PRIVACY AS CONTEXTUAL INTEGRITY

Helen Nissenbaum*

Abstract: The practices of public surveillance, which include the monitoring of individuals in public through a variety of media (e.g., video, data, online), are among the least understood and controversial challenges to privacy in an age of information technologies. The fragmentary nature of privacy policy in the United States reflects not only the oppositional pulls of diverse vested interests, but also the ambivalence of unsettled intuitions on mundane phenomena such as shopper cards, closed-circuit television, and biometrics. This Article, which extends earlier work on the problem of privacy in public, explains why some of the prominent theoretical approaches to privacy, which were developed over time to meet traditional privacy challenges, yield unsatisfactory conclusions in the case of public surveillance. It posits a new construct, "contextual integrity," as an alternative benchmark for privacy, to capture the nature of challenges posed by information technologies. Contextual integrity ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it. Building on the idea of "spheres of justice," developed by political philosopher Michael Walzer, this Article argues that public surveillance violates a right to privacy because it violates contextual integrity; as such, it constitutes injustice and even tyranny.

I. INTRODUCTION

Privacy is one of the most enduring social issues associated with information technologies. It has been a fixture in public discourse through radical transformations of technology from stand-alone computers, housing massive databases of government and other large institutions, to the current distributed network of computers with linked information systems, such as the World Wide Web, networked mobile devices, video and radio-frequency surveillance systems, and computer-enabled biometric identification. Among many privacy controversies that have stirred public concern, a particular set of cases, to which I have applied the label "public surveillance," remains vexing not only because these cases drive opponents into seemingly irreconcilable stances, but because traditional theoretical insights fail to clarify the sources of their controversial nature.[1] This Article seeks to shed light on the problem of

* Associate Professor, Department of Culture & Communication, New York University, East Building 7th Floor, 239 Greene Street, New York, New York 10003. E-mail address: helen.nissenbaum@nyu.edu.

Many people and institutions have inspired and helped me in this endeavor, beginning with the Institute for Advanced Study, School of Social Sciences, where I wrote and presented early drafts.

public surveillance first by explaining why it is fundamentally irreconcilable within the predominant framework that shapes contemporary privacy policy, and second by positing a new concept—contextual integrity—to explain the normative roots of uneasiness over public surveillance. This Article's central contention is that contextual integrity is the appropriate benchmark of privacy. Before taking up these general points, it is useful first to consider a few specific illustrations of public surveillance.

Case 1: Public Records Online. Local, state, and federal officials question the wisdom of initiatives to place public records online, making them freely available over the Internet and World Wide Web.[2] The availability to citizens of public records, such as arrest records; driving records; birth, death, and marriage records; public school information; property ownership; zoning and community planning records; as well as of court records, serves the unquestionable purpose of open government. Nevertheless, the initiatives to move these records online in their entirety, making them even more accessible, cause unease among many, including government officials and advocacy organizations, such as the National Network to End Domestic Violence and the American Civil Liberties Union.

State supreme courts, for example, with jurisdiction over court records, are mindful of concerns raised by advocates of victims of domestic violence and other crimes, among others, who point out the dangers inherent in these new levels of accessibility. Yet their worries seem paradoxical. The records in question are already publicly available. Computerizing and placing them online is merely an administrative

---

Drafts were further sharpened through opportunities to present at colloquia and workshops held at the New Jersey Bar Association, Princeton University's Program in Law and Public Affairs, University of British Columbia, University of California, San Diego, University of Maryland, University of Washington, and the Social Science Research Council. Colleagues who have shared essential insights and expertise include Grayson Barber, Rodney Benson, Aaron Goldberg, Jeroen van den Hoven, Natalie Jeremijenko, Bob Salmaggi, Bilge Yesil, and Michael Walzer. I received outstanding research and editorial assistance from Danny Bloch, Rachel Byrne, and Brian Cogan. Grants from the Ford Foundation (Knowledge, Creativity, and Freedom Program) and National Science Foundation (SBR-9729447 and ITR-0331542) have supported my research as well as the writing of this Article.

1. *See* Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 559 (1998).

2. *See* Robert Gellman, *Public Records—Access, Privacy, and Public Policy: A Discussion Paper*, 12 GOV'T INFO. Q. 391 (1995) (noting that restrictions do apply on access to government records). The point here is whether any changes are necessary in the transition from paper-based access to online access to these records.

move towards greater efficiency. Nothing has changed, fundamentally. Are these worries rational? Is there genuine cause for resistance?

Case 2: Consumer Profiling and Data Mining. Most people in the United States are aware, at some level, that virtually all their commercial activities are digitally recorded and stored. They understand that actions such as buying with credit cards, placing online orders, using frequent shopper cards, visiting and registering at certain websites, and subscribing to magazines leave digital trails that are stored away in large databases somewhere. Fewer are aware that this information is shipped off and aggregated in data warehouses where it is organized, stored, and analyzed. Personal data is the "gold" of a new category of companies, like Axciom, that sell this information, sometimes organized by individual profiles, to a variety of parties, spawning product, subscriptions, credit card, and mortgage offers, as well as annoying phone solicitations, special attention at airport security, and targeted banner and pop-up advertisements. When the popular media writes about these webs of personal information from time to time, many react with indignation. Why? Often the information in question is not confidential or sensitive in nature.

Case 3: Radio Frequency Identification (RFID) Tags. These tiny chips—which can be implanted in or attached to virtually anything from washing machines, sweaters, and milk cartons to livestock and, it is anticipated, one day, people—are able to broadcast information to radio signal scanners up to ten feet away. Although prospective users of these tags have lauded their tremendous promise for streamlining the stocking, warehousing, and delivery of goods, as well as in preventing theft and other losses, privacy advocates point out a worrisome possibility of a multitude of commodities with the capacity to disseminate information about consumers without their permission or even awareness. Why does this worry us? After all, information will be gathered mainly from open or public places where the powerful radio frequency emitters would most likely be located.

All three cases are spurred by technological developments and developments in their applications that radically enhance the ability to collect, analyze, and disseminate information.[3] Case 1 highlights how

3. It is important to note that we are not adopting a deterministic model either of technological development or of technology's impact on society. When we say that a technological development or an application of technology has had particular results, we assume an undeniably complex backdrop of social, political, economic, and institutional factors that give meaning, momentum, and direction to observed outcomes.

great increments in the ability to disseminate and provide access to information prompt disquiet, particularly at the prospect of local access giving way to global broadcast. This worry seems to be a contemporary version of the one evoked in Samuel Warren and Louis Brandeis' seminal work calling for a right of privacy in the face of then-new developments in photographic and printing technologies.[4]

In Case 2, it is advances in storage, aggregation, analysis, and extraction (mining) of information both online and off-line that spur questions.[5] One of the earliest cases to spur a grass-roots, Internet-mediated storm of protest centered on Lotus Marketplace: Households, a database intended for distribution on CD-ROMs. The database contained aggregated information about roughly 120 million individuals in the United States, including names, addresses, types of dwelling, marital status, gender, age, approximate household income, and so forth. Eventually, the two companies collaborating on the venture, Lotus Development and Equifax Inc., backed off, citing negative publicity.[6]

Case 3 focuses attention on enhanced modes of gathering or capturing information as in automated road toll systems like EZ Pass, video surveillance and face recognition systems, web browser cookies, biometrics, thermal imaging, and more.[7]

One could read these cases simply as public policy disputes in which groups with opposing interests face off against one another, each seeking to promote its own goals, desires, preferences, and interests above those of opponents in the dispute.[8] This reading is not entirely unproductive as

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

5. *See* LAURA J. GURAK, PERSUASION AND PRIVACY IN CYBERSPACE: THE ONLINE PROTESTS OVER LOTUS MARKETPLACE AND THE CLIPPER CHIP (1997). Another case that has touched off a flurry of concern and protest is profiling of online advertising companies, such as Doubleclick, that monitor the online web-surfing behaviors of millions of users, frequently merging online records with other information about these users. See the website of the Electronic Privacy Information Center for a full account of this case at http://www.epic.org (last visited Jan. 17, 2004).

6. *See* Nissenbaum, *supra* note 1.

7. *See, e.g.*, JULIAN ASHBOURN, THE BIOMETRIC WHITE PAPER (1999), *available at* http://www.jsoft.freeuk.com/whitepaper.htm; Colin J. Bennett, *Cookies, Web Bugs, Webcams, and Cue Cats: Patterns of Surveillance on the World Wide Web*, 3 ETHICS & INFO. TECH. 197 (2001); Roger A. Clarke, *Human Identification in Information Systems: Management Challenges and Public Policy Issues*, INFO. TECH. & PEOPLE, Dec. 1994, at 6, *available at* http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html; Linda Greenhouse, *Justices Say Warrant Is Required in High-Tech Searches*, N.Y. TIMES, June 12, 2001, at A1; Alice McQuillan & James Rutenberg, *E-ZPass Slows Those Trafficking in Wrong*, DAILY NEWS, Nov. 3, 1997, at 3, 49.

8. *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY (1995) (providing a rich reading of many interest based privacy disputes during the

it at least requires an understanding of how technologies can affect diverse social groups differentially and how these differences suggest particular reactive policies, which in turn have the capacity to shape further technical developments.

