3-1-2010

Undermined Norms: The Corrosive Effect of Information Processing Technology on Informational Privacy

Richard Warner
IIT Chicago-Kent College of Law, rwarner@kentlaw.iit.edu

UNDERMINED NORMS: THE CORROSIVE EFFECT OF INFORMATION PROCESSING TECHNOLOGY ON INFORMATIONAL PRIVACY

RICHARD WARNER*

INTRODUCTION 1048
I. INFORMATIONAL NORMS 1052
A. *Norms Defined* 1053
1. Informational Norms 1054
2. Value-Justified Norms 1057
B. *Why is Norm-Consistent Information Processing Acceptable?* 1059
II. WHY WILL BUSINESSES CONFORM TO NORMS? 1060
A. *Detecting Norm Violations* 1061
B. *Norm-Violation Detectors Versus Norm-Inconsistent Sellers* 1061
C. *Sellers' Inability to Discriminate* 1062
D. *The Profit-Maximizing Strategy* 1062
III. FREE AND INFORMED CONSENT 1063
IV. THE CORROSIVE EFFECT 1067
A. *Lack of Norms* 1067
B. *Direct Marketing: Retailers as Information Brokers* 1071
1. Direct Marketing 1072
2. The "Retailers as Information Brokers" Norm 1074
3. The Norm is Not Value-Justified 1075
C. *Information Aggregators* 1078
D. *The Health Insurance Industry* 1080
E. *Further Examples* 1082
V. A CONSENT REQUIREMENT IS NOT A SOLUTION 1084
A. *Consumers Do Not Read Privacy Notices* 1084
B. *Informed Consent as a Practical Matter is Impossible* 1085
C. *The Overall Pattern of Free and Informed Consent Would Yield Undesirable Tradeoffs* 1085
VI. COLLABORATE OR RESIST? 1086

---

* Professor of Law, Chicago-Kent College of Law; Visiting Foreign Professor, Law Faculty, University of Gdańsk, Poland. I profited greatly from comments by Christopher Buccafusco, Harold Krent, Margaret Stewart, and Robert Sloan.

INTRODUCTION

> If the nineteenth century was a world of privacy and prudery, a world of closed doors and drawn blinds, both literally and figuratively, then the world of the twenty-first century is the world of the one-way mirror, the world of the all-seeing eye.[1]

> See EVERYTHING on the network. With a complete historical record, there are no more secrets; every action taken on the network is recorded and stored.[2]

Imagine your life as a line of events. Color an event red if a business records personal information about it; otherwise, color it blue.[3] How "red" is your line? Very. "[I]t has become increasingly rare to deal with any . . . private-sector organization without generating and relying upon a database of personal information."[4] The consequence is a loss of informational privacy.

Informational privacy is a matter of control. It is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[5] The degree of control we once enjoyed has vanished.[6] Advances in information-processing

---

1. LAWRENCE M. FRIEDMAN, GUARDING LIFE'S DARK SECRETS: LEGAL AND SOCIAL CONTROLS OVER REPUTATION, PROPRIETY, AND PRIVACY 272 (2007).

2. *Top 10 Reasons for Complete Network Visibility*, SOLERA NETWORKS, http://www.solera networks.com/company/resources/top-ten (last visited Jan. 2, 2011). Deep packet inspection technology allows one's ISP to view virtually all the unencrypted content one sends over the Internet. *See* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 5 U. ILL. L. REV. 1417, 1437–39 (2009).

3. The image is adapted from JAMES B. RULE, PRIVACY IN PERIL 32–33 (2007).

4. James B. Rule, *Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions*, 54 U. TORONTO L.J. 183, 183 (2004).

5. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (2d prtg. 1967). *See also* U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989) ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."); RULE, *supra* note 3, at 3 (defining "privacy as the exercise of an authentic option to withhold information on one's self"); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1462 (2000) ("I will use 'informational privacy' as shorthand for the ability to control the acquisition or release of information about oneself.").

6. The erosion began in the 1950s with the development of credit reporting practices. *See* RULE, *supra* note 3, at 99. For a fuller discussion, compare Priscilla M. Regan, *The United States*, *in* GLOBAL PRIVACY PROTECTION: THE FIRST GENERATION 50, 55 (James B. Rule & Graham Greenleaf eds., 2008) (noting the development of the computer in the 1960s triggered an interest in informational privacy). Richard Posner's summary is succinct and accurate:

> [U]ntil quite recently the information that people voluntarily disclosed to vendors, licensing bureaus, hospitals, public libraries, and so forth, was scattered, fugitive (because the bulkiness of paper records usually causes them to be discarded as soon as they lose their value to the enterprise), and searchable only with great difficulty. So although one had voluntarily disclosed private information on innumerable occasions to sundry recipients, one retained as a practical matter a great deal of privacy. But with digitization, not only can recorded information be retained indefinitely at little cost, but also the

technology now give *others* considerable power to determine when personal information is collected, how it is used, and to whom it is distributed. Privacy advocates sound the alarm in regard to both the governmental and private sectors.[7] I focus entirely on the latter and, within that, exclusively on commercial interactions. Private sector commercial transactions merit separate consideration. Not only do they raise complex and important issues, they also have not been as extensively examined as governmental intrusions.[8]

Privacy advocates raise a diverse array of concerns: "[T]heorists have proclaimed the value of privacy to be protecting intimacy, friendship, dignity, individuality, human relationships, autonomy, freedom, self-development, creativity, independence, imagination, counterculture, eccentricity, freedom of thought, democracy, reputation, and psychological well-being."[9] The diversity of concerns reflects the remarkably broad effect of the power others now have over one's personal information. One important reason the effects are so far reaching is that information-processing practices now

> share a distinctive and sociologically crucial quality: they not only *collect and record* details of personal information; they also are organized to *provide bases for action toward the people concerned.* Systematically harvested personal information, in other words, furnishes bases for institutions to determine what treatment to mete out to each individual. . . . Mass surveillance is a distinctive and consequential feature of our times. Whether

---

> information held by different merchants, insurers, and government agencies can readily be pooled, opening the way to assembling all the recorded information concerning an individual in a single digital file that can easily be retrieved and searched. It should soon be possible—maybe it is already possible—to create comprehensive electronic dossiers for all Americans, similar to the sort of dossier the FBI compiles when it conducts background investigations of applicants for sensitive government employment or investigates criminal suspects. The difference is that the digitized dossier that I am imagining would be continuously updated.

Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 248 (2008).

7. Three recent books illustrate the tenor of the literature: JON L. MILLS, PRIVACY: THE LOST RIGHT, at xi (2008) ("Intrusion is commonplace. Every single individual in today's society is at risk."); RULE, *supra* note 3, at 200 (warning of the "endless erosion of privacy"); DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 4 (2008) ("[T]he profound proliferation of new information technologies during the twentieth century . . . made privacy erupt into a frontline issue around the world.").

8. The last 300 years of political philosophy have emphasized the critical role of privacy in limiting the power of the state, and although scholars may disagree about how, and how much, to protect privacy, by now we surely all agree that allowing the state to reach too deeply into its citizens' lives puts freedom at risk. Recent examples include: MILLS, *supra* note 7; RULE, *supra* note 3; SOLOVE, *supra* note 7; Froomkin, *supra* note 5; Jed Rubenfeld, *The End Of Privacy*, 61 STAN. L. REV. 101 (2008).

9. SOLOVE, *supra* note 7, at 98. *See also* John Collette, *Role Demands, Privacy and Psychological Well-Being*, 30 INT'L J. OF SOC. PSYCHIATRY 222, 223 (1984) (examining the negative effects on women from loss of privacy).

> carried out by government agencies or private-sector organizations, it shapes the ways we approach major institutions and our treatment at their hands.[10]

I assume that we should impose limits on "mass surveillance"—on what James B. Rule defines as the use of "systematically harvested personal information, . . . to determine what treatment to mete out to each individual."[11] I will not argue for this assumption; I rely instead on the arguments and examples offered in the privacy literature. My question is how we should limit mass surveillance.

