to patent a cell line.
19. A fourteen-year-old boy dies of a drug overdose, and members of the local police department videotape the autopsy and show it to friends at parties.
20. A television production company contracts with a medical examiner in Nashville, Tennessee, to obtain access to accident sites and autopsies. After the death of a married couple who

apparently jumped out of the window of a Nashville hotel, the production company films the scene and then films the autopsy of the wife for the television show *True Stories from the Morgue.*

These incidents represent a cross section of intrusions into individuals' lives by the government, individuals, corporations, and the media. The span and depth of these intrusions should enrage citizens. But the fact is that we as citizens are largely unaware of just how invasive this society can be.[38] Some of these scenarios have legal remedies—others do not. As examples, they begin to provide the context of our contemporary intrusive society.

[38] *See* Joseph Turow, Lauren Feldman, and Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline*, Annenberg Public Policy Center of the University of Pennsylvania, June 1, 2005. This poll indicated wide ignorance of the law and business practices affecting personal information. Cited, *available at* http://epic.org/privacy/survey/ (last visited June 22, 2008). 64% believed falsely that their supermarket is barred by law from selling customer data. 72% believed falsely that charities are barred by law from selling personal information without permission. 73% believed falsely that banks are barred by law from sharing information with other companies and affiliates. 75% believed falsely that the presence of a privacy policy on a Web site means that the company cannot sell customers' information to others. 76% believed falsely that the Federal Trade Commission will correct errors in credit reports.

CHAPTER VII

Strategies and Remedies to Protect Privacy

The preceding sections of this book compel two conclusions: (1) privacy rights are diminishing in contemporary society; and (2) existing legal tools, which include constitutional protections, tort remedies, statutory protections, and litigation based on property theories, are inadequate to protect privacy in a changing world. This section examines broad policy changes, reinterpretations of existing remedies, the potential for the creation of new theories, and practical options to achieve individual privacy.

In formulating new strategies to protect privacy, one must confront the fact that protecting privacy conflicts with other values, such as public safety and free speech. Furthermore, privacy is subjective to individuals and is a moving target in a quickly evolving society. Perhaps we need a basic shift in the way our society views and values the individual in the privacy context. In both the European Union and Latin America, there is an emphasis on personal dignity, whereas the American philosophy grants primacy to free expression at the expense of personal dignity.

Writers and commentators have taken a range of approaches in suggesting reforms to privacy policies. Some suggest focusing on the issues of data creation and protection rather than rejuvenating old remedies.[1399] This approach often includes establishing a national agency aimed at monitoring, overseeing, and enforcing penalties for abuses of information.[1400]

[1399] Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087 (2006), *available at* http://ssrn.com/abstract=941181.

[1400] *See id.*

This can be termed the policy approach. Another approach is to enhance and implement legal remedies in courts to make violators of privacy rights pay heavily for mistakes, thereby compelling reform. This could be termed the trial-lawyer approach. A third approach is to let the market drive information-protection reform because consumers will demand more personal privacy.[1401] This is the market approach. There is something to be learned from each of these views and approaches.

Among the various forms of privacy, informational privacy is most in jeopardy when compared with autonomy rights. Constitutional protections of personal autonomy are well developed, and the theories are well established. Personal-autonomy issues, such as abortion rights and the right to die, may face challenges from interpretations of existing law based on evolving Supreme Court positions. The challenge there, however, is not whether a remedy exists but rather how to apply that remedy. If the Supreme Court retreats from previous positions, the application of the remedy will be based on an interpretation of law that no longer recognizes a reasonable expectation of privacy or that finds a compelling governmental interest in regulating conduct. This impact is no less threatening to individual privacy. In fact, one could argue that autonomy issues will be at substantial risk in the years to come. It is not likely, however, that the Court will abolish the privacy right related to autonomy.[1402] In fact, Justice Samuel Alito, a likely swing vote on the issue, has said that a constitutional privacy right exists.[1403] Retreat on issues such as contraception and parental authority in child rearing is unlikely. The issue is defining "family," "marriage," "reproductive rights," and other constitutional catchphrases. But issues of employee and student drug testing, homosexual marriage and adoption, control of genetic material, and other unpredicted issues will test the Court's evaluation of the reasonable expectation of privacy and the compelling interests of the government.

[1401] The Internet service provider America Online announced that it would sell user information, but then quickly stopped such practices upon seeing its stock drop. *See* Malcolm Maclachlan, *Self-Regulation Needed to Ensure Privacy*, TECHWEB, Mar. 13, 1998, http://www.techweb.com/wire/story/TWB19980313S0018.

[1402] *See* Webster v. Reproductive Health Servs., 492 U.S. 490, 536 (1989) (Scalia, J., concurring in part and concurring in judgment) ("[T]he mansion of constitutionalized abortion law, constructed overnight in *Roe v. Wade*, must be disassembled doorjamb by doorjamb, and never entirely brought down, no matter how wrong it may be.").

[1403] *See* Jill Zuckman, *Alito Affirms Right to Privacy*, CHI. TRIB., Jan. 11, 2006, *available at* http://www.chicagotribune.com/news/nationworld/chi-0601110204jan11,1,3826309.story.

Regardless, with respect to autonomy issues, the argument will be how to apply the right of privacy rather than whether a right to privacy exists.

Among the various forms of privacy, informational privacy is most in jeopardy. Indeed, the more difficult issue is to find an effective remedy for intrusions on personal information. Society has moved too fast for the law to catch up. As e. e. cummings once observed, "progress is a comfortable disease."[1404] Our society has enjoyed its "progress," but are we able to define limits to protect the individual?

In addition to the march of technological progress, rational concerns about national security underpin greater governmental intrusion. The government now has access to many private communications without a search warrant. Further, information and communication systems are more vulnerable to government surveillance and observation, particularly because the predominant modes of communication—e-mail and cellular phones—are insecure by their very nature. The current situation gives the government far more power to scrutinize individuals than ever before, power that is approaching that of Orwell's Big Brother.[1405]

Next, data brokers and other companies that sell information about individuals for marketing and security purposes have the ability to gather personal information without the Fourth Amendment restrictions placed on government. In fact, the information industry works closely and shares information with the government.[1406] In addition to the government, the data brokers sell information to virtually anyone who wants it, including the medical, financial, and insurance industries. The data industry has information on millions of citizens and is proud of it.[1407] Beyond the fact that this information is highly intrusive and generally available without permission, a major concern is that the information industry is quite capable of making mistakes, including the distribution of harmful and inaccurate information[1408] and security breaches that facilitate identity theft.

[1404] E.E. CUMMINGS, 100 SELECTED POEMS 89 (paper ed. Grove Press 1959).

[1405] Congress just recently passed the Protect America Act of 2007, PUB. L. No. 110-55, 121 Stat. 552, amending the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–1811.

[1406] *See* discussion *infra* Chapter III, § A-2.

[1407] The Acxiom Corporation advertises that its InfoBase List contains the names of 176 million individuals and 111 million households nationwide. Axciom, InfoBase List, http://www.acxiom.com/default.aspx?ID=1758&DisplayID=18 (last visited Aug. 20, 2007).

[1408] For example, the credit-reporting agency Experian relied on public records from a court docket in compiling a man's credit report. The court docket incorrectly stated that a legal judgment had been entered against the man at one point, and correctly noted at another point that the case was settled and dismissed. Experian only reported

Finally, modern media actors—in particular the "stalkarazzi," attack journalists, bloggers, and "bad news" journalists—are more intrusive than ever. Yet, as discussed extensively throughout this book, media actors remain protected by the First Amendment. The "stalkarazzi," the most extreme of these "journalists," make a living by intruding upon individual privacy.[1409] Attack journalists focus on attacking the political class, and "bad news" journalists focus on sensationalism without regard to the impact on innocent third parties. Bloggers simply write whatever they deem interesting and publish it on the Internet. The First Amendment has been strained to its limits to shield actions that were never envisioned by its framers. The media can fulfill their role of informing the public and holding the government accountable without intruding on the most private parts of citizens' lives.

There are multiple sources for remedies, including the U.S. Constitution, state constitutions, federal statutes, multiple state statutes, four historic privacy torts, and other traditional and some novel legal theories. Yet intrusions without recourse abound. Effective remedies for the disclosure of personal information are limited by the myriad accepted justifications for intruding upon privacy. Additionally, there is no overarching textual commitment to privacy in either the Constitution or any federal law. Although there are some broad commitments in places like the European Union, the development of American jurisprudence and policy remains a patchwork. Moreover, whenever broad remedies are sought against privacy intrusions, the specter of lost domestic security or lost freedom of the press are raised. If there are to be solutions, the approach should combine a strengthening of traditional legal theories with a more direct granting of rights and remedies that will address the gaps in privacy protection. When remedies fail to protect basic values, even the most ardent defenders of the common-law precedent recognize the need for change.[1410] In other words, a multifaceted approach, with legal and legislative innovation, is necessary to develop effective privacy protections.

---

the incorrect entry. Bob Egelko, *Court Reverses Itself—Finds Credit Agency Violated Man's Rights*, S.F. CHRON., Sept. 27, 2007, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/09/27/BAJ5SEMHR.DTL.

[1409] *See* John Fuson, *Protecting the Press From Privacy*, 148 U. PA. L. REV. 629, 669 (1999). The publicist Dick Guttman termed this breed of paparazzi the "stalkarazzi." "Paparazzi" literally means "buzzing insects."

[1410] 1 BLACKSTONE, *supra* note 20, at 69–70 ("Yet, this rule admits of exception, where the former determination is most evidently contrary to reason, much more if it be contrary to define law."). Blackstone further said that a manifestly absurd or unjust law is not the law.