In this Article, however, the fluctuations of public interest politics, public policy, and at times law, are not central; the focus, rather, is the foundation for policy and law expressed in terms of moral, political, and social values. We will not be pursuing or presenting specific policies and strategies for achieving them, but trying to explain, systematically, *why* particular policies, laws, and moral prescriptions are correct. Another way of saying this is that our purpose is to articulate a justificatory framework for addressing the problem of public surveillance including the many disputes typified by our Cases 1, 2, and 3 above. Such a framework would not only address specific cases before us, but would allow them to serve as precedents for future disputes in a way that Lotus Marketplace: Households, despite its successful outcome, never did. A justificatory framework linking cases across time provides rationality to their resolution that rises above the power plays of protagonists and antagonists.[9]

Before proceeding, it is necessary to define boundaries and terminology. The scope of privacy is wide-ranging—potentially extending over information, activities, decisions, thoughts, bodies, and communication. A full theory of privacy would need to take account of all these dimensions, even if, eventually, it asserted theoretically grounded exclusions. Such is frequently the case for accounts of privacy that do not, for example, consider the right to abortion as a component of a right to privacy.[10] The goals of this Article are more limited, not aiming for a full theory of privacy but only a theoretical account of a

---

period roughly from 1890 through 1991); *see also* SUSANNAH FOX, THE PEW INTERNET & AM. LIFE PROJECT, TRUST AND PRIVACY ONLINE: WHY AMERICANS WANT TO REWRITE THE RULES (2000) (survey of popular privacy preferences), *available at* http://www.pewinternet.org/reports/pdfs/PIP_Trust_Privacy_Report.pdf; JOSEPH TUROW, ANNENBURG PUB. POLICY CTR. OF THE UNIV. OF PA., AMERICANS & ONLINE PRIVACY: THE SYSTEM IS BROKEN (2003) (survey of popular privacy preferences), *available at* http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf.

9. This is in contrast with the case of Lotus Marketplace: Households, where privacy advocates arguably "won" but not in a precedent setting way in the current landscape of data collection, aggregation, and analysis.

10. This is sometimes called "constitutional privacy." For discussion of the full picture and opposing views, see ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY (1988); JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY (1997); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980).

right to privacy as it applies to information about people. Furthermore, it undertakes this aim in relation to individual, identifiable persons—not taking up questions about the privacy of groups or institutions. Finally, for purposes of precision, we will reserve the term "personal information" for the general sense of information about persons; "sensitive" or "confidential" will indicate the special categories of information for which the term "personal information" is sometimes used.

The balance of this Article is divided into two parts. The first part posits and discusses a framework consisting of three conceptually independent principles that define an approach to privacy protection that dominates contemporary public discussion, policy, and legal landscape.[11] It includes subparts devoted to each of the principles, respectively,[12] and a subpart on contentious cases in which opposing sides disagree on whether given principles apply to the cases in question.[13] The final subpart explains why public surveillance is problematic for this three-principle framework. Unlike the contentious cases discussed before, public surveillance seems to fall entirely outside its range of application.[14]

The second part of this Article proposes an alternative account of privacy in terms of "contextual integrity"—an introduction to the layer of social analysis upon which the idea of contextual integrity is built.[15] Developed by social theorists, it involves a far more complex domain of social spheres (fields, domains, contexts) than the one that typically grounds privacy theories, namely, the dichotomous spheres of public and private. Following this introduction, the first two subparts describe, respectively, two "informational norms" that govern these contexts of social life, namely, appropriateness and distribution.[16] The third subpart, anticipating challenges to the normative force of contextual integrity, gives an account of its normative foundations.[17] The fourth subpart shows how contextual integrity may be applied to the three Cases described in this Article's introduction, showing that it easily captures

11. *See infra* Part II.
12. *See infra* Part II.A–C.
13. *See infra* Part II.D.
14. *See infra* Part II.E.
15. *See infra* Part III.
16. *See infra* Part III.A–B.
17. *See infra* Part III.C.

their problematic roots.[18] In the final subpart, the approach to privacy through contextual integrity is contrasted with other theoretical approaches that also extend beyond the three-principle framework.[19]

II. THREE PRINCIPLES

The search for a justificatory framework is a search for theories and principles that yield reasons for favoring one general policy or another and for resolving particular cases. It is useful to understand why prevailing principles that have guided so much of contemporary privacy policy and law in the United States offer little guidance in many hard cases, including the three described at the beginning of this Article. Surveying the fields of public policy development, regulation and statutory law, court decisions, and social and commercial practices during the twentieth century we find that three principles dominate public deliberation surrounding privacy. The three principles are concerned with: (1) limiting surveillance of citizens and use of information about them by agents of government, (2) restricting access to sensitive, personal, or private information, and (3) curtailing intrusions into places deemed private or personal.

A. Principle 1: Protecting Privacy of Individuals Against Intrusive Government Agents

This principle comes into play when questions arise about intrusions by agents of government (or government agencies or representatives) who are accused of acting overzealously in collecting and using personal information. This principle can be understood as a special case of the powerful, more general principle of protecting individuals against unacceptable government domination. Privacy is thus protected by reference to general, well-defined, and generally accepted political principles addressing the balance of power, which, among other things, set limits on government intrusiveness into the lives and liberty of individuals. Data gathering and surveillance are among many forms of government action in relation to individuals needing to be stemmed.

In the United States, the Constitution and Bill of Rights[20] provide what is probably the most significant source of principles defining limits

18. *See infra* Part III.D.

19. *See infra* Part III.E.

20. U.S. CONST. amends. I–X.

to the powers of federal government in relation to the liberty and autonomy of individuals and individual states. They also serve as a powerful reference point for privacy protection. Although, as commonly noted, the U.S. Constitution does not explicitly use the term "privacy," many legal experts agree that various aspects of privacy are, in fact, defended against government action through several of the amendments, including the First (speech, religion, and association), Third (quartering soldiers), Fourth (search and seizure), Fifth (self-incrimination), Ninth (general liberties), and even the Fourteenth (personal liberty versus state action) Amendments. The U.S. Constitution, as we know, draws on other tracts, including English common law and works of the great political philosophers that have contributed fundamentally to defining the powers and limits of governments in democratic societies embraced not only in the United States, but in the laws and political institutions of western democracies and many beyond.[21]

Not all legal restraints on governmental gathering and use of information about individuals stem from the Constitution. Others have been expressed in state and federal statutes, with a notable peak of activity in the mid- to late 1960s, coinciding with a steady increase in the creation and use of electronic databases for administrative and statistical purposes.[22] Priscilla Regan's detailed account of privacy policy from the 1960s through the 1980s suggests that informational privacy became a topic of intense public scrutiny around the late 1960s following a proposal in 1965 by the Social Science Research Council to create a Federal Data Center to coordinate centrally the use of government

21. I refer very generally to core political works that have shaped contemporary, liberal democracies. *See, e.g.*, THOMAS HOBBES, LEVIATHAN (C.B. Macpherson ed., Penguin Books 1981) (1951); JOHN LOCKE, THE SECOND TREATISE OF GOVERNMENT (Thomas P. Peardon ed., Macmillan Publ'g Co. 1986) (1690); JOHN STUART MILL, ON LIBERTY (Gertrude Himmelfarb ed., Penguin Books 1982) (1859); JEAN-JACQUES ROUSSEAU, THE SOCIAL CONTRACT (Maurice Cranston trans., Penguin Books 1968) (1762).

22. For discussions of the trend toward increasing reliance upon computerized record-keeping systems by government and other agencies, see, for example, COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES (1992); DAVID BURNHAM, THE RISE OF THE COMPUTER STATE (1983); DAVID H. FLAHERTY, PRIVACY AND GOVERNMENT DATA BANKS: AN INTERNATIONAL PERSPECTIVE (1979); KENNETH C. LAUDON, DOSSIER SOCIETY: VALUE CHOICES IN THE DESIGN OF NATIONAL INFORMATION SYSTEMS (1986); GARY T. MARX, UNDERCOVER: POLICE SURVEILLANCE IN AMERICA (1988); REGAN, *supra* note 8; JAMES B. RULE, PRIVATE LIVES AND PUBLIC SURVEILLANCE (1973); Richard P. Kusserow, *Fighting Fraud, Waste, and Abuse*, 12 BUREAUCRAT 23 (1983); James B. Rule et al., *Documentary Identification and Mass Surveillance in the United States*, 31 SOC. PROBS. 222 (1983).

statistical information.[23] This culminated in the Privacy Act of 1974,[24] which placed significant limits on the uses to which agencies of federal government could put the databases of personal information.[25] Many other statutes followed that placed specific restrictions on government agents in their collection and use of personal information.[26]

For purposes of our discussion, more relevant than the specific details about legal restrictions on government agents is the general source of momentum behind these restrictions, in particular, a principled commitment to limited government powers in the name of individual autonomy and liberty. To the extent that protecting privacy against government intrusion can be portrayed as an insurance policy against the emergence of totalitarianism, the rhetoric of limiting government powers can be parlayed into protection of privacy. During the 1950s until the end of the Cold War, when regimes in the East loomed vividly in public consciousness and fictional constructions, like George Orwell's Big Brother in *1984*,[27] entered the public imagination,[28] the U.S. Department of Health, Education, and Welfare's Secretary's Advisory Committee on Automated Personal Data Systems found a receptive audience for their seminal 1973 report on the impacts of computerized record-keeping on

23. *See* REGAN, *supra* note 8.

24. 42 U.S.C. §§ 2000aa–2000aa-12 (2000).

25. *Id*. We should not exaggerate the scope of success. The Privacy Act of 1974 addressed only government record-keeping, bowing to the lobbying of large private record-keeping institutions (like banks and insurance companies) to remove their interests from the general privacy rights umbrella. *See* REGAN, *supra* note 8, at 77–85; *see also* JERRY BERMAN & JANLORI GOLDMAN, A FEDERAL RIGHT OF INFORMATIONAL PRIVACY: THE NEED FOR REFORM (1989).

26. *See, e.g.*, Computer Matching and Privacy Protection Act (CMPPA), 5 U.S.C. § 552a (2000); Right to Financial Privacy Act, 12 U.S.C. §§ 3401–3422 (2000); Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified in scattered section of 18 U.S.C.).

27. GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949).

28. For example, recall the popularity of Arthur Koestler's *Darkness at Noon* and the Broadway stage adaptation by Sidney Kingsley. ARTHUR KOESTLER, DARKNESS AT NOON (Daphne Hardy trans., The Modern Library 1941); SIDNEY KINGSLEY, DARKNESS AT NOON (1951). In popular culture, for example, consider the success of Bob Dylan's song *Subterranean Homesick Blues* (critical of overzealous government); Janis Joplin's backup band *Big Brother and the Holding Company*; Stills, Crosby, Nash, and Young's song *Ohio* (regarding the Kent State massacre—"tin soldiers and Nixon coming"); and Francis Ford Coppola's movie *The Conversation* (1974). In news media, for example, review Anne R. Field, *Big Brother Inc. May Be Closer Than You Thought*, BUS. WK., Feb. 9, 1987, at 84. In scholarly literature see, for example, John Shattuck, *In the Shadow of* 1984*: National Identification Systems, Computer-Matching, and Privacy in the United States*, 35 HASTINGS L.J. 992 (1984). *See also* REGAN, *supra* note 8, at 81 (providing references to Big Brother rhetoric that peppered floor debates over privacy policy in both chambers of Congress).

individuals, organizations, and society as a whole.[29] The report emphasized this concern for balancing power, and for limiting the power of state and large institutions over individuals by warning that "the net effect of computerization is that it is becoming much easier for record-keeping systems to affect people than for people to affect record-keeping systems."[30] Further, "[a]lthough there is nothing inherently unfair in trading some measure of privacy for a benefit, both parties to the exchange should participate in setting the terms."[31] The lasting legacy of the report and its Code of Fair Information Practices is the need to protect privacy, at least in part, as one powerful mechanism for leveling the playing field in a game where participants have unequal starting positions.

B. Principle 2: Restricting Access to Intimate, Sensitive, or Confidential Information

This principle does not focus on who the agent of intrusion is but on the nature of information collected or disseminated—protecting privacy when information in question meets societal standards of intimacy, sensitivity, or confidentiality. Capturing the notion that people are entitled to their secrets, this principle finds robust support in scholarship developed from a variety of disciplinary perspectives, is well entrenched in practical arenas of policy and law, and is frequently raised in privacy deliberations in public or popular arenas. Several prominent philosophical and other theoretical works on privacy hold the degree of sensitivity of information to be the key factor in determining whether a privacy violation has occurred or not. These works seek to refine the category of so-called "sensitive information" and explain why the sensitivity of information is critical in defending privacy against countervailing claims.[32]

---

29. SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973) [hereinafter RIGHTS OF CITIZENS], *available at* http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm. There is no doubt that security worries following the September 11 attacks have lessened the dominance of public resistance to overly intrusive government agencies in lives of individuals, as seen in general willingness to accept legislation like the PATRIOT Act. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

30. RIGHTS OF CITIZENS, *supra* note 29.

31. *Id*.

32. *See, e.g.*, RAYMOND WACKS, PERSONAL INFORMATION: PRIVACY AND THE LAW (1989) (devoted almost entirely to establishing the foundational definition of "sensitive information");

In the United States legal landscape, sensitive information is accorded special recognition through a series of key privacy statutes that impose restrictions on explicitly identified categories of sensitive information. Examples include the Family Educational Rights and Privacy Act of 1974,[33] which recognizes information about students as deserving protection; the Right to Financial Privacy Act of 1978,[34] which accords special status to information about people's financial holdings; the Video Privacy Protection Act of 1988,[35] which protects against unconstrained dissemination of video rental records; and the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[36] which set a deadline for adoption of privacy rules governing health and medical information by the U.S. Department of Health and Human Services. Further, the common law recognizes a tort of privacy invasion in cases where there has been a "[p]ublic disclosure of embarrassing private facts about the plaintiff" or an "[i]ntrusion . . . into [the plaintiff's] private affairs."[37] Similar thoughts were expressed by Samuel D. Warren and Louis D. Brandeis, who were specifically concerned with protecting information about "the private life, habits, acts, and relations of an individual."[38]

C. Principle 3: Curtailing Intrusions into Spaces or Spheres Deemed Private or Personal

Behind this principle is the simple and ages-old idea of the sanctity of certain spaces or, more abstractly, places.[39] For example, "a man's home is his castle"—a person is sovereign in her own domain. Except when there are strong countervailing claims to the contrary, this principle apparently endorses a presumption in favor of people shielding themselves from the gaze of others when they are inside their own

---

Charles Fried, *Privacy*, 77 YALE L.J. 475 (1968) (arguing for protection of a socially determined kernel of sensitive information); Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233 (1977) (limiting privacy rights to information that is sensitive); William Parent, *Privacy, Morality, and the Law*, 12 PHIL. & PUB. AFF. 269 (1983).

33. 20 U.S.C. § 1232(g) (2000).

34. 12 U.S.C. §§ 3401–3422.

35. 18 U.S.C. § 2710.

36. 42 U.S.C. §§ 1320d–1320d-8.

37. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

38. Warren & Brandeis, *supra* note 4, at 216.

39. Michael R. Curry, *Discursive Displacement and the Seminal Ambiguity of Space and Place*, *in* THE HANDBOOK OF NEW MEDIA 502 (Leah A. Lievrouw & Sonia Livingstone eds., 2002).

private places. The Bill of Rights of the U.S. Constitution expresses commitment of a protected private zone in the Third and Fourth Amendments, defining explicit limits on government access to a home—quartering soldiers in the Third, and security against search and seizure in the Fourth. The Fourth Amendment, particularly, has been featured in countless cases where privacy is judged to have been violated by law enforcement agents who have breached private zones.[40] Warren and Brandeis give rousing voice to this principle: "The common law has always recognized a man's house as his castle, impregnable, often, even to its own officers engaged in the execution of its commands. Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?"[41] Warren and Brandeis, thus, endorse the principled sanctity of a private domain—in this case, the home—whether against the prying of government agents or any others.

Although in many cases Principles 2 and 3 can apply simultaneously, they are independent. In the cases of a peeping Tom, for example, spying on someone in her bedroom, or a wiretap connected to a person's telephone, we would judge privacy violated according to Principle 3, even if only mundane or impersonal information is gathered and hence Principle 2 is not violated. A similar distinction is found in numerous legal cases involving the Fourth Amendment and, of all things, garbage. Bearing most directly on the point here is the consistent finding that people cannot claim a privacy right in their garbage unless the garbage is placed within recognized private spaces (or the "curtilage"). In *California v. Greenwood*,[42] for example, a case that has served as precedent in many that followed, the U.S. Supreme Court concluded: "[a]ccordingly, having deposited their garbage in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it,

40. *See generally* RICHARD C. TURKINGTON & ANITA L. ALLEN, PRIVACY LAW: CASES AND MATERIALS (2d ed. 2002) (providing a discussion that specifically focuses on information and information technology); W.R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT (3d ed. 1996) (providing a general discussion of Fourth Amendment cases); DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW (2003) (providing a discussion that specifically focuses on information and information technology).

41. Warren & Brandeis, *supra* note 4, at 90.

42. 486 U.S. 35 (1988).

respondents could have had no reasonable expectation of privacy in the inculpatory items that they discarded."[43]

In insisting that privacy interests in garbage are a function not of content or constitution, but of location—whether inside or outside what is considered a person's private sphere—courts are, in effect, finding that Principle 3 is relevant to these cases, but not Principle 2; they are not finding contents of garbage to be inherently sensitive or private information.

D. Applying the Three Principles—Some Gray Areas

In claiming the three-principle framework has ascended to dominance in public deliberations over privacy, I maintain that it serves as a benchmark for settling disputes, but not that the outcome of disputes, or the application of the principles, is always obvious or clear. Even when it is clear which of the three principles is relevant, it may not always be obvious precisely how to draw the relevant lines to determine whether or not that principle applies, particularly with precedent setting cases involving new applications of information technology.

We have experienced this in a number of controversial government initiatives following the September 11, 2001, terrorist attacks. The USA PATRIOT Act[44] is one example among several where government agents have clashed with citizen advocacy organizations over attempts to redraw the boundaries of access into citizens' private lives. Even before the September 11 attacks, however, similar disagreements persisted over deployment of Carnivore, a surveillance tool for traffic flowing through the Internet.[45] Although a detailed account of these cases would require too great a detour from the central arguments of this Article, both are examples of disputes in which governmental interventions are asserted and contested. There is little doubt, in other words, that Principle 1 is of central relevance; what is disputed is whether the proposals in question—greater latitude for governmental surveillance both online and off-line—abide by or violate it.

Drawing lines in the case of intimate and sensitive information is also difficult and can be controversial. For example, an open question remains on whether to designate credit headers, which contain

43. *Id*. at 37; *see also* LAFAVE, *supra* note 40, at 603.

44. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

45. The FBI developed the Carnivore software, which is now typically called DCS 1000.

information such as names, addresses, phone numbers, and Social Security numbers, as "personal" or not. The Individual Reference Services Group, an industry association of information brokers, maintains they are not, while the Federal Trade Commission argues they are. Case 1, raising the question whether public records ought to be available online, provokes similar questions about court records in general, and more particularly, whether some of the information contained in them and other public records should be reclassified as personal and deserving of greater protection.[46] These lines are neither static nor universal as demonstrated by the case of information about students, including grades. The Family Educational and Privacy Act of 1974[47] marked a switch in conventional assumptions about student records. Among other things, it prohibited disclosure of information such as performance and staff recommendations without explicit permission of the students or their parents.

Similar line-drawing controversies challenge Principle 3. Interpretations of what counts as a private space may vary across times, societies, and cultures. The case of wiretaps in the United States illustrates variability across time: in 1928, in *Olmstead v. United States*,[48] the U.S. Supreme Court ruled that wiretapping did not constitute a breach of private space.[49] By 1967, however, in what is understood as an overturning of that ruling, in *Katz v. United States*[50] the Court concluded that tapping a person's phone does constitute an unacceptable intrusion into inviolate space.[51] At least one change this shift reflects is a change in belief about what constitutes a person's private sphere.

The *Kyllo v. United States*[52] decision reflects similar conflicting intuitions and opinions about what constitutes an intrusion into private space. In *Kyllo*, the question was whether the police's use of a thermal

46. *See, e.g.*, SPECIAL DIRECTIVE SUBCOMM., N.J. PRIVACY STUDY COMM'N, REPORT OF THE SPECIAL DIRECTIVE SUBCOMMITTEE TO THE NEW JERSEY PRIVACY STUDY COMMISSION (2003) [hereinafter REPORT OF THE SPECIAL DIRECTIVE SUBCOMMITTEE] (discussing whether home addresses and telephone numbers of citizens should be made publicly available), *available at* http://www.nj.gov/privacy/eo26.pdf.