Setting limits is no simple task. Increased information processing power yields significant benefits, including increased availability of relevant information, increased economic efficiency, and improved security.[12] Any adequate account of how to set limits must explain how to balance the benefits against the loss of information privacy. Many nonetheless find the solution obvious: require consent.[13] That is, require businesses to present consumers with relevant information (in some specified fashion) and then to secure agreement to proceed with the transaction.[14] I will call this a "consent requirement," although what is actually required is just the presentation of information accompanied by some consumer action interpreted as agreement.[15]

---

10. RULE, *supra* note 3, at 14.

11. *Id.*

12. *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1217–18 (1998) (noting that allowing the processing of personal information makes commerce more efficient, prevents fraud, promotes transparency, and increases the relevant information businesses send consumers while decreasing the irrelevant information). *See also* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 U. CHI. L. REV. 75, 86 (2008) ("[P]olicy decisions frequently counterpose privacy against two other powerful values: efficiency and security."). Paul Ohm contends that privacy scholars have overestimated the security benefits of processing personal information. Ohm, *supra* note 2, at 1466–68.

13. *See, e.g.*, RULE, *supra* note 3, at 196. Notice and consent (either by opt-in or opt-out) is required by the fair information practice principles. *Fair Information Practice Principles*, FED. TRADE COMM'N, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last updated June 25, 2007) [hereinafter FTC]. These principles were recently affirmed at the 31st International Conference of Privacy and Data Protection, which culminated in the signing of the Madrid Declaration. THE MADRID DECLARATION (2009), *available at* http://thepublicvoice.org/TheMadridPrivacyDeclaration.pdf. Despite their popularity, consent requirements have also sparked considerable criticism. *See, e.g.*, Ohm, *supra* note 2, at 1474–77; Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 822–23 (2000) (noting the criticism but endorsing a limited consent requirement).

14. *See* J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 112 (2008).

15. As Paul Schwartz notes, "when a Web site says something about its data processing practices—even if this statement is vague or reveals poor practice—the visitor to the site is deemed to be in agreement with these practices so long as she sticks around. This summary, despite its ironic tone, is no exaggeration." Schwartz, *supra* note 13, at 824.

A consent requirement not only appears to guarantee control over personal information, it also yields an acceptable tradeoff between privacy and competing concerns.[16] The overall pattern of giving or withholding consent appears to define an acceptable line between permissible and impermissible uses of personal information.

The apparent virtues of a consent requirement are an illusion. We cannot rely on a consent requirement to ensure an adequate degree of informational privacy. This is not to deny that the goal should be to ensure an adequate degree of free and informed consent. Informational privacy is, after all, the ability to control what information others collect about a person and how they use and distribute it.[17] It is difficult to see how such control can be achieved other than through freely giving or withholding informed consent. But, it is one thing to present information and secure agreement; it is quite another to actually obtain free and informed consent. My claim is that the former does not—and indeed in practice *cannot*—ensure the latter.[18] The key to achieving free and informed consent lies instead in informational norms.

Informational norms are social norms that constrain the collection, use, and distribution of personal information.[19] Informational norms explain why, for example, you expect your pharmacist to inquire about the drugs you are taking but not about whether you are happy in your marriage. Norm-governed exchanges not only implement acceptable tradeoffs between informational privacy and competing goals, they also ensure that consumers give free and informed consent to those tradeoffs. This is the rationale for focusing on informational norms, as they are in fact the means by which to make the tradeoffs and give free and informed consent to those tradeoffs.[20] These claims require one qualification: they hold only under ideal conditions.[21] The qualification does not deprive the claims of interest, as it simply shows that the interest is normative, not empirical. The conditions—called *ideal transaction conditions*—define a normative goal, an ideal we should strive to approximate in practice. Current practice unfortunately fails to adequately approximate this ideal.[22] Lack of norms is one key reason for this failure. The rapid advance in information processing technology has outstripped the relatively slow evolution of social norms in a wide range of important cases. The obvious

16. FTC, *supra* note 13.

17. *See* WESTIN, *supra* note 5, at 7.

18. *See infra* Part V.

19. *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 138 (2004).

20. *See infra* Part I.

21. Richard Warner, *Turned On Its Head?: Norms, Freedom, and Acceptable Terms in Internet Contracting*, 11 TUL. J. TECH. & INTELL. PROP. 1, 6 (2008).

22. *See, e.g.*, *infra* Part II (discussing the claim that we fall short of the ideal is the claim that there is an imperfection in the market in the context of law and economics).

response is to create the necessary norms. What combination of legal regulation, market, and social factors will most effectively do so? That is the critical question, and the question with which I conclude this essay.

Part I defines the relevant concept of a norm. It also introduces the first of the four assumptions characterizing ideal transaction conditions and argues that, given that assumption, norm-governed exchanges are an acceptable tradeoff. The argument assumes that profit-motive driven businesses conform to the relevant norms, and the objection is that businesses will violate norms when doing so increases profit. Part II answers that objection by adapting a well-known law and economics argument to complete the characterization of the ideal transaction conditions and to argue that, under such conditions, the profit-maximizing strategy is to conform to applicable informational norms. Part III contends that, under ideal transaction conditions, consumers give free and informed consent to norm-created tradeoffs. Part IV offers four examples in which technologically enhanced information processing practices are unconstrained by appropriate informational norms and, hence, fall short of the ideal. The consequence is a loss of informational privacy. In the context of the law and economics argument developed in Part II, the claim that we fall short of the ideal is the claim that there is an imperfection in the market. In the law and economics literature, market imperfections are considered imperfections because they cause inefficiency;[23] the market imperfections illustrated by the four examples, on the other hand, are imperfections because they significantly reduce informational privacy. Part V rejects a consent requirement as an adequate solution to such shortfalls. Part VI argues that our goal should be to create the informational norms necessary to adequately constrain private sector information processing.

I. INFORMATIONAL NORMS

I begin with a typical example of a norm-governed transaction. Suppose Vicky purchases wine from a retail store. She makes a number of assumptions about what information the store will collect and how it will use and distribute the information. The assumptions include collection, use, and distribution. *Collection*: Vicky assumes that the store will not request information about her liver function, record the kind of clothes she is wearing, or record whether she is in the store with her spouse or another companion. *Use*: She assumes that the store will not analyze her patterns of wine buying to predict her sexual

23. *See, e.g.*, Froomkin, *supra* note 5, at 1501–03; Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1127 (2000) (citing PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS, WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 8 (1998)); Peter P. Swire, *Efficient Confidentiality for Privacy, Security, and Confidential Business Information* (Brookings-Wharton Papers on Fin. Servs. Ser., 2003), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=398340.

orientation—even if direct marketing researchers have discovered correlations between patterns of wine selection and sexual orientation.[24] *Distribution*: When she consults the store about a party she is planning, she assumes that the store will not publish the party details on its web site. In general, Vicky assumes the store will only collect, analyze, and distribute information in ways she regards as acceptable. From now on, let us shorten "the collection, use, and distribution of personal information" to "the processing of personal information."

We typically assume acceptable processing of personal information occurs in a wide range of settings—including, for example, coffee houses, auto mechanics, universities, restaurants, and small grocers. We do so because we assume the businesses conform to relevant informational norms. This raises four questions. First, what are the relevant informational norms? Second, why is information processing consistent with those norms acceptable? Third, why think businesses will conform to the norms? Finally, why believe that individuals give free and informed consent to the norm-permitted information processing? I consider each question in turn. An essential preliminary is the definition of the relevant notion of a norm.

A. Norms Defined

A norm is a sanction-supported behavioral regularity in a group of people, where the regularity exists in part because each group member thinks that he or she ought, other things being equal, to act in accord with that regularity.[25] Imagine: you are about to enter an elevator in which others are already present. Where do you stand? The norm is to maximize the distance between you and the person nearest you. As a further example, imagine you are making a comment during a roundtable discussion; how long should you talk before it is someone else's turn? You should talk only as long as is appropriate (in a contextually determined sense of "appropriate"). As a final example, picture a narrow corridor in which a lawyer with an oversized briefcase encounters a parent with a baby in a stroller walking in the other direction; in order for one

24. Lest this seem too fanciful, consider the direct marketing "discovery in a recent presidential campaign that buyers of a particular car-washing product proved enormously susceptible to Republican campaign appeals." RULE, *supra* note 3, at 104.