A. Implement Basic Policy Changes

1. Create a Right to Informational Privacy Analogous to That of the European Union

If Americans wish to place a higher priority on personal privacy, we should examine the European Union's approach. Even though citizens in the United States revere individuality and the United States was founded on a strong foundation of personal liberties, privacy receives less legal protection here than in the European Union. If the United States was founded, at least partially, to escape hierarchy, royalty, and elitism, why do we not regard privacy more highly than the Europeans?

First, the European Union was founded in the modern era, and its founding documents could include textual regard for privacy in the contemporary context. The United States has been compelled to develop privacy law over two hundred years of court-created precedent in state and federal courts. Second, national security and safety issues have become dominant policies in the United States. This distinction is evidenced by the conflict between U.S. Homeland Security policies and E.U. privacy policies relating to commercial airline travel discussed earlier.[1411] Third, free-speech protections under the First Amendment and the newsworthiness doctrine are more sweeping in the United States. Fourth, the United States has a more open approach to public records.

Although substantial, none of these factors are absolute barriers to enacting a comprehensive privacy policy in the United States. A threshold need is broader recognition of the real and present danger of losing privacy rights in the tidal wave of contemporary society.

In a 2004 *Yale Law Journal* article, James Q. Whitman compares European and American privacy cultures.[1412] According Whitman, the differences between the two ideas are rooted in the concepts of "privacy as an aspect of dignity and privacy as an aspect of liberty."[1413] The American system of privacy protection is oriented toward the concept of privacy as an aspect of liberty.[1414] American privacy law has focused more on intrusions

---

[1411] *See* discussion *supra* Chapter III, § C-6(a).

[1412] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004).

[1413] *Id.* at 1161. Robert Post identified these values in 2001. *See* Robert Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087 (2001).

[1414] Whitman, *supra* note 1412, at 1161.

by the government than on intrusions by the private sector and the media.[1415] The law was created to "maintain a kind of private sovereignty within our own walls."[1416]

In contrast, the European system is based on the concept of privacy as an aspect of dignity.[1417] According to Whitman, the core European privacy rights, that is, the right to control one's image, name, and reputation, as well as "informational self-determination," are all rights intended to allow an individual to shape his or her own public persona.[1418] A main focus of the European laws is protection against the media.[1419] Interestingly, that was a principal focus of Warren and Brandeis's article, which is the basis of tort privacy protections in the United States.

Whitman discusses newsworthiness in the article's section on contemporary European law and free expression.[1420] In contrast to Europe, where personal honor is a constitutional value, the United States views freedom of expression as being paramount.[1421] This explains the broad newsworthiness exception to privacy actions in the United States.[1422] Whitman asserts that European courts would see cases like that involving Oliver Sipple differently from American courts.[1423] The case began on September 22, 1975, when Sara Jane Moore wielded a .38-caliber pistol and attempted to assassinate President Gerald R. Ford while he was visiting San Francisco, California. Oliver Sipple was in the crowd and grabbed or struck Moore's arm as she was about to shoot at the president. The bullet missed Ford by approximately five feet because of Sipple's reaction.

The *San Francisco Chronicle* heralded the act by publishing an article that focused on Sipple's sexual orientation and revealed to the world that Sipple was a homosexual. Sipple filed a lawsuit against the author, the *San Francisco Chronicle*, and a number of other newspapers. Sipple alleged that the papers published private facts about Sipple's life that lead to ridicule, mental anguish, embarrassment, and the disassociation of Sipple from his family.[1424]

[1415] *Id.* at 1162.
[1416] *Id.*
[1417] *Id.* at 1161.
[1418] *Id.*
[1419] *Id.*
[1420] *Id.* at 1196–1202.
[1421] *Id.*
[1422] *Id.* at 1196.
[1423] *Id.* at 1197.
[1424] Sipple v. Chronicle Publ'g Co., 154 Cal. App. 3d 1040, 1044–45 (Ct. App. 1984).

The California court dismissed the out-of-state defendants for lack of personal jurisdiction and granted the California defendants summary judgment because Sipple's sexual orientation was a well-known fact to many people in his local community. Further, the court found Sipple's sexual orientation to be newsworthy since his actions saving the president put him in the public light.[1425]

In Europe, the analysis differs. Freedom of expression is always balanced against personal dignity; and personal dignity often wins.[1426] For example, Whitman cites a French case with facts similar to that of *Sipple*. In 1985, a man attended a gay-pride parade in Paris and dressed as a participant in the parade.[1427] The man's photograph was taken and published. When the man sued, the French court found that he had a right to oppose the photograph's publication.[1428] According to Whitman, the French way of thinking is that "the fact that one has revealed oneself to a restricted public, e.g., the gay community of Paris, does not imply that one has lost all protections before the larger public."[1429]

The United States is not expected to abandon its fundamental commitment to a free press and liberty. But we can consider how to better protect personal individuality and dignity. Further, we should remember how important these rights have been, and will be, to our culture.

2. Expand Statutory Rights

If we cannot create a comprehensive national policy, then we must continue to target abuses and create new remedies. Federal and state governments have made considerable statutory efforts to protect privacy. Clearly, statutory policies are necessary in addition to traditional torts, property, and common-law remedies. Statutes have had an impact on cell-phone privacy, data-broker liability, and the right of citizens to know about the sale of their personal information. Governments could also place more restrictions on their own data collection and provide broader standards for accuracy and accountability.

[1425] *Id.* at 1050. The court also asserted that news of his courageous act was an "attempt to dispel the false public opinion that gays were timid, weak, and unheroic figures." *Id.* at 1049.

[1426] Whitman, *supra* note 1412, at 1197.

[1427] *Id.*

[1428] *Id.*

[1429] *Id.*

Several states have examined privacy rights in the context of public-disclosure policies in court systems. Some common principles for developing remedies have emerged: (1) institute limits on information put into public records; (2) limit access to information to fewer parties; (3) give notice to third parties; and (4) hold parties accountable for accuracy and conduct. Particularly important is the handling of information in public records and held by public entities, since this information is so comprehensive, sensitive, and generally accessible.

Despite the multitude of statutory remedies, a combination of politics and constitutional barriers makes the U.S. laws less comprehensive than those in other jurisdictions. Those barriers are unlikely to be substantially lowered. Nonetheless, interest groups concerned with privacy must target specific abuses and seek limited victories at the state and federal levels. Overall, privacy policies regarding personal decisions, such as the right to die, abortion, and sexual orientation (such as same sex marriage) currently are being argued around state enactments and court interpretations. Ultimately these issues will most likely be resolved in the United States Supreme Court and not in legislative bodies.

There are, however, areas where federal and state legislatures can help greatly to protect against privacy intrusions. There are seven specific areas where statutory reform should be priorities:

1. **Reexamine the extent of immunity of Internet Service Providers.** Currently, the CDA[1430] provides immunity even to ISPs that foster and encourage anonymity for writers of salacious, malicious and slanderous comments.[1431] Congress should review this broad grant of immunity.
2. **Evaluate the coverage of newly passed genetic protection policies.** The newly enacted statute represents tremendous progress.[1432] But genetics is a rapidly changing field. Private agencies are providing DNA tests through the mail.[1433] DNA

[1430] *See,* David L. Hudson, Jr., *Taming the Gossipmongers,* ABA Journal, July 2008, 19. Discussing possible expanded ISP liability.

[1431] *See supra* note 392 regarding juicycampus.com and whosarat.*com.* Plaintiffs continue to lose actions against ISPs based on the expansive interpretation of *Zeran v. America Online,* Inc. 129 F.3d 327 (4th Cir. 1997). Congress should consider at least holding ISPs that foster and protect defamation. Another option may be to provide a remedy for defamatory statements similar to the notice and takedown provision in the Digital Millennium Copyright Act as discussed in Chapter III § B-6 of this book.

[1432] Genetic Information Nondiscrim. Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (2008).

[1433] *See supra* note 202. An individual may swab the inside of their mouth with a cotton swab and mail the swab to laboratories across the country for various DNA testing.

collection by government is expanding.[1434] Also, evaluations of individuals based on their DNA are becoming more extensive including possible medical, personality and criminal tendencies.[1435] Because of the sensitivity of these issues, they deserve close legislative attention.

3. **Protect personal communications.** Cell phones and e-mail are personal communication modes that were unknown fifty years ago. We cannot know what modes of communication will become available in the next fifty years. Confidentiality of human communications are critical to our culture and to each of us. Statutes have endeavored to protect personal communications. Some have failed.[1436] Holes in protection remain. E-mail left on a server six months is no longer private.[1437] Government monitoring of e-mails is done without warrant.[1438] It is important for policymakers to continue to focus on the importance of private communications.
4. **Stay contemporary with emerging technologies.** Again, we cannot know what the next years will bring in terms of potentially intrusive technology. RFID, ITV, and GPS, among other technologies, offer new ways for individuals and governments to intrude.[1439] More protection is possible. Washington State has acted to prevent data theft from personal RFID equipped cards.[1440] ITV can potentially gather substantial data on individuals but it is not regulated the same way cable television is.[1441] For all these reasons, legislators must be vigilant and privacy advocates must continue to inform policy makers in developing areas of technology still emerging.
5. **Examine controls over company outsourcing of data management.** The practice of outsourcing the management of data to companies in other countries in increasing.[1442] The issue that needs to be

---

[1434] *See supra* note 1447.

[1435] *See supra* note 214. Some tests purport to identify a tendency towards violence.

[1436] *See* Bartnicki v. Vopper, *supra* note 604 and accompanying text.

[1437] *See supra* note 758 and accompanying text.

[1438] See Chapter III, § B-(4)(a).

[1439] *See supra* notes 135–41 and accompanying text for a discussion of these devices and others.