47. 20 U.S.C. § 1232(g) (2000).

48. 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

49. *Id*. at 466.

50. 389 U.S. 347 (1967).

51. *Id*. at 359.

52. 533 U.S. 27 (2001).

imaging device to detect patterns of heat inside the suspect's home—for purposes of determining whether he was growing marijuana—constituted a violation of the private sphere.[53] In a split (five to four) ruling, the Court determined that the police were at fault for not first obtaining a warrant.[54] Against the argument proffered by the police that use of a thermal imaging device did not constitute intrusion into physical space, Justice Scalia, writing for the majority, concluded that "[i]n the home . . . all details are intimate details, because the entire area is held safe from prying government eyes."[55] Quoting precedent, Justice Scalia further emphasized that the law "'draws a firm line at the entrance to the house.'"[56]

Another regularly contested area, though the preponderance of opinion seems to have shifted over time, is online privacy in the workplace. Where previously this "space" was considered personal and inviolate, recent public opinion as well as court decisions suggest that ownership of servers by business organizations trumps claims by employees that the realms of the computer systems with which they work be considered a personal sphere.[57] This shift in presumption means that employers may routinely monitor e-mails and web-surfing behaviors of their employees.[58]

E. The Three Principles and Public Surveillance

The challenge posed by public surveillance is different from that posed by cases falling within the gray areas described above. In the latter, the difficulty is drawing a line; in the former, it is falling completely outside the scope of a normative model defined by the three principles. Like many of the hard cases, public surveillance typically involves a new technology, or a newly developed application of entrenched technology that expands the capacity to observe people;

53. *Id*. at 27.

54. *Id*. at 28.

55. *Id*. at 37.

56. *Id*. (quoting Payton v. New York, 445 U.S. 573, 590 (1980)).

57. For a comprehensive overview of this area of law and news media, see the Workplace Privacy webpage of the Electronic Privacy Information Center at http://www.epic.org/privacy/workplace (last visited Jan. 17, 2004).

58. *But cf.* Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000) (providing a more pessimistic interpretation—that the increased presence of thermal imaging and similar technologies of surveillance augurs the collapse of a protected private sphere).

gather information about them; and process, analyze, retrieve, and disseminate it. Unlike those cases, however, public surveillance does not involve government agents seeking to expand access to citizens; or collection or disclosure of sensitive, confidential, or personal information; or intrusion into spaces or spheres normally judged to be private or personal. Although public records are initially created by government agencies, the issue of placing them online does raise troubling questions of governmental overreaching and, by definition the records are public by virtue of not falling into categories of sensitive or confidential. Tracking by radio frequency identification, similarly, would not occur in places deemed private to the subjects of tracking. Online profiling is troubling, even when the information gathered is not sensitive (excludes credit card information, for example) and when it takes place on the public Web.[59] According to the framework, therefore, it seems that public surveillance is determined not to be a privacy problem. Because this conclusion is at odds with the intuition and judgment of many people, it warrants more than simple dismissal. In this disparity lie the grounds for questioning the three-principle framework as a universal standard for public deliberations over privacy.

Before presenting an alternative, contextualized approach in the next part, one conservative response to the problem of public surveillance deserves mention. Instead of simply dismissing popular aversion to public surveillance as misguided, unfounded, or irrational, this conservative view distinguishes between privacy—the value, which is embodied in the three principles, and privacy—the more encompassing category of preference, or taste, revealed in results of numerous public opinion surveys.[60] Designating public surveillance as a member of the second category still affords it various means of social protection, in addition to "self-help."[61] As commonly understood, democratic market-based societies offer at least two robust mechanisms for expressing popular preference: first, citizens can press for laws to protect majority

59. The term "public Web" is used to mark a distinction between those realms of the Web that are publicly accessible and those that are accessible only to authorized users and frequently protected by some form of security.

60. *See, e.g.*, Oscar Gandy, *Public Opinion Surveys and the Formation of Privacy Policy*, 59 J. SOC. ISSUES 283 (2003); Electronic Privacy Information Center, *Public Opinion on Privacy*, *at* http://www.epic.org/privacy/survey (last modified June 25, 2003) (summarizing public opinion surveys).

61. *See, e.g.*, Gary Marx, *A Tack in the Shoe: Neutralizing and Resisting the New Surveillance*, 59 J. SOC. ISSUES 369 (2003).

preferences, and second, consumers, through their actions, can affect the terms and nature of commercial offerings in a free, competitive marketplace.[62] These alternatives deserve a great deal more attention than I am able to offer here.

Although this view preserves the three-principle framework, at least one problem with it is that it places resistance to public surveillance on a weak footing against countervailing claims, particularly those backed by recognized rights and values. In a free society, a person has a right to choose chocolate over vanilla ice cream, or to press for extensive protections of privacy preferences, except where such preferences happen to conflict with another person's claim to something of greater moral or political standing. Those who conduct public surveillance, or support its pursuit, have lobbied exactly on those grounds, citing such well-entrenched freedoms as speech, action, and pursuit of wealth.[63] The weak footing that this allows for the aversion to public surveillance can be demonstrated in relation to a commonly used legal standard, namely, reasonable expectation of privacy.

Justice John Harlan, concurring with the majority opinion in *Katz*, is credited with formulating two conditions that later courts have used to test whether a person has "a reasonable expectation of privacy" in any given activity or practice, namely: (1) that the person exhibited an actual expectation of privacy, and (2) that the expectation is one that society is prepared to recognize as reasonable.[64] Although the reasonable expectation benchmark raises deep and complex questions that cannot be addressed here, there is at least one point of direct interest, notably that the benchmark is a potential source of crushing rebuttal to preference-based complaints against public surveillance. It is simply this: when people move about and do things in public arenas, they have implicitly yielded any expectation of privacy. Much as they might *prefer* that others neither see, nor take note, *expecting* others not to see, notice, or

62. Privacy skeptics have argued that because people seem to do neither, they obviously do not care much about privacy. *See* Calvin C. Gotlieb, *Privacy: A Concept Whose Time Has Come and Gone*, *in* COMPUTERS, SURVEILLANCE, AND PRIVACY 156 (David Lyon & Elia Zureik eds., 1996); Solveig Singleton, *Privacy as Censorship: A Skeptical View of Proposals To Regulate Privacy in the Private Sector*, *in* CATO POL'Y ANALYSIS NO. 295, (Cato Inst. 1998), *available at* http://www.cato.org/pubs/pas/pa-295.pdf.

63. Many articles deal with privacy in relation to competing claims. *But see, e.g.*, Cohen, *supra* note 58, at 1373; Richard Posner, *The Right to Privacy*, 12 GA. L. REV. 393 (1978); Eugene Volokh, *Personalization and Privacy*, COMM. ACM, Aug. 2000, at 84.

64. *See* Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring); *see also* REGAN, *supra* note 8, at 122; SOLOVE & ROTENBERG, *supra* note 40, at 21.

make use of information so gained would be unreasonably restrictive of others' freedoms. One cannot reasonably insist that people avert their eyes, not look out their windows, or not notice what others have placed in their supermarket trolleys. And if we cannot stop them from looking, we cannot stop them remembering and telling others. In 2001, Tampa police, defending their use of video cameras to scan faces one-by-one as they entered the Super Bowl stadium, stated, "the courts have ruled that there is no expectation of privacy in a public setting."[65]

In sum, maintaining that the three principles define the value of privacy provides significant force to the reasonableness of privacy claims covered by them, but offers little cover for anything outside the principles. Cast as preference, these claims are not ruled out as grounds for favoring one outcome over another, though not accorded special consideration in competition with others. Accordingly, there is no prima facie concern over placing public records, already available for anyone to see, online, or for permitting aggregation of non-sensitive information, so long as a compelling reason such as efficiency, safety, or profit can be offered. Since RFID and other surveillance are conducted in public venues only, the expectation of privacy in any of these contexts cannot be reasonable. Those who hold that public surveillance can constitute a violation and not merely a practice that some people dislike will remain unconvinced.

III. CONTEXTUAL INTEGRITY

Highlighting two features of the three-principle framework helps to convey what lies behind the idea of contextual integrity. One is that it is posed as a universal account of what does and does not warrant restrictive, privacy-motivated measures. That is, as a conceptual framework, it is not conditioned on dimensions of time, location, and so forth.[66] Another is that it expresses a right to privacy in terms of dichotomies—sensitive and non-sensitive, private and public, government and private—that line up, interestingly, with aspects of the general public-private dichotomy that has been useful in other areas of political and legal inquiry. That which falls within any one of the appropriate halves warrants privacy consideration; for all the rest,

65. Peter Slevin, *Police Video Cameras Taped Football Fans*, WASH. POST, Feb. 1, 2001, at A10.

66. It might still admit of variability in that the categories of sensitive and non-sensitive, for example, could vary across, say, cultures, historical periods, and places.

anything goes. In both these features, the account of privacy in terms of contextual integrity diverges from the three-principle model.

A central tenet of contextual integrity is that there are no arenas of life *not* governed by *norms of information flow*, no information or spheres of life for which "anything goes." Almost everything—things that we do, events that occur, transactions that take place—happens in a context not only of place but of politics, convention, and cultural expectation. These contexts can be as sweepingly defined as, say, spheres of life such as education, politics, and the marketplace or as finely drawn as the conventional routines of visiting the dentist, attending a family wedding, or interviewing for a job. For some purposes, broad sweeps are sufficient. As mentioned before, public and private define a dichotomy of spheres that have proven useful in legal and political inquiry. Robust intuitions about privacy norms, however, seem to be rooted in the details of rather more limited contexts, spheres, or stereotypic situations.