25. *See* Michael Hechter & Karl-Dieter Opp, *What Have We Learned About the Emergence of Social Norms?*, *in* SOCIAL NORMS 394, 403 (Michael Hechtor & Karl-Dieter Opp eds., 2001) (citing Robert Sugden, *Normative Expectations: The Simultaneous Evolution of Institutions and Norms*, *in* ECONOMICS, VALUES, AND ORGANIZATION 73, 78–79 (Ben-Ner Avner & Louis Putterman eds., 1998)). There are various definitions of norms, and it would be a mistake to wonder which one is "correct." There are just different concepts serving different theoretical purposes. The text defines the concept of a norm that serves my purposes. See, for example, Warner, *supra* note 21, at 8, for its use in other contexts.

to pass, the other must make room. The norm is that (in most cases at least) the lawyer should make room for the parent.

The sanctions for violating norms in these examples consist of disapproval and its consequences.[26] Sanctions typically play a role in explaining conformity to the norm.[27] More fully, explanations for conformity spread out over a continuum. At one extreme, a person conforms *only* in order to avoid sanctions (e.g., avoid eating meat with a salad fork solely to avoid the disapproval of one's etiquette-obsessed friends). At the other extreme, fear of sanctions plays *no* role in explaining conformity; rather, a person conforms solely because he thinks that conformity realizes a state of affairs regarded as good (respect for the opinions of others, for instance, in the roundtable discussion example). In between, conformity results from a mix, in varying degrees, of both factors. The essential point is that, *across the entire continuum*, it is true to say that one thinks he *ought* to conform. The "ought" is purely prudential at the "conform only to avoid sanctions" end and entirely non-prudential at the "conform solely to realize a good state of affairs" end.

1. Informational Norms

Informational norms are norms that govern the collection, use, and distribution of information.[28] As the communications theorist Helen Nissenbaum notes, informational norms

> [g]enerally . . . 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 [sic] 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.[29]

---

26. I focus on "sanctions" as penalties; norms may also be associated with "sanctions" that consist in approval or some other benefit (a "sanction" in the sense of ratifying or approving).

27. *See* Hechter & Opp, *supra* note 25, at 403–04 (citing A.L. Epstein, *Sanctions*, *in* 14 INTERNATIONAL ENCYCLOPEDIA OF THE SOCIAL SCIENCES, at 1 (David L. Sills ed., 1968)).

28. *See* Nissenbaum, *supra* note 19, at 138.

29. *Id. See also* Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 559, 581–82 (1998) ("For the myriad transactions, situations and relationships in which people engage, there are norms—explicit and implicit—governing how much information and what type of information is fitting for them."); James Rachels, *Why Privacy Is Important*, 4 PHIL. & PUB. AFF. 323, 328 (1975) ("[T]he sort of relationship 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.").

As the reference to friends and romantic entanglements illustrates, informational norms govern commercial and non-commercial interactions.[30] In the commercial context, informational norms are instances of the following pattern: a business may collect, use, and distribute information only as is appropriate for that business.[31] "Appropriateness" is determined contextually.[32] Over a wide range of cases, group members share a complex set of values that leads them to more or less agree in their particular contextual judgments of appropriateness.[33]

Consumer and business transactions occur against a background of informational norms,[34] I will not argue for this assumption. I rely instead on the work of Nissenbaum and others.[35] An example of an informational norm is in order, however. Vicky's wine store visit serves the purpose.[36] The relevant norm is that the store may process information only in ways appropriately related to the store's role as a seller of wine. The first point to note is that the norm defines a tradeoff between informational privacy and competing concerns. The competing concerns include increased economic efficiency,

---

30. *See, e.g.*, Nissenbaum, *supra* note 19, at 138.

31. *See, e.g.*, Adam Barth et al., *Privacy and Contextual Integrity: Framework and Applications*, *in* 2006 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 184, 186; Nissenbaum, *supra* note 19, at 138.

32. *See* Barth et al., *supra* note 31, at 186.

33. As Michael Zimmer notes, "within each context, the relevant *agents*, the *types of information*, and *transmissions principles* combine to shape the governing informational norms." Michael Zimmer, *Privacy on Planet Google: Using the Theory of "Contextual Integrity" to Clarify the Privacy Threats of Google's Quest for the Perfect Search Engine*, 3 J. OF BUS. & TECH. L. 109, 115 (2008) (citing Barth et al., *supra* note 31, at 186).

34. Norms vary from group to group. For simplicity, however, I take the relevant group to be all United States consumers. Norm variation has been studied in the contractual context. In the case of warranties, for example, higher income consumers may prefer higher prices and longer warranties while lower income consumers may prefer lower prices and shorter warranties. *See* William R. Darden & C.P. Rao, *A Linear Covariate Model of Warranty Attitudes and Behaviors*, 16 J. MARKETING RES. 466, 475 (1979).

35. In addition to Nissenbaum, relevant theorists include: PIERRE BOURDIEU & LOÏC J.D. WACQUANT, AN INVITATION TO REFLEXIVE SOCIOLOGY (1992); MICHAEL PHILIPS, BETWEEN UNIVERSALISM AND SKEPTICISM: ETHICS AS SOCIAL ARTIFACT (1994); MICHAEL WALZER, SPHERES OF JUSTICE: A DEFENSE OF PLURALISM AND EQUALITY (1983); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject As Object*, 52 STAN. L. REV. 1373 (2000); Roger Friedland & Robert R. Alford, *Bringing Society Back In: Symbols, Practices, and Institutional Contradictions*, *in* THE NEW INSTITUTIONALISM IN ORGANIZATIONAL ANALYSIS 232 (Walter W. Powell & Paul J. DiMaggio eds., 1991); Jeroen van den Hoven, *Privacy and the Varieties of Informational Wrongdoing*, COMP. & SCI., Sept. 1997, at 33, *reprinted in* READINGS IN CYBERETHICS 430 (Richard A. Spinello & Herman T. Tavani eds., 2001); Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957 (1989); Rachels, *supra* note 29; Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999).

36. *See supra* pp. 1052–53.

improved security, improved inventory control, marketing, business planning, and better customer relationships.[37] The norm promotes these ends by permitting the processing of some personal information; it strikes a balance between promoting these ends and promoting informational privacy by permitting the processing of *only* some information and *only* for certain purposes.

The key question is, why is the wine store norm a norm at all? Why, that is, is it a sanction-supported regularity to which we think we ought to conform? The answer here provides a template for answering the same question in more controversial cases later. The relevant regularity exists: wine stores typically process information only in appropriate ways. They do not, for example, request information about liver functions, publish details about customer parties on the store web site, or analyze buying patterns to determine sexual orientation. The regularity is also sanction-supported. The sanction for the wine store's violation is lost business; customers would tend to desert a store they discovered engaged in such practices.[38] The sanction for consumer non-conformity is the inconvenience of always paying cash and the loss of store discounts and other advantages that require identifying oneself.[39] Conformity benefits consumers and society as a whole by promoting more efficient businesses that better serve consumers' needs.[40] The price we pay for these benefits is merely allowing businesses to process personal information within norm-imposed constraints—constraints that ensure the processing is acceptable.[41] In light of these facts, we think (or would after adequate reflection think) we are better off if we conform; therefore, we decide that we ought to conform.

---

37. *See supra* note 12 and accompanying text.

38. *See* James. R. Averill, *Studies on Anger and Aggression: Implications for Theories of Emotion*, 38 AM. PSYCHOLOGIST 1145, 1149 (1983) (noting that violation of norms in an exchange provokes anger and may lead to the termination of the exchange); Janice Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, INFO. SYS. RES., ePub ahead of print Feb. 19, 2010, at 2, 15, http://isr.journal.informs.org/cgi/reprint/isre.1090.0260v1 ("Our results suggest that individuals are willing to pay a premium for privacy when privacy information is made prominent and intuitive. . . . We found that participants provided with salient privacy information took that information into consideration, making purchases from websites offering medium or high levels of privacy.").

39. *See infra* note 144 and accompanying text.

40. *See supra* note 12 and accompanying text.

41. *See* COMM. ON PRIVACY IN THE INFO. AGE, NAT'L RESEARCH COUNCIL, ENGAGING PRIVACY AND INFORMATION TECHNOLOGY IN A DIGITAL AGE 164 (James Waldo et al. eds., 2007).