[1440] *See supra* note 383 and accompanying text. Washington state has banned skimmers that can be used to steal personal data from credit cards with RFID chips.

[1441] *See supra* note 153 and accompanying text describing Interactive TV.

[1442] See Chapter III, § C-(6)(c) discussing outsourcing practices.

examined is the availability of remedies to a citizen, for example in the U.S., if the abuse or disclosure of his information occurs in another country by a company that is from the other country.

6. **Protect consumer information.** Increasing electronic sales and marketing will exponentially expand the amount of consumer information available to retailers and marketers. There are substantial statutory protections—both state and federal—expanding protection of consumer information. New marketing and new technology will continue to make this issue difficult. "Cookies" in our computers can and do track our movements on the Internet.[1443] Further, many consumers voluntarily disclose personal information. But innovations such as discount cards[1444] and ITV have substantial amounts individual data and are less regulated than previously known means of collection.
7. **Evaluate data broker practices.** Data brokers are here to stay. There are extensive statutory enactments dealing with data brokers. Still, they are collecting more and more information. Some expansion is the result of increasing amounts of public information of uncertain general value. Other types of information are being marketed that have questionable value. For example, the whosarat.com Web site provides a list of government informants.[1445] The accumulation of information about individuals continues to expand. So should the protections such as notification and liability for inaccuracies and harm to individuals.

Creating statutory privacy protections requires continual diligence at both the state and federal levels. Some issues will be more appropriate for federal policy because of nationwide and global implications. But states have an extremely important role and can augment individual privacy rights in a great number of instances and in emerging issues.

[1443] *See infra* note 1555 and accompanying text for a definition of cookies. Following is Macy's policy on cookies. *See* Appendix III.

> "We have carefully selected a company, Coremetrics, to assist us in better understanding how people use our site. macys.com will place cookies on your computer to collect information. The information that is collected through these cookies tells us things like which search engine referred you, how you navigated around our site, what you browsed and purchased and what traffic is driven by banner ads and emails."

[1444] *See supra* note 709 and accompanying text concerning discount cards.

[1445] *See supra* note 392.

3. Establish a New Agency with Oversight on Privacy Issues

One option for improving privacy protection is to create a single governmental agency with the power to set standards for privacy protection, investigate abuses of individual privacy, and enforce privacy policies.[1446] Creating another governmental agency should never be the first option for improving public policy. However, there have been successful examples in other countries in protecting individual privacy.[1447] The closest analogy is that E.U. member states established data protection authorities to enforce each state's data-protection laws.[1448] This model is effective for the European Union partly because a single data-privacy-protection policy applies to both the government and private industry. Indeed, the data-protection laws also created the data-protection authority. Regulatory power still lies in the hands of the legislative authority; the data-protection authority simply has enforcement power.

Creating a similar agency in the United States would be most beneficial if it oversaw both the public and private sectors alike, as in the European Union. Even without a single privacy statute, this outcome would still be possible if Congress enumerated the statutory provisions over which the new agency would have authority. The problem, however, is that unregulated areas would still go uncontrolled. Thus, it would be important for Congress to grant the new agency rule-making power, a

---

[1446] This recommendation has been on the table for many years. For example, the *9/11 Commission Report* alludes to the need for an authority to oversee privacy across the federal government. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 395 (2004), *available at* http://www.9-11commission.gov/report/911Report.pdf ("If . . . there is substantial change in the way we collect and share intelligence, there should be a voice within the executive branch for [liberty] concerns. Many agencies have privacy offices, albeit of limited scope."). The report resulted in the creation of the Privacy and Civil Liberties Oversight Board, with no independence from the White House and no clear mandate. Bennie G. Thompson, *The National Counterterrorism Center: Foreign and Domestic Intelligence Fusion and the Potential Threat to Privacy*, 10 U. PITT. J. TECH. L. & POL'Y 3 (2006); *see also* Christopher F. Carlton, *The Right to Privacy in Internet Commerce: A Call for Federal Guidelines and the Creation of an Independent Privacy Commission*, 16 ST. JOHN'S J. LEGAL COMMENT. 393, 426 (2002) ("Congress should create an independent privacy commission to develop privacy legislation and lead the efforts to advance it both in the public and private sector.").

[1447] *See* discussion *supra* Chapter III, § C-2(a).

[1448] Data-protection laws in the European Union originate from a common source, Directive 95/46/EC, which is a binding obligation of member states and served as model legislation for each state. *See* E.U. Directive, *supra* note 366. See *supra* Chapter III, § C-(2)(a) for a discussion of the E.U. data-protection regime.

departure from the E.U. model. Such an agency would still be constrained by other U.S. laws, including the First Amendment, so enforcement would not be directly analogous to enforcement in the European Union. The existence of a privacy agency is not a substitute for better statutory policies.

Although some governmental agencies, such as the FTC, act to protect privacy, they "dabble in privacy when it is a hot political subject."[1449] Currently, the FTC has broad authority over matters of trade and consumer protection. Particularly, the FTC requires financial institutions to implement information-security safeguards, and it has exercised its authority over retailers whose "unfair" practices expose an individual's personal information to hackers and identity thieves.[1450] However, other entities, such as schools or governmental entities that do not engage in trade, are beyond the FTC's jurisdiction. And because the FTC is tasked with many other initiatives, privacy protection may not remain on its agenda forever. A single federal agency that has the power to establish and enforce information-security rules would protect individuals. Such an agency would have limited authority over the protection of personal information and could use the FTC's enforcement regime as a starting point.[1451]

B. Expand Existing Remedies, Reduce Barriers, and Create a New Approach

One of the time-tested advantages of the common law and jurisprudence more generally is the ability to adapt old remedies and principles to new problems. The evolution of constitutional privacy in the autonomy arena over the last fifty years is stunning. The advancement on such issues as race represents a complete shift in positions held merely a century ago. The principles underlying the remedies discussed below are protecting individuals from intrusions into their personal lives and punishing those who intrude. Those simple principles must confront a complex and evolving

---

[1449] Robert Gellman, *Taming the Privacy Monster: A Proposal for a Non-regulatory Privacy Agency*, 17 GOV'T INFO. Q. 235, 236 (2000).

[1450] *See supra* note 817.

[1451] One commentator argues that regulatory power for a privacy agency is not necessary and that the agency could succeed by assisting the legislature in recommending legislation and reviewing industry's self-regulation of privacy. *See* Gellman, *supra* note 1449.

society. But we should not give up hope that the implementation of the law—and the protections it provides—can catch up to its principles. This section examines how long-standing principles and remedies can be adapted to new realities.

1. Reexamine the "Reasonable Expectation" Doctrine

The first step in evaluating a broad new approach to privacy is to ask whether the "reasonable expectation"[1452] doctrine is working. "Reasonableness" is the threshold for constitutional privacy protections, tort privacy protections, and Fourth Amendment protections against governmental intrusion. We, and other jurisdictions such as Great Britain, do not protect against intrusions that society believes are reasonable and expected. Some of those determinations are easy and intuitive. One's name is not a secret in most contexts. It is less intuitive, however, to find that telephone numbers we have called are not private and that intimate sexual conduct may not reasonably be expected to be private.

The problem with the "reasonable expectation" aspect of the right to privacy is that it is an amorphous threshold, outside of which an individual has no right of privacy. As stated previously, the law does not allow each individual to determine his or her own privacy right; this right must be determined by reference to a reasonable expectation. Who defines "reasonable expectation"? It can be either a judge or a jury depending on the circumstances.[1453] The assessment is not based on a vote or a majoritarian view. Court decisions are comically inconsistent. For example, in Alaska, an individual has a reasonable expectation of privacy to smoke marijuana in his home,[1454] but in Florida, in 1995, information that a person smokes cigarettes was not subject to a reasonable expectation of privacy.[1455] In the first half of the twentieth century, the state could regulate the distribution of contraceptives. In the later part of the century, there was a reasonable expectation of privacy to buy and use contraceptives.[1456]

How do we define what a reasonable expectation is today in an intrusive society? Should juries decide? As in the case of obscenity, should the

---

[1452] *See* Chapter VII, § B-1.

[1453] *See, e.g.*, Plaxico v. Michael, 735 So. 2d 1036, 1038 (Miss. 1999). For a discussion of the case, see *supra* Chapter VI § F.

[1454] Ravin v. State, 537 P.2d 494 (Alaska 1975).

[1455] City of N. Miami v. Kurtz, 653 So. 2d 1025 (Fla. 1995).

[1456] Griswold v. Connecticut, 381 U.S. 479 (1965).

local community define the standard? Professors Chris Slobogin and Lior Strahilevitz have suggested using empirical data to determine a society's expectations and social norms.[1457] Professor Post reminds us that commentators have invited the review of social norms.[1458] Even the Supreme Court in *Katz v. United States* suggested that Fourth Amendment jurisprudence ought to recognize society's apparent expectations.[1459] Ultimately, society's willingness to recognize the reasonableness of one's privacy expectation may depend on the intruder. That is, society may be more concerned that the government is obtaining information about us, as compared with a private marketing company that will use the information to sell us books and clothes. There is some evidence that people are more concerned by governmental intrusions, and arguably, the Fourth Amendment holds the government to a higher standard.[1460]

If one accepts that society's expectations should be tested and should be the basis for defining "reasonable expectations" in all its contexts, such a policy could make a major difference. Professor Slobogin's data indicates that some currently unprotected information available both to the government and to private data brokers is viewed as more intrusive than searches that would require Fourth Amendment permission. For example, the disclosure of e-mail addresses to and from which messages were sent and received was deemed more intrusive than the search of a car.[1461]

Perhaps there is a possibility for an evolution of the definition of "reasonable expectation" to reflect the real concerns of citizens today rather than the lowest common denominator of the "YouTube society." Although we should respect sensitivities of the majority, we should remember that some important privacy interests might not garner a majority vote.[1462]

[1457] Lior Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 932 (2005); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727, 728 (1993).