Observing the texture of people's lives, we find them not only crossing dichotomies, but moving about, into, and out of a plurality of distinct realms. They are at home with families, they go to work, they seek medical care, visit friends, consult with psychiatrists, talk with lawyers, go to the bank, attend religious services, vote, shop, and more. Each of these spheres, realms, or contexts involves, indeed may even be defined by, a distinct set of norms, which governs its various aspects such as roles, expectations, actions, and practices. For certain contexts, such as the highly ritualized settings of many church services, these norms are explicit and quite specific. For others, the norms may be implicit, variable, and incomplete (or partial). There is no need here to construct a theory of these contexts. It is enough for our purposes that the social phenomenon of distinct types of contexts, domains, spheres, institutions, or fields is firmly rooted in common experience and has been theorized in the profound work of reputable philosophers, social scientists, and social theorists.[67] Any of these sources could provide

67. *See generally* PIERRE BOURDIEU & LOIC J.D. WACQUANT, AN INVITATION TO REFLEXIVE SOCIOLOGY 95–115 (1992) (providing general discussion of Pierre Bourdieu's fields); *id.* at 97 ("In highly differentiated societies, the social cosmos is made up of a number of such relatively autonomous social microcosms . . . . For instance, the artistic field, or the religious field, or the economic field all follow specific logics . . . ."); MICHAEL PHILLIPS, BETWEEN UNIVERSALISM AND SKEPTICISM: ETHICS AS SOCIAL ARTIFACT (1994); MICHAEL WALZER, SPHERES OF JUSTICE: A DEFENSE OF PLURALISM AND EQUALITY (1983); Roger Friedland & Robert R. Alford, *Bringing Society Back In: Symbolic Practices, and Institutional Contradictions*, *in* THE NEW INSTITUTIONALISM IN ORGANIZATIONAL ANALYSIS 232, 247–59 (Walter W. Powell & Paul J. DiMaggio eds., 1991) (also discussing institutions); *id.* at 251 ("[Institutions] generate not only that

foundational concepts for articulating the concept of contextual integrity in relation to personal information.

Contexts, or spheres, offer a platform for a normative account of privacy in terms of contextual integrity. As mentioned before, contexts are partly constituted by norms, which determine and govern key aspects such as roles, expectations, behaviors, and limits. There are numerous possible sources of contextual norms, including history, culture, law, convention, etc. Among the norms present in most contexts are ones that govern information, and, most relevant to our discussion, information about the people involved in the contexts. I posit two types of informational norms: norms of appropriateness, and norms of flow or distribution. Contextual integrity is maintained when both types of norms are upheld, and it is violated when either of the norms is violated. The central thesis of this Article is that the benchmark of privacy is contextual integrity; that in any given situation, a complaint that privacy has been violated is sound in the event that one or the other types of the informational norms has been transgressed.[68]

A. Appropriateness

As the label suggests, norms of appropriateness dictate what information about persons is appropriate, or fitting, to reveal in a particular context. Generally, these norms circumscribe the type or nature of information about various individuals that, within a given context, is allowable, expected, or even demanded to be revealed. In medical contexts, it is appropriate to share details of our physical condition or, more specifically, the patient shares information about his or her physical condition with the physician but not vice versa; among friends we may pour over romantic entanglements (our own and those of others); to the bank or our creditors, we reveal financial information; with our professors, we discuss our own grades; at work, it is appropriate to discuss work-related goals and the details and quality of performance.

As important is what is not appropriate: we are not (at least in the United States) expected to share our religious affiliation with employers,

---

which is valued, but the rules by which it is calibrated and distributed."); *id.* at 253 ("society is composed of multiple institutional logics"); Jeroen van den Hoven, *Privacy and the Varieties of Informational Wrongdoing*, *in* READINGS IN CYBER ETHICS 430 (Richard A. Spinello & Herman T. Tavani eds., 2001).

68. It still holds that a violation can be justified in the event that another, more serious or urgent value is at stake.

financial standing with friends and acquaintances, performance at work with physicians, etc. As with other defining aspects of contexts and spheres, there can be great variability from one context to the next in terms of how restrictive, explicit, and complete the norms of appropriateness are. In the context of friendship, for example, norms are quite open-ended, less so in the context of, say, a classroom, and even less so in a courtroom, where norms of appropriateness regulate almost every piece of information presented to it. The point to note is that there is no place not governed by at least some informational norms. The notion that when individuals venture out in public—a street, a square, a park, a market, a football game—no norms are in operation, that "anything goes," is pure fiction. For example, even in the most public of places, it is not out of order for people to respond in word or thought, "none of your business," to a stranger asking their names.

While norms of appropriateness are robust in everyday experience, the idea that such norms operate has not been explicitly addressed in most of the dominant research and scholarship that feed into public deliberations of privacy policy in the United States.[69] Within the philosophical literature of the past few decades, however, we find recognition of similar notions. James Rachels, for example, has posited something like a norm of appropriateness in arguing that adequate privacy protection accords people the important power to share information discriminately, which in turn enables them to determine not only how close they are to others, but the nature of their relationships:

> businessman to employee, minister to congregant, doctor to patient, husband to wife, parent to child, and so on. In each case, the sort of relationship that people have to one another involves a conception of how it is appropriate for them to behave with each other, and what is more, a conception of the kind and degree of knowledge concerning one another which it is appropriate for them to have.[70]

Ferdinand Schoeman, a philosopher who has offered one of the deepest and most subtle accounts of privacy and its value to humans, writes,

69. The formal regulation of confidentiality within professional fields is an exception, but this Article argues that similar norms hold in all contexts, even if not stipulated in explicit laws or regulations.

70. James Rachels, *Why Privacy Is Important*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 290, 294 (Ferdinand David Schoeman ed., 1984).

"[p]eople have, and it is important that they maintain, different relationships with different people."[71] Further,

> [a] person can be active in the gay pride movement in San Francisco, but be private about her sexual preferences vis-à-vis her family and coworkers in Sacramento. A professor may be highly visible to other gays at the gay bar but discreet about sexual orientation at the university. Surely the streets and newspapers of San Francisco are public places as are the gay bars in the quiet university town. Does appearing in some public settings as a gay activist mean that the person concerned has waived her rights to civil inattention, to feeling violated if confronted in another setting?[72]

These cases illustrate Schoeman's sense that appropriating information from one situation and inserting it in another can constitute a violation. Violations of this type are captured with the concept of appropriateness.

B. Distribution

In addition to appropriateness, another set of norms govern what I will call flow or distribution of information—movement, or transfer of information from one party to another or others. The idea that contextual norms regulate flow or distribution of information was profoundly influenced by Michael Walzer's pluralist theory of justice.[73] Although Walzer's theory does not specifically address the problems of privacy and regulation of information, it provides insights that are useful to the construction of privacy as contextual integrity.

In his book, *Spheres of Justice: A Defense of Pluralism*, Walzer develops a theory of distributive justice in terms of not only a single good and universal equality, but in terms of something he calls complex equality, adjudicated across distinct distributive spheres, each with its own, unique set of norms of justice.[74] Walzer conceives of societies as made up of numerous distributive spheres, each defined by a social good internal to them.[75] Social goods include such things as wealth, political

71. Ferdinand Schoeman, *Privacy and Intimate Information*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY, *supra* note 70, at 403, 408.

72. Ferdinand Schoeman, *Gossip and Privacy*, *in* GOOD GOSSIP 72, 73 (Robert F. Goodman & Aaron Ben-Ze'ev eds., 1994).

73. *See* WALZER, *supra* note 67. Jeroen van den Hoven pointed out the relevance of this work to me.

74. *See id*.

75. *See generally id.*

office, honor, commodities, education, security and welfare, and employment.[76] These social goods are distributed according to criteria or principles that vary according to the spheres within which they operate.[77] In the educational sphere, for example, access to instruction up to a certain level (a good) might be guaranteed to all residents of a community with appropriate mental capacities and instruction beyond the basic level, say, a university undergraduate education, allocated only to those who have performed to a particular standard. Commodities (goods) in a marketplace are distributed according to preferences and ability to pay; in the sphere of employment, jobs (goods) are allocated to those with appropriate talents and qualifications, and so on.[78] According to Walzer, complex equality, the mark of justice, is achieved when social goods are distributed according to different standards of distribution in different spheres and the spheres are relatively autonomous.[79] Thus, in Walzer's just society, we would see "different outcomes for different people in different spheres."[80]

Complex equality adds the idea of distributive principles or distributive criteria to the notion of contextual integrity. What matters is not only whether information is appropriate or inappropriate for a given context, but whether its distribution, or *flow*, respects contextual norms of information flow.

Let us return to the context of friendship, this time to consider some examples of norms of flow. As described earlier, relatively few general norms of appropriateness apply, though practices may vary depending on whether the friends are close, have known each other for a long time, and so on. Information that is appropriate to friendship can include mundane information about day-to-day activities, likes and dislikes, opinions, relationships, character, emotions, capacity for loyalty, and much more. The same open-endedness, however, does not hold for norms of flow, which are quite substantial. In friendship, generally, information is either shared at the discretion of the subject in a bidirectional flow—friends *choose* to tell each other about themselves—or is inferred by one friend of another on the basis of what the other has done, said, experienced, etc. But that is not all. Confidentiality is

76. *See generally id.*

77. *See generally id.*

78. *See generally id.*

79. *See generally id.*

80. *Id*. at 320.

generally the default—that is, friends expect what they say to each other to be held in confidence and not arbitrarily spread to others. While some departure from the norms is generally allowable, as when friends coax information from each other, straying too far is usually viewed as a serious breach. Where a friend ferrets out information from third party sources, or divulges information shared in friendship to others for reasons having nothing to do with the friendship, not only might the friend justifiably feel betrayed, but the actions may call into question the very nature of the relationship.[81]

Free choice, discretion, and confidentiality, prominent among norms of flow in friendship, are not the only principles of information distribution. Others include need, entitlement, and obligation—a list that is probably open-ended. In a healthcare context, for example, when a patient shares with her physician details of her current and past physical condition, the reigning norm is not discretion of the subject (that is, free choice of the patient) but is closer to being mandated by the physician who might reasonably condition treatment on a patient's readiness to share information that the physician deems necessary for competent diagnosis and treatment. Another difference from friendship is that in the healthcare context, the flow is not normally bidirectional. Confidentiality of patient health information is the subject of complex norms—in the United States, for example, a recent law stipulates when, and in what ways, a physician is bound by a patient's consent: for example, where it is directly pertinent to diagnosis and treatment, where it poses a public health risk, and where it is of commercial interest to drug companies.[82]

Other cases of information practices following rational norms of flow include, for example, transactions between customers and mail-order merchants. In such transactions, customers are required to provide sufficient and appropriate information to satisfy companies that they can pay, and provide an address indicating where packages should be sent. Police are bound by law to abide by various regulations governing modes of acquiring information and how to deal with its flow thereafter. However, suspects arrested by police on criminal charges may volunteer

81. We may wonder how it would affect a friendship if one party discovers his friend has engaged the help of the much advertised snoop programs that promise the ability to track e-mail correspondence.