2. Value-Justified Norms

Business information processing practices are inadequately constrained by informational norms. The problem is that the rapid increase in information processing has outpaced the evolution of norms, leading to a lack norms in many important cases.[42] To stop the critique here, however, would be to overlook another crucial way in which we lack appropriate norms. Across a wide range of significant cases, informational norms *do* exist, but they are not consistent with our values; they are not *value-justified*.[43] In such cases, we do not lack norms *per se*, but we do lack value-justified norms. What, then, is a value-justified norm? And, why does it matter whether a norm is value-justified?

To answer the first question, consider that we typically conform to norms without much thought; when you step into an elevator, for example, you just unreflectively stand in the appropriate spot. You think you ought to stand there, but you do not worry or wonder about the justification for that "ought." But you *could* justify it if you reflected on the norm under ideal conditions (including having sufficient time, information, lack of bias, and so on).[44] You could justify the balance the norm strikes between 'not feeling crowded' and being able to use the elevator when it arrives. Roughly speaking, a norm is value-justified when one can, in light of one's values, justify the norm.

This is "rough speaking" because justification is a matter of degree. One might, for example, regard the elevator norm as justified but also think that the following alternative is even *more* justified: maximize the distance from your nearest neighbor *and do not enter the elevator unless that distance is at least three inches*. It is essential to take degrees of justification into account to arrive at an explanation of value-justification that will serve our purposes in what follows. Thus, let us define a value-justified norm: a norm is value-justified when, in light of the values of all (or almost all) members of the group in which the norm obtains, the norm is *at least as well justified as any alternative*.[45] It is worth emphasizing the requirement of justification, in light of the values of *all (or almost all)* members of the group in which the norm obtains; this plays an important role later in the argument that, under ideal

42. *See, e.g., id.* at 215–16 (discussing the informational processing concerns surrounding the mapping of the human genome).

43. Warner, *supra* note 21, at 8–9.

44. The appeal to reasoning under appropriate conditions to justify normative conclusions begins (at least) with Aristotle. *See generally* ARISTOTLE, NICOMACHEAN ETHICS (Martin Ostwald trans., Liberal Arts Press, 19th prtg. 1980). For a modern exposition and defense of this approach, see generally STEPHEN L. DARWALL, IMPARTIAL REASON (1983).

45. *See* Warner, *supra* note 21, at 8–9.

transaction conditions, *all (or almost all)* consumers freely consent to norm-implemented tradeoffs.[46]

My critique of current information processing practices focuses on a particular type of failure of value-justification. The following example illustrates the relevant type and serves as a useful reference point in developing the critique. Until the 1970s, the norm among National Hockey League players was *not* to wear a helmet.[47] The norm remained despite the clear risk of severe head injury[48] and the majority vote in a secret ballot where players said that the league should require them to wear helmets.[49] "One player summed up the feelings of many: 'It's foolish not to wear a helmet. But I don't—because the other guys don't. I know that' [sic] silly, but most of the players feel the same way.'"[50] Thus, most players preferred that most players—themselves included—wear a helmet but preferred not to wear a helmet if most others did not. The players conformed to the no-helmet norm to avoid two sanctions: non-helmet-wearing players' perception that helmet-wearers lacked toughness, and a small loss in playing effectiveness against non-helmet-wearing players.[51] In light of the sanctions, each player thought he ought to conform. The result was that it remained a norm not to wear a helmet until 1979, when the League required all players to wear helmets.[52] Despite its persistence, the "no helmet" norm was not value-justified. There was an alternative the players regarded as far better justified: that all players should wear helmets.

This suffices for an explanation of value-justification. Now, why does value-justification matter? The hockey helmet example shows why. The no-helmet norm defined a tradeoff between the risk of head injury, on the one hand, and on the other, retaining peripheral vision and appearing tough. When they conformed to this norm, the players accepted the tradeoff—even though they regarded another norm (all players wear helmets) and another tradeoff (reduced risk of head injury) as far better justified. This is why value-justification matters: conformity to a norm that lacks value-justification means acting contrary to one's values. This same pattern appears in the lack-of-value-justification norms examined in Part IV. We are trapped in conformity

46. The point is to avoid a "majoritarian bias." The view is *not* that if a *majority* find a norm value-justified, then *all* who conform do so freely.

47. *See* NATIONAL HOCKEY LEAGUE, THE HISTORY OF HOCKEY EQUIPMENT (2002), *available at* http://stars.nhl.com/ext/pdf/NHL_UniformBooklet.pdf.

48. Thomas C. Schelling, *Hockey Helmets, Concealed Weapons, and Daylight Saving: A Study of Binary Choices with Externalities*, 17 J. CONFLICT RESOL. 381, 381 (1973).

49. James Surowiecki, *Fuel for Thought*, NEW YORKER, July 23, 2007, at 25, 25.

50. Schelling, *supra* note 48, at 381 (quoting *The Stick that Sickens*, NEWSWEEK, Oct. 6, 1969, at 95, 95).

51. *Id.*

52. *Id.*

to those norms even though our values lead us to regard alternative norms as far better justified.

B. Why is Norm-Consistent Information Processing Acceptable?

Why is information processing that is consistent with relevant informational norms acceptable? Indeed, does not the immediately preceding discussion show that this is not always true? When we are trapped in conformity to a norm that lacks value-justification, we are trapped into acting contrary to our values. How can that qualify as acceptable? My answer is that, *under ideal transaction conditions*, information processing consistent with the relevant norms is acceptable to the extent practice approximates the ideal. The first step in defending this claim is to explain the relevant sense of "acceptable." "Acceptable" in this context means the following: norm-consistent information processing is acceptable when (and only when) the norm is value-justified. The first of the four assumptions characterizing the ideal conditions—the *norm completeness* assumption—guarantees that norms are value-justified.

The assumption is that value-justified norms govern *all* personal information processing by businesses. The assumption is approximately true, and its approximate truth ensures that the ideal it defines is a viable normative guide, not an ideal so unattainable that it is irrelevant. A rich and varied set of value-justified informational norms has arisen through centuries of information exchanges between sellers and buyers. The current problem is that rapid technological and economic change has outstripped the relatively slow evolution of norms, thereby creating types of transactions that are not governed by appropriate norms.[53]

I make two simplifying assumptions about norm completeness. First, transactions are either entirely consistent or entirely inconsistent with applicable norms. Consistency may be a matter of degree in practice. Second, in regard to value-justification, the simplifying assumption is that our values show either that we ought to act in accord with a given norm or that we ought not. In practice, our values may leave questions undecided—showing neither that we ought act in accord with a norm, nor showing that we ought not.

To summarize: norm completeness guarantees that transactions are governed by value-justified informational norms; hence, given the assumption, it follows that norm-consistent information processing is acceptable in the sense defined. Some may object that this is just a bit of definitional sleight of hand that glosses over an obvious problem. The apparent problem is that people vary greatly in the sensitivity about informational privacy, so it is

53. *See* COMM. ON PRIVACY IN THE INFO. AGE, *supra* note 41, at 215–16.

entirely possible, for example, that Vicky[54] might prefer that the wine store not collect any personal information about her at all—even when the relevant norm allows the store to do so. What is the point of insisting that information processing is acceptable in the sense defined if Vicky prefers a different treatment? To see the point, consider that, as a member of the community in which the norm obtains, Vicky herself accepts and generally adheres to the norm. Thus, if she were to insist on being an exception to the norm, she would be violating her own standards and demanding to be made an exception to a norm that *she* regards as at least as well-justified as any alternative. One can easily imagine Vicky insisting on her preferred treatment. But this just shows that, like all of us, Vicky can be tempted by what she nonetheless thinks she should not have.

II. WHY WILL BUSINESSES CONFORM TO NORMS?

Why think businesses will conform to the norms? Suppose, for example, that wine stores could increase profits by surreptitiously using information about buying patterns to determine their customers' sexual orientation.[55] Rational, profit-motive-driven businesses will violate the norm that prohibits using information in that way.[56] So won't businesses often violate informational norms? My answer is that, under ideal transaction conditions, the profit-maximizing strategy for a business is to conform to applicable informational norms.[57] I begin with a summary of the argumentof this claim: (1) some buyers will notice when a business violates a norm; (2) buyers will not buy from a business they perceive as norm-inconsistent; (3) businesses can discriminate between buyers who will, and those who will not, detect norm-inconsistencies; therefore, (4) norm-conformity is the profit-maximizing strategy.[58] In presenting the argument, I assume that both businesses and consumers know all relevant norms, and know what tradeoffs they

54. *See supra* pp. 6–7.