[1458] Post, *supra* note 1413, at 2092, 2094 (explaining privacy as a form of dignity that is dependent on everyday social practices).

[1459] 389 U.S. 347 (1967).

[1460] *See generally* Slobogin, *supra* note 204.

[1461] *Id.* According to the Ninth Circuit, users have no reasonable "expectation of privacy in the to/from addresses" of their e-mails. *United States v. Forrester*, 512 F.3d 500, 510–11 (9th Cir. 2008).

[1462] An absolute majoritarian view might not protect socially unpopular privacy interests that courts have protected in the past; e.g., courts have upheld abortion rights and struck down antimiscegenation laws. *See* polls on privacy at http://epic.org/privacy/survey/.

2. Expand Fourth Amendment Protections Against Government Surveillance

The traditional safeguard against governmental searches and seizures is the Fourth Amendment to the U.S. Constitution. The Fourth Amendment protects against unreasonable searches and seizures and requires probable cause for the issuance of warrants. However, these protections apply only if the subject has a reasonable expectation of privacy in the information sought.

As previously discussed, data mining presents a new mode of intrusion that demands a new look at protections. First, the government attains much of its information through private data-mining firms and other institutions, and the so-called third-party rule generally exempts this type of information from the Fourth Amendment's protection.[1463] However, the government's accumulation of this data in today's society is different from obtaining random information from private sources. In effect, the government is obtaining an intimate biography of unprecedented detail, and doing so without showing any reason. Therefore, the current state of Fourth Amendment protections must be expanded to ensure safeguards against governmental intrusions into the private lives of individuals through the practice of data mining.

Fourth Amendment jurisprudence currently states that there is no reasonable expectation of privacy in information knowingly exposed to the public. The issue is, what does "exposed to the public" mean? In *United States v. Miller*, the Supreme Court held that information given to a bank did not enjoy Fourth Amendment protection.[1464] In *Smith v. Maryland*, the Court held that individuals do not have a reasonable expectation of privacy in phone records obtained from phone companies.[1465] E-mail addresses are not protected.[1466] The analysis in these cases points to the individual's act of releasing information with the knowledge that transactional records are routinely kept in these situations. The courts thus concluded information retrieved from third parties does not enjoy Fourth Amendment protection.

[1463] *See* Andrew J. DeFilippis, Note, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1097–1102 (2006) (explaining and critiquing the third-party rule).

[1464] 425 U.S. 435, 445 (1976).

[1465] 442 U.S. 735, 745–46 (1979).

[1466] United States v. Forrester, 512 F.3d 500, 510–11 (9th Cir. 2008).

Data mining presents a unique problem. When a large amount of disparate information is gathered, synthesized, and compiled, the resultant picture of an individual is much more specific than that provided by any of the singular components.[1467]

Several legal scholars have argued for overturning *Miller* and *Smith* and have suggested that individuals have a reasonable expectation of privacy in this type of information. Anita Ramasastry attacks the analysis underlying these two decisions.[1468] To consider the act of relinquishing information to third parties a relinquishment of an expectation of privacy in that information to government surveillance is to ignore the reality of modern life. It is almost impossible to function in a modern society without making telephone calls, having a bank account, shopping, or using a credit card. Indeed, Professor Slobogin notes that the type of information obtained from third parties, such as bank and telephone records, is considered by the public to be as private as a person's bedroom, a search of which requires a warrant and probable cause.[1469]

The aftermath of the *Miller* and *Smith* decisions reflects this paradox. The reality today is that an enormous amount of data is mined, collected, distributed, analyzed, and applied without the consent or knowledge of the individual and without constitutional protections.

Professor Slobogin argues that although data mining can be intrusive in some instances, the types of intrusion do not always rise to the level deserving a high degree of justification. Slobogin argues that to properly assess the degree of justification required, we must categorize data-mining methods and weigh the motives and consequences of governmental action. The three major types of data mining are (1) target-driven data

---

[1467] *See* discussion *supra* Chapter III § B-4(c). For instance, the knowledge that someone makes calls to Kiev, as evidenced by phone records, is seemingly innocuous. However, combined with information that the same person was arrested in college at an antidemocratic rally, recently purchased *Das Kapital* at a book store, and flew to Beijing five times in a year paints a different picture. The information, when assembled collectively, transforms a series of random facts into a mosaic of the person's apparent beliefs and conduct. The inference, of course, is that the individual is a Communist, a fact that in the not-so-distant American past could be quite damaging to one's reputation, career, and personal life. Leaving aside the possibility that the information leads to a false positive (one could simply have a particular intellectual interest, rather than a political creed) this information is private in the same sense that one's sexual orientation is private. The intrusion, then, is one into the informational privacy of a person's thoughts and beliefs.

[1468] Anita Ramasastry, *Lost in Translation? Data Mining, National Security and the "Adverse Inference" Problem*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 757, 764 (2006).

[1469] Slobogin, *supra* note 204.

mining (after a target has been identified, records are searched to obtain information about that person); (2) match-driven data mining (records are searched to match an individual as a person of interest in other databases such as no-fly lists and fingerprint and DNA databases); and (3) event-driven data mining (information from large databases, such as credit-card purchases and travel records, is analyzed in order to discover patterns and predict terrorist or criminal activity). Slobogin recommends specific governmental justifications for each type of data mining, as well as varying justifications within each category. Ultimately, he concludes that private data, sought in connection with an investigation of a single target, deserves a higher degree of justification than impersonal, anonymous records or information sought to identify a perpetrator.

This argument takes into account both the need to protect the privacy of individuals and the countervailing governmental need to investigate criminal activity. Placing different forms of data mining at different points on the spectrum of Fourth Amendment protection would ensure that the government shows probable cause and a legitimate interest in obtaining corporate and public records when obtaining, through target-driven data mining, personal information such as the bank and phone records at issue in *Miller* and *Smith*. Event-driven data mining, on the other hand, as less personal and intrusive, would require only the showing of a legitimate need for the information.

In sum, the current state of Fourth Amendment jurisprudence fails to solve the privacy issues raised by the practice of data mining and electronic surveillance. Although the current state of domestic and geopolitical affairs certainly calls for diligence in the pursuit of criminals and terrorists, the interests of the individual need not yield entirely. The expansion of Fourth Amendment remedies would not necessarily inhibit the government's ability to pursue information, but rather would place limits on that pursuit when it begins to invade the privacy of individuals.

3. Reexamine Intrusion upon Seclusion

Intrusion upon seclusion may provide the most viable tort remedy remaining. A primary strength of the intrusion-upon-seclusion tort is that, at least in some cases, First Amendment rights are not necessarily implicated, because no publication is required for the wrong to be committed. For example, the act of videotaping someone having sex in the

privacy of his or her own house is an intrusion in and of itself, whether the images are published or not. The remaining challenge is to develop a consistent definition of "seclusion" and physical solitude. For example, can an individual have a reasonable expectation of seclusion in a public place?

This remedy could have utility for public-space intrusions. A modern concern is intrusion by the government and private parties in public spaces. This phenomenon is described earlier as the panopticon effect.[1470] The interest to be protected is the desire for relative obscurity and perceived obscurity when individuals are generally going about their business in public. For example, an individual might be caught on video by a surveillance camera or by a private individual. If that image is made of someone in a truly public space, like a public square, there is usually no remedy for distributing that image. Either the government or a private party will say that the individual has no reasonable expectation of privacy in a public place. Commentators have been focusing on this issue for years.[1471] There have been court decisions that found intrusions in public spaces. A Pennsylvania court held that "[c]onduct that amounts to a persistent course of hounding, harassment and unreasonable surveillance, even if conducted in a public place or semi-public place, may nevertheless rise to the level of an invasion of privacy based on intrusion upon seclusion."[1472]

Professors Clay Calvert and Justin Brown have urged the expansion of the intrusion-upon-seclusion tort to say that some matters are private even in a public space.[1473] For example, what if a camera positioned in a public square was oriented in such a way as to take pictures of a person's underwear?[1474] Calvert and Brown propose a rule that would protect against an indecent intrusion, without plaintiff's volition, that would be embarrassing to a reasonable person.[1475]

How might this formula work if the intrusion involved photographs taken of a child playing in a park and published on a child-pornography site? The above formula might fail because the photograph itself

---

[1470] *See* discussion *supra* Chapter III § B-6.

[1471] *See, e.g., infra* notes 1410–15.

[1472] Woflson v. Lewis, 924 F. Supp 1413, 1420 (E.D. Pa. 1996).

[1473] Clay Calvert & Justin Brown, *Video Voyeurism, Privacy, and the Internet: Exposing Peeping Toms in Cyberspace*, 18 CARDOZO ARTS & ENT. L.J. 469 (2000).

[1474] RESTATEMENT (SECOND) OF TORTS § 652B, cmt. c (1977).

[1475] *See* Calvert & Brown, *supra* note 1473, at 491–93.

might not be "indecent," although it might be utilized for indecent purposes.[1476]

Professor McClurg and others have proposed a multifactor balancing test that considers the motive of the defendant and conduct of the plaintiff.[1477] This test would be a remedy for child pornography. But this test is subject to criticism because it also might support an action based on a picture taken of a person in a skimpy bathing suit at a public beach.

A more limited test could include a defendant's motive, whether a reasonable person would consider the conduct intrusive, and whether the information or image was a matter of public interest. Under this test, the pornographic pictures would be actionable. Also, pictures of well-known people in public would not be actionable, nor would nonoffensive pictures. What about publishing information about a private person entering a strip club from a public street? This is not a matter of public interest, and a reasonable person might consider it intrusive.