82. 45 C.F.R. §§ 164.102–.535 (2003). For a general discussion of the privacy regulations implemented pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. §§ 1320d–1320d-8 (2000), see the Health Privacy Project website at http://www.healthprivacy.org (last visited Jan. 17, 2004).

certain categories of information beyond those that they are compelled to provide. A sexual partner may be entitled to information about the other's HIV status, although the same demand by a friend is probably not warranted. A job applicant may volunteer information she considers evidence of her ability to do the job. Candidates for political office volunteer proof of professional competence, political loyalty, personal integrity, political connections, and past political activities. But it is accepted that employers and voters, respectively, might choose to conduct independent investigations as to fitness and competence. These cases are intended merely to illustrate the many possible configurations of informational norms we are likely to encounter, and they just begin to scratch the surface.

C. Change, Contextual Integrity, and Justice

As proposed above, a normative account of privacy in terms of contextual integrity asserts that a privacy violation has occurred when either contextual norms of appropriateness or norms of flow have been breached. One point of contrast with other theoretical accounts of privacy rights is that personal information revealed in a particular context is always tagged with that context and never "up for grabs" as other accounts would have us believe of public information or information gathered in public places. A second point of contrast is that the scope of informational norms is always internal to a given context, and, in this sense, these norms are relative, or non-universal. Before revisiting the problem of public surveillance in light of contextual integrity, two potentially worrisome implications should first be addressed, both consequences of this built-in contextual dependence.

One is that by putting forward existing informational norms as benchmarks for privacy protection, we appear to endorse entrenched flows that might be deleterious even in the face of technological means to make things better. Put another way, contextual integrity is conservative in possibly detrimental ways. As a brief example, consider the substantial benefits that networked information systems with good search capabilities provide consumers wishing to find out more about products, services, or service providers, say, to check whether a particular surgeon has been found guilty of malpractice. Because the capabilities are new, ferreting out such information constitutes a radical departure from past practice, which, in the case of the surgeon, might have meant a patient having to ask the surgeon directly or engage someone else in a costly search. It would be problematic if the theory of

contextual integrity would judge new forms of information gathering to be a privacy violation in such instances.

A second worry is that contextual integrity, being so tied to practice and convention, loses prescriptive value or moral authority. In this era of rapid transformations due to computing and information technologies, changes are thrust upon people and societies frequently without the possibility of careful deliberation over potential harms and benefits, over whether we want or need them.[83] Practices shift almost imperceptibly but, over time, quite dramatically, and in turn bring about shifts in conventional expectations. These changes have influenced outcomes in a number of important cases, such as determining that the Fourth Amendment was not breached when police discovered marijuana plants in a suspect's yard by flying over in a surveillance plane.[84]

The U.S. Supreme Court held that people do not have a reasonable expectation of privacy from air surveillance because flights have become a common part of our lives.[85] In *Kyllo*,[86] even though the Court concluded the Fourth Amendment had been breached, one of the reasons for its conclusion was that thermal imaging trained on a private residence (unlike plane flights) was not yet common practice and so would count as a search.[87] As long as contextual integrity is tied, in these ways, to practice and convention, it would be unconvincing as a source of moral prescription, that is, constituting adequate justification for what one morally should or should not do.

Although the two worries come from apparently opposite directions, in fact, they provoke a similar set of elaborations. First, they highlight the importance of distinguishing *actual* practice from *prescribed* practice. Second, even within the category of prescribed practice, the grounds for prescription can vary among several possibilities. Third, even entrenched norms can change over time and may vary across not only historical moments, but cultures, geographic locations, societies, nations, etc. Although these considerations mean that just because something is the case, does not mean it morally or politically ought to be the case, they also mean that something more is needed to enable us to

83. I am aware of an oversimplification in the way I express this issue, for change is not strictly a consequence of devices and systems by themselves but, of course, may involve other social, economic, or legal determinants.

84. Florida v. Riley, 488 U.S. 445, 447, 452 (1989).

85. *Id*. at 458.

86. *See supra* notes 52–56 and accompanying text.

87. *See* Kyllo v. United States, 533 U.S. 27, 34, 40 (2001).

distinguish changes that are morally and politically acceptable, or even desirable, from those that are not (and ought to be resisted). As explained below, this can be done, but only indirectly.

I propose that the requirement of contextual integrity sets up a presumption in favor of the status quo; common practices are understood to reflect norms of appropriateness and flow, and breaches of these norms are held to be violations of privacy. Walzer's account of justice asserts a similar presumption in the case of spheres, namely, that distributing social goods of one sphere according to criteria of another constitutes injustice.[88] Evidence of a commitment to this presumption is that our society recognizes as wrong wealthy people buying favorable verdicts in courts of law, bosses demanding sexual favors as a condition of promotion, awarding political office on the basis of kinship, and determining wage scales by gender or race. These examples are unjust not only because goods from one sphere have intruded into another, but also because distributional norms of one sphere are being applied to another. Further, Walzer considers it a form of tyranny when goods of one sphere intrude into, or become dominant in, not only one sphere but many; local norms that embody the settled rationale of the tyrannized sphere are overturned as those who possess vast amounts of dominant goods are able to exert tyrannical power over those who do not.[89]

A presumption in favor of the status quo for informational norms means we initially resist breaches, suspicious that they occasion injustice or even tyranny. We take the stance that the entrenched normative framework represents a settled rationale for a certain context that we ought to protect unless powerful reasons support change. The settled rationale of any given context may have long historical roots and serve important cultural, social, and personal ends. The hugely complex system of regulations in the medical context can be traced at least as far back as the fourth century B.C.E., when Hippocrates exhorted fellow physicians to maintain confidentiality because of the shame involved in passing on any further what they learn about their patients in the course of treatment: "And about whatever I may see or hear in treatment, or even without treatment, in the life of human beings—things that should

88. *See* WALZER, *supra* note 67, at 17–20.

89. *Id*.

not ever be blurted out outside—I will remain silent, holding such things to be unutterable [sacred, not to be divulged]."[90]

The context of elections for political office is another case of a settled normative framework that functions in generally positive ways.[91] On election day, citizens converge on polling stations to cast votes. From the moment they cross the threshold, information flows are highly regulated, from what elections officers can ask them to what they can ask officers, what voters are required to document in writing, who sees it, what happens to the vote cast and who sees that, what exit pollsters can ask citizens as they leave—for whom they voted but not voters' names—and what the exit pollsters are free to disseminate publicly. These two familiar cases illustrate how systems of norms of appropriateness and flow may evolve to serve determinable ends and institutions.

A presumption in favor of status quo does not, however, rule out the possibility of a successful challenge where adequate reasons exist. Resolving these contested cases calls for reliable means of evaluating the relative moral standing of entrenched norms and the novel practices that breach or threaten them. Specifically, I propose that entrenched norms be compared with novel practices that breach or threaten them, and judged worth preserving, or not, in terms of how well they promote not only values and goods internal to a given context, but also fundamental social, political, and moral values. Conducting the second of these two modes of evaluation, namely, a comparison in terms of social, political, and moral values, involves identifying fundamental values that may be served by (or obscured by) the relevant informational norms imposing restrictions on the flow and distribution of personal information in the given case. According to the insights of several privacy scholars, the list of values likely to be affected includes: (1) prevention of information-based harm, (2) informational inequality, (3) autonomy, (4) freedom, (5) preservation of important human relationships, and (6) democracy and other social values.[92] Values that are regularly cited in support of

90. *"In a Pure and Holy Way:" Personal and Professional Conduct in the Hippocratic Oath*, 51 J. HIST. MED. & ALLIED SCI. 406 (1996) (Heinrich Von Staden trans.) (alteration in original), *available at* http://www.indiana.edu/~ancmed/oath.htm.

91. I am speaking of elections in a democratic state, with details drawn more specifically from the context of the United States.

92. This list is informed by the work of Julie Cohen, Stanley Benn, Ruth Gavison, Jeroen van den Hoven, James Nehf, Paul Schwartz, Jeffrey Reiman, Jeffrey Rosen, and others. Citations to specific works are given in footnotes to follow.

free or unconstrained flows include: (1) freedom of speech, (2) pursuit of wealth, (3) efficiency, and (4) security.

1. Prevention of Informational Harms

Information in the wrong hands or generally unrestricted access to information can be harmful. The harm in question can be severe, such as occurred in the case of the murder of actress Rebecca Schaeffer in 1989, when it was discovered that the murderer located her home address through Department of Motor Vehicles records.[93] Less palpable, but also serious, are harms like identity theft, which occurs with increasing frequency, apparently as a result of the ready availability of key identifying information like Social Security numbers, addresses, and phone numbers. Furthermore, various goods such as employment, life, and medical insurance, could be placed at risk if the flow of medical information were not restricted, or if information regarding people's religious and political affiliations, sexual orientation, or criminal records were readily available.