55. *Cf., e.g.*, RULE, *supra* note 3, at 104 (discussing a direct marketing "discovery in a recent presidential campaign that buyers of a particular car-washing product proved enormously susceptible to Republican campaign appeals").

56. *See, e.g.*, Elisabetta Povoledo, *Italian Judge Cites Profits as Justifying a Google Conviction*, N.Y. TIMES, Apr. 13, 2010, at B8 (discussing a conviction of Google employees for violating Italian privacy laws in order to profit from a video of an autistic boy being bullied).

57. The argument is adapted from the influential article by Schwartz and Wilde. Alan Schwartz & Louis L. Wilde, *Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis*, 127 U. PA. L. REV. 630 (1979). My argument proposes a normative ideal: Schwartz and Wilde in contrast make empirical claims. It also bears emphasis that my argument concerns informational norms, not—as with Schwartz and Wilde—terms in standard-form contracts. I focus on terms in Richard Warner, *Turned on Its Head?: Norms, Freedom, and Acceptable Terms in Internet Contracting*, *supra* note 21.

58. Warner, *supra* note 21, at 14.

implement.[59] This *knowledge completeness* assumption eliminates the possibility of non-compliance through lack of knowledge of norms. It is the second of the four assumptions characterizing ideal transaction conditions.[60] Practice approximates knowledge completeness; one is likely to know the norms governing the types of transactions in which one typically engages.[61]

A. Detecting Norm Violations

It is quite unlikely that norm-inconsistent information processing will escape the notice of every buyer. Awareness of norm-inconsistent information processing can come from, *inter alia*, news reports, magazine articles, books, consumer watchdog groups, negative publicity from consumer complaints, and litigation.[62] This is the third assumption characterizing ideal transaction conditions. Call it the *inconsistency-detection* assumption.[63]

B. Norm-Violation Detectors Versus Norm-Inconsistent Sellers

Other things being equal, buyers will not buy from sellers they regard as norm-inconsistent.[64] A norm, after all, is a regularity to which one thinks everyone ought to conform; thus, to see a seller as norm-inconsistent is to see that seller as treating one as one ought *not* to be treated. Other things being equal, buyers will not purchase from norm-inconsistent sellers as long as

---

59. *See* EDWIN MANSFIELD & GARY YOHE, MICROECONOMICS: THEORY/APPLICATION, 290–91 (11th ed. 2004) (describing perfect knowledge as a requirement for perfect economic competition).

60. The other three assumptions are discussed elsewhere within this article. *See supra* Part I.B (discussing the norm completeness assumption); *infra* Part II.A (discussing the inconsistency-detection assumption); Part II.A (discussing the assumption of a sufficiently norm-competitive market).

61. It is worth noting that if a consumer knows that practice approximates norm completeness, then even when he or she does not know what the relevant norm is, he or she will still have reason to think that, whatever it is, it is value-justified.

62. *See, e.g.*, Robert A. Hillman, *Online Boilerplate: Would Mandatory Website Disclosure of E-Standard Terms Backfire*, 104 MICH. L. REV. 837, 853 (2006) (discussing the role of watchdog groups).

63. Warner, *supra* note 21, at 14. Compare the "informed minority" assumption in the Schwartz and Wilde argument. Schwartz & Wilde, *supra* note 57, at 635–39. *See also* Alan Schwartz & Louis L. Wilde, *Imperfect Information in Markets for Contract Terms: The Examples of Warranties and Security Interests*, 69 VA. L. REV. 1387, 1417–18 (1983). For criticism, see R. Ted Cruz & Jeffery J. Hinck, *Not My Brother's Keeper: The Inability of an Informed Minority to Correct for Imperfect Information*, 47 HASTINGS L.J. 635, 656 (1996) (arguing that the assumption is empirically false). The inconsistency-detection assumption is not an empirical claim, however, but part of the specification of a normative ideal. *See infra* Part IV.

64. Warner, *supra* note 21, at 14.

norm-consistent sellers exist.[65] The fourth assumption, introduced shortly, ensures that such sellers exist.

C. *Sellers' Inability to Discriminate*

Suppose sellers could reliably differentiate between buyers who will, and those who will not, detect a norm-inconsistency; such sellers could then act norm-consistently for inconsistency-detectors and violate norms for the rest. Such discriminations are, however, extremely difficult to make in mass market contexts.[66] Imagine walking into a retail store or ordering an item online. Nothing reliably signals the seller whether one is a norm-inconsistency detector.[67]

D. *The Profit-Maximizing Strategy*

Assume businesses cannot identify norm-inconsistency detectors; then, profit-motive driven sellers will conform to norms because that is the profit-maximizing strategy—provided the market is *sufficiently norm-competitive*. The existence of a perfectly norm-competitive market is the fourth assumption characterizing ideal transaction conditions. A market is perfectly competitive with respect to a certain range of product risk-norms when—and only when—the following two conditions hold. *First, perfect competition*: 1) there is a large number of independently acting (non-colluding), perfectly informed sellers and consumers; 2) no one of whom can unilaterally control the features a product has; 3) sellers sell homogenous products, 4) in a market in which competitors may costlessly enter and leave; and 5) in which consumers can costlessly switch from one seller to another.[68] *Second, norm-violation detection*: there is a range of product-risk norms, and for each norm in that range, there are enough norm-violation-detecting buyers that a seller's gain

65. For further explanation, see Tsai et al., *supra* note 38.

66. *See* Schwartz & Wilde, *supra* note 57, at 663–65 (arguing that sellers cannot discriminate between relevant types of buyers in mass market transactions). Cruz and Hinck argue that, in contractual settings, sellers may be able to discriminate between different types of buyers. Cruz & Hinck, *supra* note 63, at 672–75. However, only one of their arguments explicitly addresses the ability of sellers to differentiate between buyers *based on their attitudes toward contractual terms*, and that argument assumes a sales-person explicitly proposes a contractual term, and hence assumes a context in which detection of norm-inconsistency would be likely. *Id.* at 673.

67. You may, of course, reveal yourself as an inconsistency-detector if you explicitly insist on norm-consistent treatment, or if you detect and object to norm-inconsistent behavior.

68. The condition is just one definition of a perfectly competitive market. *See, e.g.*, JEFFERY L. HARRISON, LAW AND ECONOMICS IN A NUTSHELL 261 (West Nutshell Ser., 4th ed. 2007).

from norm-inconsistent behavior is smaller than the loss which results if norm-violation detectors are able to buy from a substitute, norm-consistent seller.[69]

The first condition ensures that norm-inconsistent sellers will (other things being equal) lose the business of every norm-violation-detecting buyer—provided that at least one norm-consistent seller exists.[70] This follows from the fact that buyers who detect a norm-violation will not buy from that seller—other things being equal.[71] The second condition ensures that there are enough norm-consistent sellers. When both conditions hold, the profit-maximizing strategy is to behave norm-consistently towards all buyers.[72] Rational, profit-motivated sellers will conform with that strategy.[73]

Since I only propose norm competitiveness as a normative goal, I will put to one side the question of the extent to which norm-competitive markets exist in practice.[74] The issue requires a detailed antitrust analysis. Failures of norm-competitiveness may justify legal resolution. Such analysis lies outside the scope of this Article.

III. FREE AND INFORMED CONSENT

Under ideal transaction conditions, rational, profit-driven sellers will comply with all relevant informational norms, and those norms will implement

---

69. The idea of a *norm*-competitive market is adapted from Schwartz and Wilde's definition of a *term*-competitive market. They propose that there is lack of sufficient term-competition (in their terminology, a "monopolistic" market with respect to terms) if "(1) the market is not price competitive; and (2) the term at issue appears in arcane legal language and fine or otherwise inconspicuous print." Schwartz & Wilde, *supra note* 57, at 661. The point of (2) is to identify those cases in which there is a high cost to consumers of searching for and understanding relevant contractual terms; the idea is that in such cases "too few [norm] searchers may exist to generate a nonmonopolistic term structure. *Id.*

70. *See* HARRISON, *supra* note 68, at 261.