A more aggressive application could provide a remedy for several of the intrusions described in this book. For example, a woman was filmed during rescue workers efforts to extricate her from a crash.[1478] She was filmed while in a rescue helicopter receiving emergency treatment and saying "I just want to die." These images were broadcast. She became a paraplegic.[1479] If this is not a public disclosure of private facts because it is newsworthy, could it not be an intrusion upon seclusion? The acts of filming and disclosure could be considered an intrusion upon the seclusion of Ms. Shulman. Of course, the Plaxico[1480] case previously described where a husband films a third party having sex with his wife in her own bedroom is an example of intrusion upon seclusion whether the video is

---

[1476] A photograph of a child playing in a park probably is not embarrassing. The intrusion of taking photographs in a public park probably is not indecent itself; rather, it is the subsequent posting of the photographs on a child-pornography site that elicits moral opprobrium.

[1477] Andrew J. McClurg, *Bringing Privacy Out of the Closet*, 73 N.C. L. REV. 989, 1057 (1995). The factors to be considered include (1) the defendant's motive; (2) the magnitude of the intrusion; (3) whether the plaintiff could expect to be free from this intrusion because of customs or habits of location; (4) whether the defendant sought the plaintiff's consent; (5) actions by the plaintiff manifesting a desire not to be intruded upon; (6) whether the defendant disseminated the images; and (7) whether the images involve a legitimate public interest.

[1478] *See* Shulman v. Group W. Productions, Inc., 955 P.2d 469 (Cal. 1988) *supra* note 1024.

[1479] The California Supreme Court found that the story was of a legitimate public interest (newsworthy), as were the plaintiff's words, and therefore that the plaintiff could not meet the elements of the private-facts tort.

[1480] See discussion on Plaxico v. Michael at Chapter VI, § F.

ever viewed. The intrusion tort should also be available to close family members based on the nonconsensual filming of a death scene and autopsy of their parents, as occurred in the Perkins case.[1481]

Also, what if a person goes onto an Internet dating Web site and discloses details about another person such as their name, address, e-mail and invites others to call and write that individual?[1482] That individual's actions should be an intrusion upon seclusion.

When private parties are intruding upon the "seclusion" of an individual, this remedy should be an option. Reexamining the basis for intrusion upon seclusion may provide a real and viable remedy to expand privacy protections.

4. Reexamine the Limits of Newsworthiness

Because many current intrusions are said to be cloaked by First Amendment protection, we should ask, what, if any, are the limits of newsworthiness protections? First, we must understand that the new definition of "the press" may include anyone with a Web site and e-mail capability. Claims of coverage of newsworthiness extend to an extraordinary number of entities.

What are the principles and purposes protected by the First Amendment? Today, the First Amendment protects disclosures of what most would consider private matters. If these matters are deemed newsworthy, even if through no fault of the subject, the disclosures are protected. Certainly, analysis, coverage, and information about the government and public figures are at the core of a free and democratic society. But are there limits? There are few cases that have decided that a published item was not newsworthy.

One significant case is the previously discussed *Diaz* case in California.[1483] In this case, a court decided that the fact that an individual had undergone a sex change was not newsworthy and therefore was not

---

[1481] See discussion on Perkins v. Principal Media Group, Chapter VI, § K.

[1482] *See e.g.*, Carafano v. Metrosplash.com, Inc., 339 F. 3d 1119 (9th Cir. 2003) On the dating Web site an individual in Berlin profiled an individual in California and invited others to go to another e-mail address cmla2000@yahoo.com, which, when contacted, produced an automatic e-mail reply stating, "You think you are the right one? Proof it!!" [sic], and providing Carafano's home address and telephone number. The individual was never found and the ISP was held to be immune. *See supra* notes 387–91 and accompanying text.

[1483] *See* Diaz v. Oakland Trib., Inc., 139 Cal. App. 3d 118 (Ct. App. 1983).

protected speech under the First Amendment.[1484] This reasoning might be different if the person involved was a public figure of greater significance than a student body president. In other words, a particular piece of information may be newsworthy in one instance and not newsworthy in another, depending on the individuals involved. An individual's previous drinking habits may become newsworthy following a conviction for driving while intoxicated, even if this behavior would not have been newsworthy previously. The *Diaz* case weighed three factors: (1) the social value of the information; (2) the degree of intrusion; and (3) the extent to which the party consented.[1485] The court said that newsworthiness was to be determined by the jury. Most First Amendment advocates would be troubled by allowing a jury to evaluate the social value of a news story. Usually, the press or news sources are found liable only when their conduct is malicious or grossly negligent. First Amendment rights are also specifically protected in legislative enactments.

Privacy statutes often contain exceptions for information in the public interest. Even if a statute has no specific provision dealing with protected speech, the speech may be protected under the First Amendment. And a court may find such a statute unconstitutional to the extent it prohibits or penalizes speech protected under the First Amendment, as was the case in *Bartnicki v. Vopper*.[1486]

If newsworthiness is not to be a cloak for every abuse, there must be limits. Of course, there currently are limits—First Amendment protections do not apply when one deliberately or maliciously publishes false information.[1487] But these exceptions do not provide comfort to victims of crimes or others who become the subject of media scrutiny through no fault of their own. Television and newspaper stories routinely disclose the names of victims and sometimes their addresses.[1488]

[1484] *Id.* at 134.

[1485] *Id.* at 132 (citing Briscoe v. Reader's Digest Ass'n, 483 P.2d 34 (Cal. 1971)).

[1486] 532 U.S. 514 (2001) (holding that the Wiretap Act prohibitions does not remove the First Amendment shield of freedom of speech when the disclosing party received an illegally intercepted cellular telephone conversation about a public issue, but did not play a part in obtaining the illegal interception).

[1487] New York Times Co. v. Sullivan, 376 U.S. 254 (1964); Time, Inc. v. Hill, 385 U.S. 374 (1967).

[1488] 63.4% of newspaper stories and 42.2% of television stories name crime victims in their stories. 50% of newspaper stories and 34.5% of television stories stated the age of crime victims, while just over 35% of newspaper stories and 29% of television stories named either the victim's or defendant's address, STEVEN M. CHERMAK, VICTIMS IN THE NEWS: CRIME AND THE AMERICAN NEWS MEDIA 126–27 (1995).

What should the limits be? It seems that we have come too far to require that publication of information provide an actual benefit to the public, a consideration that may be a test in other jurisdictions.[1489] So worthless information may still be protected speech. But if that information is highly intrusive, then sometimes privacy prevails.[1490] Further, the Supreme Court has said that "speech involving no matters of public concern" is of "reduced constitutional value."[1491] Therefore, a balancing test may be used to justify protection against intrusive disclosures, at least where the information is worth less to the public.

Some balancing between interests is the basis of the decision in *Diaz* and other cases in which the public benefit is weighed against the degree of intrusion. In other words, to justify an egregiously intrusive disclosure, those courts look for a real public benefit. The formula could include a requirement that a plaintiff show not only a substantial intrusion but also that the information is not newsworthy and does not affect the public interest. If there is a significant intrusion and no public interest, then there should be liability. If the First Amendment is to be protected, the burden to show injury and the absence of "newsworthiness" should be on plaintiff. This type of approach more closely mirrors the test in the European Union and in Great Britain, where a higher value is placed on personal dignity.[1492] We should not expect to abandon the long history of protection for the press, but given the evolving meaning of "press" to include bloggers and paparazzi, there is a need to examine the limits of conduct. The mainstream press has itself recognized the risks that the outrageous conduct of fringe elements pose to the important protections for the press and they should work with privacy advocates to strike a reasonable balance.

[1489] A court in Great Britain held that even when private information relates to a celebrity, there is a prima facie right to keep this information private. *See* Mckennitt v. Ash, [2006] EWCA (Civ) 1714 (Eng.). The *Mckennitt* case represents the British view that "what interests the public is not necessarily in the public interest."

[1490] McCabe v. Village Voice, Inc., 550 F. Supp. 525 (E.D. Pa. 1982) (holding that a photograph of a nude woman in a bathtub was *not* newsworthy. Even though plaintiff impliedly consented to the publication of the nude photograph by a professional photographer in a book, she did not consent to its publication in a weekly newspaper and the photo was not found to be "newsworthy."); Vassiliades v. Garfinckels, 492 A.2d 580 (D.C. 1985) (holding that before and after cosmetic surgery photos were *not* newsworthy).

[1491] Dunn & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 761 (1985).

[1492] *See supra* text accompanying notes 1372–76.

5. *Employ Property Theory to Protect Personal Information*

In his prescient book on privacy, Arthur Miller said that using property theory to protect personal information was like putting old wine in a new bottle.[1493] Professor Miller did an excellent job of predicting many of our current problems and pointing out that the law was falling behind. The law still is falling behind, and information has become a different commodity since Professor Miller wrote his book in 1971. I wonder how differently he might look at this remedy today.[1494]

Currently, there is an entire industry based on finding and selling information. Data brokers have a broad base of information, and that information has proprietary value. Because of continual breaches,[1495] there is a need for more effective remedies.

Property theory is not an alien concept for protecting information: right of publicity and appropriation of personality are property-based privacy rights. The utility of property theory is that it can achieve results where the tort remedies for privacy breaches fall short. For example, a claim for public disclosure of private facts will fail in cases involving information that is, in fact, not private, whereas the marketing or abuse of that information might be a breach of an individual's property right in the information, providing the basis for a successful action.