2. Informational Inequality

There are a number of facets to this value. In the crucial 1973 U.S. Department of Health, Education, and Welfare's report on computerized records, the opening sentences presented fairness, or we might say justice, as a foundational value for regulating the collection, storage, and use of personal information in computerized databases.[94] The Department's politically grounded argument will be familiar in the American contexts where entities, such as government and financial institutions, wield significant power over the fates of individual citizens and clients. Allowing these institutions free reign in collecting and using information further tips the balance of power in their favor. Responsive to the strong sentiment in favor of leveling the playing field, the widely influential Code of Fair Information Practices defined restrictions on gathering, storing, and using information about people in the name of fairness.[95]

93. *See* Margan v. Niles, 250 F. Supp. 2d 63, 68 (N.D.N.Y. 2003). Passage of the Driver's Privacy Protection Act (DPPA), 18 U.S.C. §§ 2721–2725 (2000), followed shortly thereafter in 1994. *Margan*, 250 F. Supp. 2d at 68–69.

94. RIGHTS OF CITIZENS, *supra* note 29.

95. *Id*. at xxiii–xxxv.

Inequalities may also arise in the context of routine commercial transactions mediated by technologies of information. As described by Jeroen van den Hoven, individuals acquiring goods or services are also giving (some would say, selling) something, namely, information about themselves, such as their credit card numbers, names, or addresses.[96] Usually the parties in the transaction are far from equal. For the most part, individuals have little knowledge and understanding of the potential value of this economic exchange; do not know what will be done with the information; do not grasp the full implications of consenting to release of information; and almost certainly have no power to retract or redraw the arrangement should it prove annoying, burdensome, or simply different from what they had initially sought. van den Hoven calls for "openness, transparency, participation, and notification on the part of business firms and direct marketers to secure fair contracts," in order to promote fairness in exchange.[97]

3. Autonomy and Freedom

For purposes of this abbreviated discussion, we consider ways in which autonomy and freedom, taken together, have indicated the need for wise restrictions on access to personal information.[98] Typically associated with the liberal political vision, autonomy is the mark of thoughtful citizens whose lives and choices are guided by principles they have adopted as a result of critical reflection.[99] Thoughtful works on privacy by Ruth Gavison, Jeffrey Reiman, Julie Cohen, and others have demonstrated a rich array of associations between autonomy and privacy.[100] These works assert that freedom from scrutiny and zones of "relative insularity"[101] are necessary conditions for formulating goals, values, conceptions of self, and principles of action because they provide venues in which people are free to experiment, act, and decide without

96. van den Hoven, *supra* note 67.

97. *Id*. at 435.

98. Consider the title of Alan F. Westin's early and influential book, *Privacy and Freedom*. ALAN F. WESTIN, PRIVACY AND FREEDOM (1967).

99. *See, e.g.*, GERALD DWORKIN, THE THEORY AND PRACTICE OF AUTONOMY (1988).

100. Stanley I. Benn, *Privacy, Freedom and Respect for Persons*, *in* NOMOS XIII: PRIVACY 1 (J. Roland Pennock & John W. Chapman eds., 1971); Cohen, *supra* note 58; Gavison, *supra* note 10; Jeffrey Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 27 (1995).

101. *See, e.g.*, Cohen, *supra* note 58, at 1424.

giving account to others or being fearful of retribution.[102] Uninhibited by what others might say, how they will react, and how they will judge, unhindered by the constraints and expectations of tradition and convention, people are freer to formulate for themselves the reasons behind significant life choices, preferences, and commitments. In defending robust broad protections for informational privacy, Cohen reminds us that autonomy touches many dimensions of peoples' lives, including tastes, behaviors, beliefs, preferences, moral commitments, associations, decisions, and choices that define who we are.[103]

Besides the causal or enabling connection between privacy and autonomy, a further, constitutive connection that is hardly ever recognized as such plays an essential role in the most widely held definition of a right to privacy—the right to control information about oneself.[104] The plausibility of such a right to control information about oneself, even one that is limited and constrained by other competing or countervailing rights and obligations, rests on the premise that information about ourselves is something over which individuals may exercise autonomy. In this way, it is comparable to the prima facie rights of self-determination that we have over our bodies and access to them.

4. Preservation of Important Human Relationships

Information is a key factor in the relationships we have and form with others. Charles Fried has said that controlling who has access to personal information about ourselves is a necessary condition for friendship, intimacy, and trust.[105] James Rachels, as mentioned earlier, has made a related point that distinctive relationships, for example individual to spouse, boss, friend, colleague, priest, teacher, therapist, hairdresser, and so on, are partially defined by distinctive patterns of information sharing.[106] Insofar as these relationships are valued, so would we value adequate and appropriate restrictions on information flows that bolster them.

---

102. *See, e.g.*, Gavison, *supra* note 10.

103. Cohen, *supra* note 58, at 1425.

104. *See* REGAN, *supra* note 8; WESTIN, *supra* note 98; Cohen, *supra* note 58. However, I believe this conception is deeply flawed for reasons offered by Ruth Gavison and Jeffrey Reiman. *See* Gavison, *supra* note 10; Reiman, *supra* note 100.

105. *See* Fried, *supra* note 32.

106. *See* Rachels, *supra* note 70.

5. Democracy and Other Social Values

Several proponents of strong privacy protections point out the importance of privacy not only to individuals but to society. Priscilla Regan, in *Legislating Privacy*, provides one of the best-informed versions of this claim:

> Privacy has value beyond its usefulness in helping the individual maintain his or her dignity or develop personal relationships. Most privacy scholars emphasize that the individual is better off if privacy exists; I argue that society is better off as well when privacy exists. I maintain that privacy serves not just individual interests but also common, public, and collective purposes.[107]

Regan and others describe ways in which privacy is essential to nourishing and promoting the values of a liberal, democratic, political, and social order by arguing that the vitality of democracy depends not only on an autonomous and thoughtful citizenry—bolstered through privacy—but on the concrete protection against public scrutiny of certain spheres of decision-making, including but not limited to the voting booth.[108] Privacy is a necessary condition for construction of what Erving Goffman calls "social personae," which serves not only to alleviate complex role demands on individuals, but to facilitate a smoother transactional space for the many routine interactions that contribute to social welfare.[109] Similar arguments have been offered by Janlori Goldman defending robust protections of medical information on grounds that individuals would then be more likely both to seek medical care and agree to participate in medical research. In turn, this would improve overall public health as well as social welfare through scientific research. Arguments favoring restrictions of online transactional information cite potential gains, namely, the increased likelihood of participation in electronic commerce.[110] Finally, Oscar Gandy has

107. REGAN, *supra* note 8, at 221.

108. *See* Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723 (1999); Cohen, *supra* note 58; Janlori Goldman, *Protecting Privacy to Improve Health Care*, HEALTH CARE, Nov./Dec. 1998, at 47.

109. *See* ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959) (discussing the importance of maintaining a "backstage" where people are allowed to relax out of character (ch. 3) and describing the preferences of both audiences and performers to maintain a façade in various ritualized social settings, even when both know that the performances in question do not reveal the whole truth (ch. 6)); *see also* Cohen, *supra* note 58, at 1427.

110. *See* Donna L. Hoffman, *Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web*, 15 INFO. SOC'Y 129 (1999) (providing discussion as

vividly conveyed how profiling and the widespread collection, aggregation, and mining of data increase social injustice and generate even further discrimination against traditionally disadvantaged ethnic groups.[111]

6. Countervailing Values

There are obviously many reasons for favoring the collection, sharing, and widespread distribution of personal information, including maintaining free speech[112] and a free press, economic efficiency[113] and profitability, open government, and security.[114] When these values clash with those that support restrictive treatment, we need to pursue trade-offs and balance.

D. Applying Contextual Integrity to the Three Cases

One of the key ways contextual integrity differs from other theoretical approaches to privacy is that it recognizes a richer, more comprehensive set of relevant parameters. In addressing whether placing public records online is problematic, whether moving records from filing cabinets or stand-alone databases onto the net marks a significant change, it forces us to look beyond whether the information in question is public. To establish whether contextual integrity is breached requires an examination of governing norms of appropriateness and flow to see whether and in what ways the proposed new practices measure up.

When the first case, the availability of public records online, is viewed through the lens of contextual integrity, certain aspects of the

---

well as empirical analysis); Donna L. Hoffman et al., *Building Consumer Trust Online*, COMM. ACM, Apr. 1999, at 80 (same); *see also* L. JEAN CAMP, TRUST AND RISK IN INTERNET COMMERCE (2000).

111. *See* OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993); Oscar H. Gandy, Jr., *Coming to Terms with the Panoptic Sort*, *in* COMPUTERS, SURVEILLANCE, AND PRIVACY 132 (David Lyon & Elia Zureik eds. 1996); Oscar H. Gandy, Jr., *Exploring Identity and Identification*, 14 NOTRE DAME J.L. ETHICS & PUB. POL'Y 1085 (2000).

112. *See, e.g.*, Cohen, *supra* note 58; Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607 (1999); Volokh, *supra* note 63, at 84; *see also* SOLOVE & ROTENBERG, *supra* note 40, ch. 2, sec. C (providing extensive case law).

113. *See* Singleton, *supra* note 62 (describing economic efficiency as potentially in conflict with privacy).

114. *See* Orrin Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607 (2003). In general, literature and cases surrounding the Fourth Amendment involve a quest to balance privacy against security.

change in placement from locally kept records (whether hardcopy or electronic) to Web-accessible records, are highlighted in novel ways. The change in placement, which vastly alters the range of accessibility from local to global, is significant because it constitutes a breach of entrenched norms of flow. As such, it demands scrutiny in terms of values. Although a full-blown analysis is not possible in the context of this Article, it is instructive to consider, briefly, how this affects a case that, arguably, draws little sympathy—the convicted sex offender. Recent changes in the laws of various states require that neighbors be informed if someone with a record of a serious sex offense moves into the neighborhood.[115] Despite objections, a good case may be made in favor of altering the distributional norms, from storing a record in a publicly available cabinet to actively informing neighbors. A proposal to place these records online, however, is different. While residents of, say, Hamilton, New Jersey, might reasonably argue that being informed about a released sex offender in their neighborhood is a justified measure of protection against the dangers of recidivism, believed to be high in the case of sex crimes, a similar argument seems specious for a citizen of, say, Fairbanks, Alaska. Furthermore, placing the myriad categories of public records online would greatly facilitate the aggregation and analysis of these records by third parties. This radical alteration of availability and flow does little to address the original basis for creation of public records, namely, public accountability of governmental agencies.[116]

The second case, consumer profiling and data mining, can be analyzed in a similar way. As before, the crucial issue is not whether the information is private or public, gathered from private or public settings, but whether the action breaches contextual integrity. The use of credit cards and the emergence of information brokers, along with a host of technical developments, however, have altered patterns of availability and flow in well-known ways. But are these changes significant from the perspective of contextual integrity? The answer is variable. In the past, it was integral to the transaction between a merchant and a customer that the merchant would get to know what a customer purchased. Good, that is to say, competent merchants, paying attention to what customers wanted, would provide stock accordingly. Although the online bookseller Amazon.com maintains and analyzes customer records

115. *See, e.g.*, N.J. STAT. ANN. § 2C:7-2 (West 2002).