71. The "other things being equal" rider merely concerns trivial exceptions that do not matter here (for example, the buyer purchases from a norm-inconsistent seller because the seller is a relative).

72. *See* HARRISON, *supra* note 68, at 261.

73. *Id.*

74. There is some evidence that norm-competitiveness does not hold. Privacy International points out that competitive pressures lead to less informational privacy:

> [W]e are witnessing an increased 'race to the bottom' in corporate surveillance of customers. Some companies are leading the charge through abusive and invasive profiling of their customers' data. This trend is seen by even the most privacy friendly companies as creating competitive disadvantage to those who do not follow that trend, and in some cases [is seen as a reason] to find new and more innovative ways to become even more surveillance-intensive.

PRIVACY INT'L, A RACE TO THE BOTTOM: PRIVACY RANKING OF INTERNET SERVICE COMPANIES (2007), *available at* http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-553961. One possible explanation is that there are not enough norm-violation-detecting buyers.

an acceptable tradeoff between informational privacy and competing concerns.[75] It does not, however, follow that informational norms thereby ensure an adequate degree of informational privacy. That requires that buyers give free and informed consent to the norm-created tradeoff.[76] Otherwise, they do not have the ability "to determine *for themselves* when, how, and to what extent information about them is communicated to [and used by] others."[77] The "informed" part of "free and informed" is not problematic—not in ideal transaction conditions. Consent to a norm-created tradeoff is informed, provided consumers know what the norm is and what tradeoff it implements. The knowledge completeness assumption guarantees that consumers have the requisite knowledge.[78] It is more problematic to regard consent as free, since—even under ideal conditions—consent appears involuntary.

Consider the wine store example.[79] It appears problematic to regard Vicky's consent as free because, as a practical matter, she cannot avoid consenting to the norm-imposed tradeoff. Vicky can, of course, prevent wine stores from processing information about her by simply not doing business with wine stores that process personal information. But, since she wishes to buy wine, it is often difficult to avoid wine stores. Further, Vicky is not interested in pursuing inconvenient, time-consuming searches and stratagems. She already committed to a variety of goals—raising her children, pursuing her career, enjoying her friends, and so on; the time she can allot to buying wine is relatively small. Of course, she could simply not buy wine at all, but Vicky enjoys wine and is not willing to give it up. Thus, as a practical matter, not doing business with wine stores is not an option. This is true even when all assumptions characterizing the ideal transaction conditions hold.

So how can Vicky's consent be free? Constrained choices are, after all, the "example *par excellence* of unfree choices."[80] When a thief holding a gun to your head demands, "Your money or your life!," the thief violates your freedom by compelling your choice. You have only one meaningful option: hand over your money. Informational-norm-governed transactions hardly rise to the level of gun-to-the-head compulsion; nonetheless, they both do, as a practical matter, reduce a person's options to one. Does not the restriction of options entail a lack of free consent?

---

75. Warner, *supra* note 21, at 18.

76. *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1459 (2004).

77. WESTIN, *supra* note 5, at 7 (emphasis added).

78. *See supra* note 59 and accompanying text.

79. *See supra* Part I.

80. Warner, *supra* note 21, at 18.

Margaret Radin argues strongly for a "Yes" answer.[81] According to Radin, free "consent involves a knowing understanding of what one is doing, in a context in which it is *actually possible* for one to do otherwise, and an affirmative action in doing something, rather than a merely passive acquiescence in accepting something."[82] Grant that non-compliance with a norm is not a practical option. Then, does not compliance violate these conditions? It is not "actually possible for one to do otherwise," so how does it not follow that compliance is "merely passive acquiescence in accepting something" and not "an affirmative action in doing something."[83]

It does not follow, because a highly constrained choice can nonetheless be a free choice. Imagine that you long to vacation in the Cayman Islands, but you are convinced that you cannot afford to do so. You then discover an "all inclusive" vacation package which offers airfare, hotel, and food for a single low price. You opt for the package. When you eat the hotel food included in the package, you have no practical option to do otherwise; you cannot afford to eat any other way. Your choice is constrained. But, it was constrained through your own *voluntarily* imposed order to *freely* realize your vacation goal. The choice was one you regarded as better justified than any alternative. In the thief example, earlier, you did not freely choose a scenario that included being robbed by the thief.

Compare Vicky's wine store transaction. Vicky allots only a relatively small amount of time to purchasing wine. She wants to purchase suitable wine within that time and return to pursuing her other goals.[84] She knows the store will process some range of personal information, and she wants an acceptable tradeoff between her informational privacy and the various interest served by processing the information. The wine store norm—process personal information only in ways appropriately related to the store's role as a seller of wine—offers her a ready-made tradeoff that she *knows* is acceptable. It follows from knowledge completeness that Vicky knows what tradeoff the norm entails. But, how does it follow that she knows that tradeoff is acceptable? Vicky knows this because: 1) tradeoffs implemented by value-justified norms are acceptable;[85] 2) norm completeness guarantees that the norm is value-justified;[86] and 3) knowledge completeness guarantees that

81. *See* Margaret Jane Radin, *Humans, Computers, and Binding Commitment*, 75 IND. L.J. 1125, 1125–26 (2000) (equating a lack of options with a lack of consent).

82. *Id.* (emphasis added).

83. *See id.*

84. *Cf.* W. David Slawson, *Standard Form Contracts and Democratic Control of Lawmaking Power*, 84 HARV. L. REV. 529, 532 (1971) (attributing the rise of standard-form contracts to the scarcity of time in modern life).

85. *See supra* Part I.B.

86. *See supra* Part I.B.

Vicky realizes that the norm is value-justified.[87] This means that Vicky need not spend any time discovering what information the store will process about her, nor on negotiating information processing terms should she find the store's intended information processing unacceptable. It bears emphasis that this argument relies on the second premise, that norm completeness guarantees all norms are value-justified. I will return to that point shortly.

Vicky meets two of Radin's three requirements for free consent: "[1] a knowing understanding of what one is doing [2] in a context in which it is actually possible for one to do otherwise, and [3] an affirmative action in doing something, rather than a merely passive acquiescence in accepting something."[88] Vicky meets the first and third requirements. She has "a knowing understanding of what [she] is doing" since she knows what the norm-created tradeoff is and knows that it is acceptable. In addition, consent to the norm-created tradeoff cost-effectively furthers the pursuit of important goals, and is thus is not an "affirmative action" that fits into an overall plan aimed at effectively realizing ends.[89] The only requirement Vicky fails to meet is that it should be "actually possible for one to do otherwise." It is not possible for Vicky to do otherwise—in the sense that she is committed to purchasing wine, and any transaction in which she does so will be governed by the relevant norm. But it is precisely a *pre-packaged* tradeoff Vicky wants; it is the convenient, cost-effective way to pursue ends that is important to her.[90]

I conclude that consumers give free and informed consent to norm-implemented tradeoffs—*under ideal transaction conditions*. This qualification is essential. Ideal conditions include the norm-completeness assumption, which ensures that all norms are value-justified.[91] Recall that norms are value-justified when, in light of the values of *all (or almost all)* members of the group in which the norm obtains, the norm is *at least as well justified as any alternative*.[92] In practice, diversity in values among group members will typically ensure that groups only approximate this definition. For simplicity, set the problem of diversity of values aside.[93] In the case of informational norms governing consumer-merchant transactions, assume that there is sufficient agreement on values to make the simplification permissible. The point to emphasize here is that it is essential to the argument that the norms are value-justified. This is a key step in the argument that consumers know that

87. *See supra* Part II.

88. Radin, *supra* note 81, at 1126.

89. Warner, *supra* note 21, at 20.

90. For a similar examination of these norms as applied to standard form contracts, see Warner, *supra* note 21, at 20.

91. *See supra* Part II.B.

92. *See supra* text accompanying note 45.

93. Value-diversity cries out for further investigation but is outside the scope of this Article.

norm-implemented tradeoffs are acceptable, and hence, that consumers' consent to such tradeoffs qualifies as free.[94] The link between value-justified norms and free consent free plays a pivotal role in the next section. The section examines four scenarios in which advances in information processing technology have had a corrosive effect on informational norms.