One problem is that the accumulation of information has great value to marketers and data gatherers even though data about one individual is not of such great value: the whole is greater than the sum of its parts. What is the damage incurred to an individual whose data is disclosed or even inaccurately disclosed? Unless an individual has been directly harmed, for example, by losing a job, the actual damages associated with the release of information regarding one individual may be so small as to deter litigation. However, class-action suits could bring smaller claims together and make litigation worthwhile. Also, the FTC has remedies focused on the bad conduct of a data gatherer.[1496]

[1493] MILLER, *supra* note 1150, at 211.

[1494] For more recent views, see Paul M. Schwartz, *Privacy Property, and Personal Data*, 117 HARV. L. REV. 2055 (2004); Leslie G. Berkowitz, *Computer Security and Privacy Law: The Third Wave of Property*, 33 COLO. LAW., Feb. 2004, at 57.

[1495] For a chronology of data-security breaches, see Privacy Rights Clearinghouse, http://www.privacyrights.org/ar/chrondatabreaches.htm (last visited May 18, 2008).

[1496] *See* discussion *supra* Chapter IV, § C-1(b).

Property theory may offer remedies that otherwise might not be available, and should be part of the list of options considered by privacy advocates.[1497]

6. Reexamine "Appropriation of Personality" and "Right of Publicity"

The remedies of appropriation of personality and right of publicity are expandable and valuable. First, newsworthiness is not necessarily a defense to these actions. Second, these remedies, more than any other traditional privacy tort action, are based on property theory. In other words, the wrong to be righted is committed by one who appropriates for his or her own benefit another person's name or likeness. This principle has evolved into two separate causes of action: appropriation of personality and right of publicity.

The plaintiff's identity distinguishes these two actions. One tort is an invasion of the psyche, whereas the other is an invasion of the pocketbook.[1498] These are separate torts under section 46 of the *Restatement (Third) of Unfair Competition*[1499] and under section 652C of the *Restatement (Second) of Torts.*[1500] The unfair-competition tort is defined as a right of publicity, whereas the other tort is appropriation of personality. The *Restatement (Second) of Torts* suggests that although the appropriation right acknowledges the importance of dignity, the right is, by nature, a property right. Consequently, each of these torts designed to protect against unauthorized publication is based on property law.

Although newsworthiness is not necessarily a defense, some statutes allow recovery only if a person's identity is used in advertising. Therefore, under those statutes, the use of a person's name in news, art, or literature is not a violation.

This remedy could be expanded by allowing for recovery for any commercial use of a person's identity, as opposed to solely for advertising. In fact, the Florida statute includes such broad language, but the Florida

---

[1497] For a discussion of these remedies, see *infra* Chapter IV, § F.

[1498] 1 McCarthy, *supra* note 905, § 5:61, at 5–110.

[1499] The *Restatement* states in part, "One who appropriates the commercial value of a person's name, likeness, or other indicia of identity for purposes of trade is subject to liability. . . ." Restatement (Third) of Unfair Competition § 46 (1995).

[1500] Restatement (Second) of Torts § 652C (1977).

Supreme Court has construed the statute only to include advertising, despite the statutory language.[1501] The result of the advertising limitation is that this tort becomes very limited. The remedy should allow recovery against commercial exploitation beyond advertising.

The expansion of this remedy also could allow broader recovery. For example, in *Grant v.* Esquire, *Inc.*, the court awarded both property-related damages and damages for emotional distress.[1502] The threshold right protected was *Esquire*'s misuse of Mr. Grant's personality. But the court then allowed recovery for emotional distress. Could this formula be used to allow a noncelebrity to gain access to a better remedy? Yes.

7. Use State Constitutional Rights to Blaze a Legal Trail

State constitutions consistently have been interpreted as more stringent and comprehensive than the federal constitution in protecting privacy. Accordingly, some privacy interests may be recognized first in the states. For example, in *State v. Wasson*, the Kentucky Supreme Court found a statute criminalizing homosexual sodomy unconstitutional before the U.S. Supreme Court reached a similar result.[1503]

In the area of decisional privacy, the states often have gone further than the federal government. For example, Oregon has a more far-reaching right-to-die policy than has been allowed nationally by the Supreme Court.[1504] In fact, the federal government unsuccessfully challenged the Oregon policy.[1505]

The fact that a substantial number of states have constitutional privacy provisions gives rise to more opportunities to define the limits of

---

[1501] The Florida statute provides, "No person shall publish, print, display or otherwise publicly use for purposes of trade or for any commercial or advertising purpose the name, portrait, photograph, or other likeness of any natural person without the express written or oral consent to such use. . . ." FLA STAT. § 540.08 (1998). In Tyne v. Time Warner Entertainment Co., 901 So. 2d 802, 805 (Fla. 2005), the Florida Supreme Court said that "section 540.08, by prohibiting the use of one's name or likeness for trade, commercial or advertising purposes, is designed to prevent the unauthorized use of a name *to directly promote the product or service of the publisher*. Thus, the publication is harmful not simply because it is included in a publication that is sold for a profit, but rather because of the way it associates the individual's name or his personality with something else."

[1502] 367 F. Supp. 876 (S.D.N.Y. 1973).

[1503] *See* 842 S.W.2d 487 (Ky. 1992).

[1504] *See* Oregon Death with Dignity Act, OR. REV. STAT. §§ 127.800–.897 (2007).

[1505] *See* Gonzales v. Oregon, 546 U.S. 243 (2006).

privacy. Although informational privacy is clearly not defined as a fundamental right under the federal Constitution, some states consider informational privacy a fundamental right.[1506]

So the states, as "laboratories of democracy," may be the proving grounds for privacy policy. Individuals injured by intrusions should carefully examine state law and constitutional protections, since there is a real likelihood that the available state protection exceeds federal protections.

For those states without constitutional privacy provisions, the addition of such a right would provide significant and real additional protections. Because most states do not have a constitutional privacy provision, citizens concerned about privacy rights should evaluative how to add that specific right to their constitution.[1507] One need only review the cases implementing state provisions to see the substantial expansion of individual rights.[1508]

8. Expand Common-Law Remedies to Address Current Abuses

a. Conversion[1509]

The tort of conversion is not usually cited as a remedy for enforcing the right to privacy. However, if one accepts the property theory, then one accepts conversion as a remedy.[1510] The tort of conversion arises if there is wrongful interference with one's right of possession. If a person's control or possession of property is denied because of the actions of another, the tort of conversion is a possible tool. Conversion can be applied to either tangible or intangible property. Thus, information, data, images, and other key elements affecting privacy may be protected under a claim for conversion. This action, like trespass to chattels, is based on the acceptance of the property theory[1511] to allow an individual a series of property-related remedies.

[1506] *See* Rasmussen v. South Fla. Blood Servs., 500 So. 2d 533, 534 (Fla. 1987) (ruling that the privacy rights of blood donors (which fostered the ability to obtain more donations) outweighed a blood recipient's right to know if one of the donors from whom he received blood had AIDS).

[1507] *See infra* Appendix II.

[1508] *See* Chapter VII, § B-1. *See, e.g.*, Winfield v. Div. of Pari-Mutuel Wagering, 477 So. 2d 544, 547 (Fla. 1985) (adopting the "compelling state interest" standard to justify an invasion of privacy and shifting the burden to the state to justify an intrusion of privacy).

[1509] Susan E. Gindin, *Lost and Found in Cyberspace*, 34 SAN DIEGO L. REV. 1153 (1997).

[1510] See the discussion on the property theory *supra* Chapter IV, § F.

[1511] *See infra* Chapter III.

b. Trespass to Chattels

Trespass is a remedy to punish intrusion. The challenge is to redefine contemporary intrusions to allow this remedy to be effective in today's world.

Professor Michael Siebecker argues that the common practice of using pieces of data known as cookies[1512] to gather specific consumer information and track an Internet user's browsing habits, which are then used to profile individual Internet visitors, actually represents a common-law trespass to chattels.[1513] According to Siebecker, there has been a dearth of court cases dealing with Internet advertisers' use of cookies to gather information on consumer activity.[1514] Siebecker believes that earlier court precedent regarding the use of the trespass-to-chattels tort to enjoin the use of Internet "spam" advertising means that courts will look favorably on claims that implanting cookies on personal computers could be a trespass to chattels. Using the common-law remedy of trespass to chattels is not a guaranteed remedy, but Siebecker concludes that the likelihood of success of such a strategy is strong.[1515]

How to impose damages is a tough issue. Would damages be only the cost of the minimal memory space used? A better valuation would be an assessment of the value companies would pay to advertise on individual computers. The theory is that they are trespassing on the property of another to advertise. Collectively, that amount would be substantial and could justify a class-type action.

[1512] Cookies are defined by webopedia at http://www.webopedia.com/TERM/c/cookie.htm (last visited May 18, 2008), as "a message given to a web browser by a web server. The browser stores the message in a text file. The message is then sent back to the server each time the browser requests a page from the server. The main purpose of cookies is to identify users and possibly prepare customized Web pages for them. When you enter a Web site using cookies, you may be asked *to* fill out a form providing such information as your name and interests. This information is packaged into a cookie and sent to your Web browser which stores it for later use. The next time you go to the same Web site, your browser will send the cookie to the Web server. The server can use this information to present you with custom Web pages. So, for example, instead of seeing just a generic welcome page you might see a welcome page with your name on it.

The *name cookie* derives from UNIX objects called *magic cookies*. These are tokens that are attached to a user or program and change depending on the areas entered by the user or program.

[1513] *See* Siebecker, *supra* note 113, at 894.

[1514] *Id.* at 900.