116. REPORT OF THE SPECIAL DIRECTIVE SUBCOMMITTEE, *supra* note 46; Gellman, *supra* note 2.

electronically, using this information as a basis for marketing to those same customers seems not to be a significant departure from entrenched norms of appropriateness and flow. By contrast, the grocer who bombards shoppers with questions about other lifestyle choices—e.g., where they vacationed, what movies they recently viewed, what books they read, where their children attend school or college, and so on—does breach norms of appropriateness. The grocer who provides information about grocery purchases to vendors of magazine subscriptions or information brokers like Seisint and Axciom is responsible not only for breaches of norms of appropriateness but also norms of flow.[117]

Contextual integrity generates similar questions about RFID tags because they too significantly alter the nature and distribution patterns of information. Prior to the advent of RFID tags, customers could assume that sales assistants, store managers, or company leaders recorded point-of-sale information. RFID tags extend the duration of the relationships, making available to the jeans retailer, the manufacturer, and others a range of information about customers that was not previously available. These potential uses of RFID tags can affect not only who gains access to customer information, but at whose discretion. In a departure from past assumption, the customer would no longer control the distribution of information beyond point of sale. Unless RFID tags are designed specifically to allow for easy detection and disabling, discretion is removed from the customer and placed into the hands of information gatherers. This departure from entrenched norms triggers an assessment in terms of values.

E. Contextual Integrity and Other Privacy-Centric Approaches

For the three cases, I have been able to provide only sketches of arguments to support particular prescriptions to restrict (or not restrict) information gathering, aggregation, and dissemination on the basis of contextual integrity. In general, the norms of appropriateness and flow demand consideration of a number of parameters, including the nature of the information in question and its relationship to the context, the roles involved in the context, the relationships among the roles, the rules of flow, and how any changes made within a context might affect the underlying values. For the most part, building a conclusive argument in

117. To complete the argument would require showing that these breaches are justifiable neither in terms of values internal to the context nor in terms of more fundamental social, political, and moral values.

terms of contextual integrity involves painstaking analysis of details (or building upon analyses of identical or very similar cases), including even a reference to factual findings, which might ground claims about the empirical effects of a change on key parameters.

In developing the rationale for a new way of thinking about some of the puzzles of public surveillance or "privacy in public,"[118] deficiencies (or blind spots) in the three-principle framework served as a springboard for an alternative normative theory built around the concept of contextual integrity. Although this strategy highlights the specific strength of contextual integrity to resolve puzzles of public surveillance, it gives short shrift to a body of theoretical works on privacy—many proposed in the past few years—whose broadly encompassing privacy principles also extend to various forms of public surveillance, among other things.[119] Given space constraints, I am not able here to give them the degree of individual consideration they deserve except briefly to mention the one most significant point of contrast. Where these other accounts offer interpretations of privacy in terms of universal prescriptions, contextual integrity couches its prescriptions always within the bounds of a given context.

The widely held conception of a right of privacy as a right to control information about oneself, for example, is sufficiently capacious to entail protections even in categories of so-called public information, public spaces, and against non-governmental agents. The same potential holds for rights posited in terms of freedom from visual surveillance or restrictions on access to the subject. From the perspective of contextual integrity, where prescriptions are always couched in context-specific terms, these conceptions would be considered too blunt, possibly dogmatic. Even allowing for tradeoffs with other competing claims and rights, for balancing privacy against other values such as security, property, or speech (which any reasonable version would), the claim to control and limit access remains too open-ended and still leaves out too much of the picture.

According to the theory of contextual integrity, it is crucial to know the context—who is gathering the information, who is analyzing it, who is disseminating it and to whom, the nature of the information, the

118. Nissenbaum, *supra* note 1.

119. *See, e.g.*, GANDY, *supra* note 111; FERDINAND DAVID SCHOEMAN, PRIVACY AND SOCIAL FREEDOM (1992); Cohen, *supra* note 58; Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998); Reiman, *supra* note 100; Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002).

relationships among the various parties, and even larger institutional and social circumstances. It matters that the context is, say, a grocery store as opposed to, say, a job interview or a gun shop. When we evaluate sharing information with third party users of data, it is important to know something about those parties, such as their social roles, their capacity to affect the lives of data subjects, and their intentions with regard to subjects. It is important to ask whether the information practice under consideration harms subjects; interferes with their self-determination; or amplifies undesirable inequalities in status, power, and wealth.

We might agree that there is something disrespectful, even sinister, in the relentless gathering, aggregation, mining, and profiling conducted by companies like Seisint and Axciom. In other cases, contexts, or activities that are similar in form might strike most people as desirable, or at least acceptable. Consider teachers in the setting of primary and secondary education in the United States—they collect and aggregate information about students in order to assign grades. Over time, these grades are further aggregated to yield grade point averages and are combined with other information to form a student dossier, which, in some form, may be submitted to colleges or employers to which students have applied for admission or employment. A school might be judged remiss if it failed to notice that the performance of particular students had changed significantly in one way or another, if it failed to "mine" its data for other categories of change that reflected on students' and the school's performance.

IV. CONCLUSION

This Article develops a model of informational privacy in terms of contextual integrity, defined as compatibility with presiding norms of information appropriateness and distribution. Specifically, whether a particular action is determined a violation of privacy is a function of several variables, including the nature of the situation, or context; the nature of the information in relation to that context; the roles of agents receiving information; their relationships to information subjects; on what terms the information is shared by the subject; and the terms of further dissemination. The model is prescriptive in that it is intended to serve as a justificatory framework for prescribing specific restrictions on collection, use, and dissemination of information about people.

Although other normative theories of privacy have produced important insights into privacy and its value and foundations, they

typically are framed in overly general terms. As a result, important details that in my account give rise to systematic context-relative qualifications need to be treated as exceptions, or tradeoffs. By contrast, the possibility of context-relative variation is an integral part of contextual integrity.

By contrast, if we adopt contextual integrity as the benchmark for privacy, these context relative qualifications can be built right into the informational norms of any given context. One consequence is that privacy prescriptions, now shaped to a significant degree by local factors, are likely to vary across culture, historical period, locale, and so on. Although some might find this problematic, I consider it a virtue. As prominent contributors to the study of privacy have noted, norms of privacy in fact vary considerably from place to place, culture to culture, period to period; this theory not only incorporates this reality but systematically pinpoints the sources of variation.[120] A second consequence is that, because questions about whether particular restrictions on flow are acceptable call for investigation into the relevant contextual details, protecting privacy will be a messy task, requiring a grasp of concepts and social institutions as well as knowledge of facts of the matter. Ideally, this approach will encourage future research into prominent and problematic domains in order to uncover how technical innovations in these domains affect informational norms.[121]

Finally, a brief note on how to respond to violations of contextual integrity, particularly those associated with widespread adoption of technologies of public surveillance. In connection with similar questions about injustices, Michael Walzer recommends that certain types of exchanges be blocked in order to preserve complex equality. Distribution principles of one sphere should not be permitted to intrude into others, so that those who are wealthy in one sphere are not allowed to spread tyranny to others. In our own society, we experience at least some such safeguards in law and policy—such as those prohibiting monetary exchanges for various kinds of goods (e.g., votes, babies, and organs), those invalidating kinship as a basis for handing down political office, and those rejecting political office as a sound basis for favorable decisions in court; even outlawing insider trading.[122]

---

120. *See, e.g.*, WESTIN, *supra* note 98.

121. *See* Kang, *supra* note 119 (providing an exemplary naturalized analysis of a particular domain—although not couched in terms of contextual integrity).

122. *See* Alex Kuczynski & Andrew Ross Sorkin, *For Well-Heeled, Stock Tips Are Served with the Canapés*, N.Y. TIMES, July 1, 2002, at A1, B6 ("The investor Wilbur L. Ross Jr., who spends his

Policy and law are not the only means of preserving contextual integrity. Outside the legal arena, norms of decency, etiquette, sociability, convention, and morality frequently address appropriateness and distribution of information. Certain contexts, such as friendship and courtship, for example, as rich and important as they are, are likely to remain the purview of these non-legal systems. In certain contexts, such as that of a lawyer-client (or other professional) transaction, a middle ground has so far seemed workable—norms explicitly articulated, backed by sanctions of the relevant professional associations.[123] When to codify contextual integrity into law, policy, and regulation is a familiar question about the scope of the law. Here, there is space to propose only that when violations of norms are widespread and systematic as in public surveillance, when strong incentives of self-interest are behind these violations, when the parties involved are of radically unequal power and wealth, then the violations take on political significance and call for political response.

weekends in the socially conscious town of Southampton, said that the people who divulge information and pass along tips are most likely concerned with improving their social status. . . . With a wink or a nod among friends and acquaintances, information heard along the boulevard is used to lubricate a promising personal or business relationship, impress a dinner table and repay a favor.").

123. *But see* Jonathan D. Glater, *Lawyers Pressed to Give Up Ground on Client Secrets*, N.Y. TIMES, Aug. 11, 2003, at A1, A12 (reporting that new government rules following corporate scandals, tax evasion, and concerns over terrorism are forcing professional groups, such as the American Bar Association, to cede ground on client confidentiality). Within this approach, such a change is framed as a change in norms of distribution on the lawyer-client context.