IV. THE CORROSIVE EFFECT

I focus exclusively on a single corrosive effect: violations of the norm completeness assumption. I do not mean to suggest that it is unproblematic to assume either that the relevant markets are sufficiently norm-competitive or that the inconsistency-detection and knowledge-completeness assumptions are approximately true. Norm-completeness especially calls for investigation. I focus on norm completeness because it clearly fails to hold in practice, and the failure has important consequences. There are two ways in which norm completeness fails to hold. The first is a lack of relevant norms altogether; the second is a lack of value-justified norms.[95] I examine one example of a lack of norms and three examples in which the norms exist but are not value-justified. The reason for the emphasis on the latter is that I presume that technological advances have created novel transactions that are simply not governed by conventional norms; whereas, on the other hand, the loss of value-justification is less obvious and indeed has so far gone unnoticed.

A. Lack of Norms

As a result of technological advances, businesses now process consumers' personal information in novel ways.[96] In many cases, the following two conditions hold: 1) businesses vary considerably in the degree to which their information processing invades informational privacy; and 2) there is no agreement on the extent to which they *ought* to respect informational privacy.[97] It follows that no relevant informational norm exists. Recall that a norm exists only when there is a regularity to which one thinks one ought to conform.[98] The variation in the privacy-invasiveness of information processing means that no appropriate regularity exists, and the disagreement over how informational privacy ought to be respected shows that there is no regularity to which we

94. *See* Warner, *supra* note 21, at 26.

95. *Id.* at 21.

96. *See* Joseph Phelps et al., *Privacy Concerns and Consumer Willingness to Provide Personal Information*, 19 J. PUB. POL'Y & MARKETING 27, 28 (2000).

97. *Cf.* Diane P. Michelfelder, *The Moral Value of Informational Privacy in Cyberspace*, 3 ETHICS & INFO. TECH. 129, 129 (2001) (citing JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 3 (1992)) (noting inconsistent understandings of privacy by academics).

98. *See supra* Part I.

think we ought to conform.[99] Google's "cloud computing"[100] services are an example.

Google's cloud computer services include Gmail (an email service),[101] Google Docs (a document editing, storage, and sharing service),[102] Google Desktop (an integrated search tool for both a computer's local hard drive and the Internet),[103] Picasa Web Albums (a photo storage and sharing service),[104] Google Calendar (a calendar sharing service), [105] and Google Buzz (a social networking service).[106] Google retains all data generated by users' activity on its servers.[107] Users of these services identify themselves when they log in—an action necessary to use these services—and when they add personal information to documents.[108] The result is that Google obtains and stores a vast amount of personal information.[109]

---

99. *See supra* Part I.

100. In cloud computing, applications and data are stored on servers remotely accessed by web browsers. *See* Peter Mell & Tim Grance, *The NIST Definition of Cloud Computing*, NAT'L INST. OF STANDARDS (Oct. 7, 2009), http://csrc.nist.gov/groups/SNS/cloud-computing/index.html.

101. GMAIL, http://mail.google.com (last visited Apr. 10, 2011).

102. GOOGLE DOCS, http://www.docs.google.com (last visited Apr. 10, 2011).

103. GOOGLE DESKTOP, http://www.desktop.google.com (last visited Apr. 10, 2011).

104. PICASA WEB ALBUMS, http://www.picasaweb.google.com (last visted Apr. 10, 2011).

105. GOOGLE CALENDAR, http://calendar.google.com (last visted Apr. 10, 2011).

106. GOOGLE BUZZ, http://www.google.com/buzz (last visted Apr. 10, 2011).

107. *Privacy Policy*, GOOGLE PRIVACY CTR., http://www.google.com/intl/en/privacy-policy.html (last visited Apr. 10, 2011).

108. Complaint and Request for Injunction, Request for Investigation, and For Other Relief at 7, *In re* Google, Inc. & Cloud Computing Servs. (F.T.C. Mar. 17, 2009), *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf.

109. Here is a brief summary of the information Google processed at the time the Complaint was filed in *In re Google*. Each privacy policy allowed Google to use the information to maintain and improve Google services. Depending on how "maintain and improve" is interpreted, the provision could have granted Google a broad license to use the information as it wishes. On October 3, 2010, however, Google amended their general privacy policy to extend to all products, services, and websites including Gmail, Google Docs, Google Desktop, Picasa Web Albums, Google Calendar, and Google Buzz. *Privacy Policy*, *supra* note 107. For more information, see Zimmer, *supra* note 33, at 115–18 (summarizing Google's information processing practices).

Gmail: "Google records information such as account activity (including storage usage, number of log-ins), data displayed or clicked on (including UI elements, ads, links), and other log information (including browser type, IP-address, date and time of access, cookie ID, and referrer URL)." GMAIL PRIVACY NOTICE, Feb. 9, 2010, http://mail.google.com/mail/help/privacy.html (on file with ST. LOUIS U. L.J.).

Google Docs: "Google records information such as account activity (e.g., storage usage, number of log-ins, actions taken), data displayed or clicked on (e.g., UI elements, links), and other log information (e.g., browser type, IP address, date and time of access, cookie ID, referrer URL). *Content.* Google Docs stores, processes and maintains your files (as well as previous versions of your files), sharing lists, and other data related to your account in order to provide the

No norm defines what a cloud computing service provider may do with the information it processes. To begin with, there is no regularity; the service providers vary significantly in the extent to which their information processing invades informational privacy.[110] Further, as the sharp controversy over cloud computing privacy shows, there is no agreement as to what the regularity ought to be.[111] Similar remarks could be made about a number of other technology-

---

service to you." GOOGLE DOCS PRIVACY POLICY, Oct. 30, 2009, http://www.google.com/google-d-s/privacy.html (on file with ST. LOUIS U. L.J.).

Google Desktop: "The Google Desktop application indexes and stores versions of your files and other computer activity, such as email, chats, and web history. These versions may also be mixed with your Web search results to produce results pages for you that integrate relevant content from your computer and information from the Web. Your computer's content is not sent to Google without your explicit permission. Your copy of Google Desktop includes a unique application number. This number and information about your installation (e.g., operating system type, version number) will be sent to Google when you first install and use it and when Google Desktop automatically checks for updates." GOOGLE DESKTOP PRIVACY POLICY, Nov. 2008, http://desktop.google.com/privacypolicy.html (on file with ST. LOUIS U. L.J.).

Picasa Web Albums: "Google's servers automatically record certain information . . . such as account activity (including storage usage and number of log-ins), data displayed or clicked on (including UI links); and other log information (including browser type, IP-address, date and time of access, cookie ID, and referrer URL)." PICASA PRIVACY NOTICE, Dec. 02, 2008, http://picasa.google.com/privacy.html (on file with ST. LOUIS U. L.J.).

Google Calendar: "Usage statistics. We may record information about your usage of Google Calendar, such as when and for how long you use the service, the frequency and size of data transfers, and the number of events and calendars you create. Information displayed or clicked on in your Google Calendar account (including UI elements, ads, links, and other information) is also recorded for the purposes described below. Every ninety days, if not more frequently, we permanently delete usage statistics associated with your use of Google Calendar. We retain this information beyond 90 days in aggregate form only." GOOGLE CALENDAR PRIVACY NOTICE, Oct. 14, 2010, http://www.google.com/intl/en/googlecalendar/privacy_policy.html (on file with ST. LOUIS U. L.J.).

Google Buzz: "When you use Google Buzz, we may record information about your use of the product, such as the posts you like or comment on and the other users with whom you communicate . . . . Your activity on "connected sites" (such as Picasa Web Albums or Twitter) may be shared in Google Buzz." GOOGLE BUZZ PRIVACY POLICY, May 19, 2010, http://www.google.com/buzz/help/intl/en/privacy.html (on file with ST. LOUIS U. L.J.).

110. *See* ROBERT GELLMAN, WORLD PRIVACY FORUM, PRIVACY IN THE CLOUDS: RISKS TO PRIVACY AND CONFIDENTIALITY FROM CLOUD COMPUTING 6 (2009), *available at* http://www.worldprivacyforum.org/cloudprivacy.html.