[1515] *Id.*

c. Intentional Infliction of Emotional Distress

The tort of intentional infliction of emotional distress is another remedy that may be further expanded to protect privacy. This tort occurs if a person acts intentionally or recklessly in a manner that is extreme and outrageous enough to cause the plaintiff severe emotional distress.[1516] This tort can serve as an effective proxy for public disclosure of private facts, but the plaintiff must show the defendant's intent. Further, because the issue is wrongful conduct, protected speech is not a defense. Therefore, intentionally outrageous conduct will support liability.

One example described in this book could give rise to intentional infliction of emotional distress. The *True Stories from the Morgue* case involved the intentional display on television of an autopsy of a close relative.[1517] If the plaintiff could show the requisite intent, this case would be a perfect example of intentional infliction of emotional distress.

d. Utilize Expanded Contract Theories

As described earlier any direct violation of privacy agreement will be actionable.[1518] A more expansive use of contract theory based on unjust enrichment and implied contract may provide new remedies for intrusion and misuse of information.

1. Unjust Enrichment

As a common-law remedy, unjust enrichment allows for restitution, which is the restoration of the benefit of money, services, or goods that unjustly benefit another.[1519] Unjust enrichment is an equitable remedy that is available when no other remedy at law is applicable. Restitution via unjust enrichment is a remedy designed to prevent a person from retaining property to which the person is not justly entitled.[1520]

To succeed on a claim of unjust enrichment, a plaintiff must prove (1) a benefit conferred on the defendant by the plaintiff; (2) an appreciation

---

[1516] Williams v. City of Minneola, 575 So. 2d 683, 690 (Fla. Dist. Ct. App. 1991) (recognizing that intentional infliction of emotional distress can occur through the release of information).

[1517] This case is discussed in Chapter VI, § K.

[1518] *See* Chapter IV, § E-4.

[1519] Krug v. Sanzaro, No. CV010454102S, 2004 Conn. Super. LEXIS 966 (Super. Ct. Mar. 30, 2004).

[1520] Rowland v. Carr, No. CA9727, 1986 Ohio App. LEXIS 9931 (Ct. App. Dec. 24, 1986).

or knowledge by the defendant of the benefit; and (3) the acceptance or retention by the defendant of the benefit under such circumstances as to make it inequitable for the defendant to retain the benefit without payment of its value.[1521]

This remedy could apply as an adjunct to appropriation of name or likeness. However, because it is based in contract principles, a suit on the theory of unjust enrichment may not benefit everyone alike. A person who appropriates the identity of a common person may be less enriched than one who appropriates the identity of a celebrity. Therefore, the common person, although injured, may not collect as much in restitution, because the benefit conferred may be less; the celebrity, however, would likely collect a much greater amount. But the ultimate issue is not how much the wronged persons identity is worth but how much the wrongdoer benefited. So even if an individual's identity were not highly valuable on the market, if someone profited greatly, then they are liable for the degree they benefitted. "Because the basic idea underlying the law of unjust enrichment is that it is inequitable for one party to receive a benefit from another without paying for it, the measure of damages is ordinarily some function of the defendant's gain, rather than the value of what is taken."[1522]

For example, a case was filed by the comedian Rodney Dangerfield's widow to prevent the broadcast of videos of Mr. Dangerfield recorded in his house by his producer, David Permut.[1523] Mr. Permut is said to be planning to edit the material into a film. If Mr. Permut profited from the showing or broadcast of such a film, there would likely be a claim for unjust enrichment. And, as a contract action, it could be brought by Mr. Dangerfield's estate.

Another example involves Virgin Mobile in Australia, which took images from the photograph-sharing Web site Flickr and used them in its advertising campaign. One photograph Virgin Mobile took from Flickr was that of a sixteen-year-old girl, Alison Chang. In the ad, the company printed one of its slogans, "Dump your pen friend," over Chang's picture,

---

[1521] *See* 26 Williston on Contracts § 68:5 (4th ed.) Chapter 68. Rescission *and* Restitution; Quasi Contractual Recovery.

[1522] Arthur Miller, *Common Law Protection for Products of the Mind: An "Idea" Whose Time Has Come*, 119 Harvard Law Review 703, 773 (2006).

[1523] The Associated Press, *Dangerfield's Widow Sues Over Film*, Sept. 22, 2007, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/09/22/AR2007092200801.html (last visited May 9, 2008).

and included another, "Free text virgin to virgin," beneath her photo. Virgin Mobile likely benefited from using the plaintiff's image in its advertising campaign. And because the photograph was chosen to be used in an advertising campaign, it is reasonable to assume that Virgin Mobile appreciated the benefit the use of Chang's likeness would confer. Finally, because Virgin Mobile used Chang's photograph without her consent and ostensibly profited from the use of her photo, it would be inequitable for Virgin Mobile to retain the benefit without payment of its value. However, although there appears to be a cause of action here, the actual value of just compensation for using her image may not be high.

This concept of unjust enrichment requires proof that there has been enrichment, but the remedy has the virtue of being based in property theory and contract theory. Therefore, this type of remedy may avoid First Amendment defenses because recovery is a contract-based equitable remedy to compensate a wrongful taking. The wrong involved is the taking, not the act of communicating information, which might be subject to free-press defenses.

II. Implied Contract

Another contract-based remedy may be available to protect disclosure of intimate information. Professor Andrew McClurg has proposed that implied contract could be used as a substitute for the tort of public disclosure of private facts.[1524] Indeed, others have argued that recovery through contract theory is the way to protect free speech yet provide a remedy for certain intrusions.[1525] The theory is that there is an implied promise not to reveal certain intimate information. McClurg cites the case of the Washingtonienne, in which a woman posted intimate details about a previous lover on her blog.[1526] Under this theory, the lovers impliedly imposed a restriction on their speech by entering into an intimate relationship, and the court should enforce that contract. To find such a contract, a court must necessarily evaluate the context of the relationship and the information involved to determine the rationality of deeming it a contract.

[1524] McClurg, *supra* note 1373.

[1525] *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 Stan. L. Rev. 1049 (2000).

[1526] *See* discussion *infra* Chapter VI, § I.

Although the proof may be challenging, this theory is certainly worth exploring in the courts. Further, the idea finds support in the cause of action for breach of confidence, which has essentially become Great Britain's substitute for privacy torts.[1527] In sum, a person faced with the disclosure of intimate details should definitely consider using the implied-contract theory.

9. Evaluate Transnational Remedies

There will be instances when an individual may obtain a remedy and recovery in a foreign jurisdiction that is not available to him or her in the United States. A specific example is the *Gutnick* case discussed previously: the statement made about the Australian businessman would have been protected speech in the United States, but it was not protected speech in Australia and the defendant was held liable.[1528] Some "believe that the U.S. First Amendment reflects universal values and is somehow written into the architecture of the Internet. But the First Amendment does not reflect universal values; to the contrary, no other nation embraces these values, and they are certainly not written in the Internet's architecture."[1529] So we should not be surprised if a person with proper jurisdiction in another country receives relief that would not be available in the United States for the publication of information on the Internet.

Actions by multinational companies may violate an individual's privacy right under the laws of some nations, but not under those of others. Even so, the fact that companies do business worldwide makes them susceptible to public pressure for violating privacy rights.[1530] For example, London-based Privacy International graded the various search engines in a report released on June 9, 2007. The company gave Google its lowest grade out of twenty-two surveyed companies and said that the company had "comprehensive consumer surveillance and entrenched hostility to privacy."[1531] This kind of international scrutiny may provide a path for privacy advocates in various countries.

[1527] *See* Wacks, *supra* note 428 (discussing the theory employed in British courts).

[1528] *See supra* text accompanying note 484.

[1529] GOLDSMITH & WU, *supra* note 484, at 157.

[1530] *See* Skarda-McCann, *supra* note 484.

[1531] Associated Press, *Watchdog Group Slams Google's Privacy Policies*, GAINESVILLE SUN, June 10, 2007, at 7A.

No doubt individuals will look to sympathetic jurisdictions when they have been harmed by international or transborder communications. Given the global nature of communications, more and more individuals may be able to shop for better forums.

American celebrities and foreign public figures have been using the more expansive protections under European law to obtain tort recovery from the media. This tactic has been called "libel tourism." Britney Spears settled a lawsuit against the *National Enquirer* that she filed in Northern Ireland in late summer 2006.[1532] Spears is not the only celebrity to sue in the U.K. courts for libel. Paula Abdul, Whitney Houston, and Jennifer Lopez also have filed suits against American-based publishers in the European courts. But it is not just celebrities who are using the U.K. system to seek vindication for information published about them by the media. According to an article in the *Times*, the latest individuals to use the broad U.K. libel laws are businesspeople, not unlike the Australian businessman's use of the Australian courts in his suit against the *Wall Street Journal*.[1533]

These circumstances indicate that an intrusion that occurs in another jurisdiction may be treated far differently from the same intrusion in the United States and that such alternative remedies may become more popular.

[1532] Associated Press, *Tabloid Retracts Britney Spears Stories*, USA TODAY, July 18, 2006, *available at* http://www.usatoday.com/life/people/2006-07-18-spears-enquirer_x.htm.

[1533] *See* Mark Stephens, *New Celebrities of the Libel Courts*, TIMES (U.K.), July 18, 2006, *available at* http://business.timesonline.co.uk/tol/business/law/article687881.ece. It should be noted, however, that an article in the *Wall Street Journal* from late 2006 heralded a judicial decision in the House of Lords that narrowed, albeit only a little, the U.K. libel law. *See* Aaron O. Patrick, *U.K. British Court Ruling Gives Boost to Serious Journalism*, WALL ST. J., Oct. 12, 2006, at B1, *available at* http://online.wsj.com/public/article/SB116055935348389227-uzoY3SuOpLzgmhletBF_w6ghxj8_20061018.html?mod=blogs.

In *Jameel v. Wall Street Journal Europe*, [2006] UKHL 44, Saudi businessmen sued the *Wall Street Journal Europe* for libel because of a 2002 article published by the newspaper detailing investigations into the bank accounts of Saudi businesses suspected of funding terrorism. The *Wall Street Journal* lost the case at trial and was ordered by the jury to pay damages. On appeal, the House of Lords said that the newspaper article may have been privileged under what is called the *Reynolds* defense, which protects matters that are of public interest. (The privilege gets its name from the case *Reynolds v. Times Newspapers Ltd.*, [2001] 2 A.C. 127.) Lord Bingham noted, however, that what engages the interest of the public is not always in the public interest. *Jameel*, [2006] UKHL 44, ¶ 31. (Although traditionally thought of solely as a legislative body, the House of Lords also acts as the highest court for the courts of the United Kingdom. A group called the Lords of Law decides cases appealed to the House of Lords.).

Another variation of this issue is the increased use of "outsourcing" of data compilations. Violations of an American's citizen's privacy may occur in another country, by a company's outsourced provider or by a hacker in another country.[1534] Intrusions are becoming truly global, and remedies must be global as well.

C. Use Personal and Technical Means to Protect Privacy

1. Evaluate Practical and Technological Means to Reduce Loss of Privacy

Although technology is part of the problem in protecting personal privacy, it also can be part of the solution. Citizens can take actions that will limit their exposure to abuse, but ultimately legal protections are still the key to protecting personal privacy.

A key technological strategy in protecting privacy is making communication anonymous. This strategy does not protect the interception of data as much as it hides the source of a signal or the recipient of a message. For example, a political dissident in China can use an anonymizing Web browser to read the news of the Western press or post messages on a blog promoting democracy. Another example is the use of prepaid calling cards or prepaid mobile phones that may leave conversations open to eavesdropping but can make identifying the speakers difficult. Anonymity can protect privacy.

Requiring authentication of identity can also protect privacy in a different context. Authentication may be used as a privacy tool. This method requires users, communicating parties, or persons accessing information to verify their identity.[1535] If authentication is required, only an authorized person should have access to the information sought. The simplest form of authentication is the use of a password or personal identification number ("PIN"). More advanced forms include biometric identification, like iris and fingerprint scans.[1536] Authentication protocols may require verification of multiple pieces of information. The future might even

---

[1534] *See, e.g.*, Brian Krebs, *Shadowy Russian Firm Seen as Conduit for Cybercrime*, WASH. POST, Oct. 13, 2007, at A15 (discussing the "Russian Business Network," an Internet service provider that provides access for a multitude of cybercrimes).

[1535] WESTBY, *supra* note 414, at 200.

[1536] *Id.* at 202.

bring DNA authentication.[1537] The goal of authentication is to guard against unauthorized access to private information.

Encryption also may be used to protect privacy. Any data, such as e-mails, voice communications, images, or other files, can be scrambled in such a way that the content is meaningless without a decryption key.[1538] In this way, both stored and live communications can remain secure, and unauthorized users can be prevented from gaining access.

After information has already been created and stored, erasing data is another method for protecting privacy.[1539] Although pressing the delete button may appear to eliminate a file or e-mail, traces may still remain on a computer. Specially designed software programs may be able to retrieve information the user thought was deleted. A user may obtain software to securely and permanently delete information, such that all traces of the data are destroyed, by repeatedly writing over the physical areas on the storage medium where that information was once stored. Computer files often contain metadata, information about the data stored, such as the data's creator and editor as well as timestamps. Deleting this information also may serve to protect privacy. Thus, the pool of information available to threaten one's privacy can be minimized and managed.

2. Practical Personal Steps

Protecting one's own privacy is no easy task. Although the previously mentioned technological methods for protecting privacy are useful, the methods are not a panacea. There is little one can do to protect one's privacy from personal blogs with no quality-control editors, from CCTV cameras, or from GPS devices in some cell phones.

[1537] *Id.*

[1538] WESTBY, *supra* note 376, at 197.

[1539] But the erasure must be complete and effective. When a user "deletes" a file, not all traces of that file are removed, and often, the entire file can be recovered using readily available data-recovery tools. For a technical discussion of how computers store and erase files, see ALBERT J. MARCELLA & ROBERT S. GREENFIELD, CYBER FORENSICS: A FIELD MANUAL FOR COLLECTING, EXAMINING, AND PRESERVING EVIDENCE OF COMPUTER CRIMES 48–51 (2002). The practice of selling used cellular phones is a key example of how one's sensitive personal information can be put at risk. Cellular phones use flash memory to store phone numbers and other data. Information presumed to be erased often can be easily accessed using inexpensive software available on the Internet. *See* Ted Bridis, *Cell Phones Spill Secrets*, MSNBC, Aug. 30, 2006, http://www.msnbc.msn.com/id/14588433.

The FTC offers minimal instruction on how to protect one's own privacy.[1540] Some tips offered by the FTC are do not carry any more credit cards or identification cards in your purse or wallet than is necessary, order credit reports from the three credit-reporting agencies once a year, and create difficult passwords for your online information.[1541]

A person may choose to exercise some control over how his or her information is used and stored. For instance, a national "Do Not Call" registry (www.donotcall.gov) allows individuals to stop (most) telemarketers from calling their phones. Individuals may request to stop receiving preapproved credit offers via www.optoutprescreen.com. Also, individuals may contact many of the data brokers, such as Acxiom and Abacus, to remove their names from the mailing lists that they sell to others.

Individuals may obtain information stored about themselves for free, usually annually, to ensure the accuracy of the information. Once a year, an individual can contact the Medical Information Bureau ("MIB") to receive a free copy of his or her MIB report, which contains medical information stored in the insurance industry database. Likewise, one may obtain a free annual credit report via www.annualcreditreport.com. Further, HIPAA gives patients the right to access their medical records at any time to check for discrepancies.

One can be proactive by giving required information only when requested and taking business elsewhere if not satisfied with the manner in which various companies handle personal information. Finally, privacy can be better protected by taking advantage of the opt-out opportunities provided by credit-card companies and others to limit the distribution of personal information.

The bottom line is that many of these tips for privacy protection are limited and do not comprehensively protect against the various potential intrusions by the government, the press, individuals, or data brokers. It is also clear that although following these steps might reduce the number of telemarketers that have your phone number, or reduce the number of mistaken transactions on your credit report, there is no foolproof safeguard against the improper use of personal information, and we must live with and react to this harsh reality.

[1540] FTC, Privacy: Tips for Protecting Your Personal Information, http://www.ftc.gov/bcp/conline/pubs/alerts/privtipsalrt.shtm (last visited May 9, 2008).

[1541] *Id.*

CHAPTER VIII

Conclusion

Privacy, as a central part of personal liberty and individuality, is a touchstone of American democracy and a generally accepted, yet amorphous, global right. A combination of forces from the government, an intrusive society, commercial interests, and segments of the press are, in effect, crushing the individual's right to be let alone. If they were concerned about an intrusive world in 1890, what might Warren and Brandeis think today? In 2008, the law is ill equipped to protect citizens from the private and public assault on their privacy. This onslaught is not the result of some grand conspiracy. No conspiracy could work so well. In fact, the government, the information industry, and the press are, at least on the surface, doing what the public demands: they are providing security, needed information, and the news and gossip that the public wants. The status of our collective privacy is unpredictable, inconsistent,[1542] and changing continually[1543]—a reflection of a society with changing mores and changing technology.

The confluence of technology and the motivations of data brokers are causing the individual to be treated more and more as a statistic. The threshold question is, do we care? Well, we do when we are hurt. We care when the government dictates that a loved one must die painfully.

[1542] In Alaska you have an expectation of privacy for smoking marijuana in your home, but in Florida you do not have an expectation of privacy in smoking tobacco if you want a public job.

[1543] Examples of complete changes in policy in the last century include policies regarding abortion, interracial marriage, and homosexual sex.

We care when we are crime victims scrutinized by the press. We care when we do not get a job because of inaccurate criminal records.

As part of today's culture and society, no individual is immune. As suggested in the introduction, there are very few private aspects of a "day in the life" of a modern citizen. Further, as this book has made clear, the legal solutions are piecemeal and incremental, requiring the public to demand remedies for violations of their right to privacy. The impact is so vast and comprehensive that no one ethnic, religious, or other group is singled out. We are all part of the privacy interest group. So far, most of us are underinformed as to what is happening to us and are largely unaware of any effective legal remedies.

However, there are legal remedies for privacy violations. And, if the privacy right is important, the courts have an obligation to fashion effective options from the myriad remedies. There will be no single sweeping reform that will bestow privacy on each of us. The forces and policies that support intrusions on individual privacy are too substantial and in some cases, are supported by most of the public. For example, most of the public supports warrantless searches and constant camera surveillance to counter violence and terrorism. Likewise, most of the public shows a voyeuristic interest in tabloids and disaster journalism, at least until someone in their own family becomes an unwilling subject. This most individual of rights requires our personal commitment to protect ourselves through our personal choices and actions and our advocacy.

The central lessons of a study of privacy today are as follows:

- No universal agreement exists on the scope of privacy because of inherent moral, political, and perceptual differences.
- Privacy is a broad concept affecting multiple facets of human existence that individuals and governments value as a general principle.
- A single policy is not probable or practical to protect privacy across the globe or even across the county.
- A broader understanding of the scope of privacy (i.e., recognizing which issues are important to individual liberty) is a prerequisite for protecting individual privacy.

The future of individuality and personal autonomy is a cause in need of a constituency. We need to evaluate why we tolerate intrusions on our individual privacy by the government, bloggers, the press, and our fellow citizens. The responsibility is ours. In the immortal words of the cartoon character Pogo, "we have met the enemy . . . and he is us."