111. *Id.* at 4. *See also* Brian Hayes, *Cloud Computing*, COMM. OF THE ASSOC. OF COMPUTING MACHINERY (ACM), July 2008, at 9, 11 (noting that the cloud-computing "issues of privacy and confidentiality are equally perplexing"). In December 2009, the FTC filed a comment with the Federal Communications Commission; the comment noted that the "FTC staff presently is examining "cloud computing" and its privacy and data security implications for consumers." *See* Letter from David C. Vladeck, Office of the Dir. of the Bureau of Consumer Prot., FTC, to Marlene H. Dortch, Sec'y, FCC (Dec. 9, 2009), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=7020352132.

fostered activities, including those utilizing cookies,[112] flash cookies,[113] deep packet inspection,[114] and radio frequency identification tags.[115] By using these devices, consumers provide personal information. But, without relevant informational norms in place, consumers cannot effectively consent to the dissemination of their information to businesses. To lack free and informed consent is to lack informational privacy;[116] but, without relevant informational norms in place, they lack an effective means to give or withhold free and informed consent to the ways in which the businesses will process the information, and to lack free and informed consent is to lack informational privacy.

As important as this conclusion is, to stop the analysis here would be to overlook another important way in which we lack norms. In an important range of cases, relevant informational norms exist but, as a consequence of increased effectiveness in processing information, they are not value-justified.[117] The result is a lack of *value-justified* norms. The consequences are the same: consumers cannot rely on norms to ensure free and informed

112. A cookie is a small text file stored on a computer by a web browser when one visits a web site. *See* HAL ABELSON ET AL., BLOWN TO BITS: YOUR LIFE, LIBERTY, AND HAPPINESS AFTER THE DIGITAL EXPLOSION 40 (4th prtg. 2010). The Internet Engineering Task Force has promulgated an international standard for the use of cookies. Memorandum from David M. Kristol & Lou Montulli, Internet Eng'g Task Force on HTTP State Management Mechanism (Feb. 2007), *available at* http://www.ietf.org/rfc/rfc2109.txt. Uses of cookies that depart from this standard can raise privacy concerns. *See, e.g.*, Lori Eichelberger, *The Cookie Controversy*, Cookiecentral.com, http://www.cookiecentral.com/ccstory (last visited Apr. 11, 2011).

113. Flash cookies are essentially cookies that are stored in a different location. *See What Are Local Shared Objects?*, ADOBE SYS. INC., http://www.adobe.com/products/flashplayer/articles/lso/ (last visited Apr. 11, 2011). Unlike traditional cookies, many users are unaware of their existence and standard spyware removal tools do not delete them; this raises a number of privacy issues. *See* Ashkan Soltani et al., Flash Cookies and Privacy 1 (Aug. 10, 2009) (unpublished Summer Undergraduate Program in Engineering Research at Berkley (SUPERB) study, University of California, Berkley), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862.

114. Deep packet inspection is a technology that allows an ISP to view the content that its subscribers send over the Internet. *See* Ohm, *supra* note 2, at 1468. It has a number of reasonable uses but raises serous privacy concerns.

115. An RFID tag is a silicon chip that emits a radio signal that identifies the tagged item. *See* ABELSON ET AL., *supra* note 112, at 25. RFID tags have number of important uses (for example, they have been implanted in cattle in order to track them). *See id.* They do raise a number of privacy concerns, however. *See* RULE, *supra* note 3, at 182–83 (describing the use of RFID tags to track school children). *See also generally* KATHERINE ALBRECHT & LIZ MCINTYRE, SPYCHIPS: HOW MAJOR CORPORATIONS AND GOVERNMENT PLAN TO TRACK YOUR EVERY MOVE WITH RFID (2005).

116. One might object that a consent requirement could ensure free and informed consent in the absence of norms. I argue against this claim. *See infra* Part V.

117. *See supra* Part I.A.2.

consent to norm-implemented tradeoffs and, hence, cannot rely on such norms to ensure an adequate degree of informational privacy.

An analogy illustrates the connection between increased effectiveness in processing information and the loss of value-justification. Imagine two elementary school friends who adhere to the norm, "throw as hard as you can," when they play catch. One of them moves away and returns later as a teenager. When the reunited friends again play catch, one of them injures the other by throwing the ball with great force. When the injured friend complains, the thrower says that she was simply following the norm to throw as hard as possible. Both agree that, in light of their current physical abilities and values, the norm is no longer value-justified; they no longer think that "throw as hard as you can" is at least as well justified as any other alternative (e.g., "throw half as hard as you can").

Technological advances have made businesses able to "throw harder." Technology makes businesses far more effective in determining whether an individual meets whatever requirements businesses wish to impose.[118] The consequence is the same as in the friends-playing-catch example: the relevant norms are no longer value-justified. There is, however, one crucial difference. The friends would abandon their old norm; in case of business information processing, however, the norms are retained. Thus, like the hockey players, consumers find themselves trapped in conformity to norms that are not value-justified.[119] I offer three examples of businesses that use norms which are not value-justified: the role of retailers in collecting personal information for the purposes of direct marketing; information aggregation services; and the information processing practices of the health insurance industry.

B. Direct Marketing: Retailers as Information Brokers

Direct marketing sorts buyers into groups according to their willingness to purchase certain products and services for the purpose of targeting advertising.[120] Targeted advertising matches advertising content to recipients in ways that maximize the likelihood that recipients will purchase the marketed materials.[121] Defining direct marketing categories requires processing a great deal of personal information about consumers. Retailers routinely collect

---

118. *Cf. Finance*, BUREAU OF CONSUMER PROT.: BUS. CTR., http://business.ftc.gov/selected-industries/finance (last visited Apr. 10, 2011) (describing use of technology by banks to avoid fraudulent consumers).

119. *See supra* notes 47–52 and accompanying text.

120. Carol Scovotti & Lisa Spiller, Abstract, *Revisiting the Conceptual Definition of Direct Marketing: Perspectives from Scholars and Practitioners*, at *3 (2005), *available at* http://www.the-dma.org/dmef/proceedings05/Revisitingthe-Spiller.pdf ("Direct marketing is a database-driven process of directly communicating with targeted customers or prospects using any medium to obtain a measurable response or transaction via one or multiple channels.").

121. Solove, *supra* note 76, at 1404.

sufficient personal data such that they can also function as information brokers.[122] Retailers acting as information brokers play a critical role in feeding direct marketing the personal information it needs.[123] Credit card companies are a convenient example. *Dywer v. American Express Co.*[124] illustrates their information brokerage practices:

> [American Express] categorize[s] and rank[s] [its] cardholders into six tiers based on spending habits and then rent[s] this information to participating merchants as part of a targeted joint-marketing and sales program. For example, a cardholder may be characterized as "Rodeo Drive Chic" or "Value Oriented." In order to characterize its cardholders, [American Express] analyze[s] where they shop and how much they spend, and also consider behavioral characteristics and spending histories. . . . The merchants using the [] service can also target shoppers in categories such as mail-order apparel buyers, home-improvement shoppers, electronics shoppers, luxury lodgers, card members with children, skiers, frequent business travelers, resort users, Asian/European travelers, luxury European car owners, or recent movers.[125]

I make two contentions: first, that allowing retailers to function as information brokers for the purposes of direct marketing is a *norm*; and second, that the norm is not value-justified. An essential preliminary to arguing for this claim is a fuller description of direct marketing.

1. Direct Marketing

The development of direct marketing provides an excellent example of how advances in information processing technology can enable businesses to "throw harder"—to more effectively determine a specific individual's willingness to purchase. Direct marketing was not particularly effective and, hence, not widely used until the 1970s.[126] Prior to that time, direct marketers did a poor job of differentiating consumers according to their willingness to

---

122. *Id.* at 1408 ("An increasing number of companies with databases—magazines, credit card companies, stores, mail order catalog firms, and even telephone companies—are realizing that their databases are becoming one of their most valuable assets and are beginning to sell their data."). An information broker collects, analyzes, and distributes information to clients. ANGIE A. WELBORN, CONG. RESEARCH SERV., RS22087, INFORMATION BROKERS: FEDERAL AND STATE LAWS 2 n.2 (2005) (citations omitted).

123. Daniel Solove notes:

> The effectiveness of targeted marketing depends upon data . . . . Billions of bytes are released each second as we click, charge, and call. A treasure trove of information already lay untapped within existing databases, retail records, mailing lists, and government records. All that marketers had to do was plunder it as efficiently as possible.

DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 19 (2004).

124. 652 N.E.2d 1351 (Ill. App. Ct. 1995).

125. *Id.* at 1353.

126. Solove, *supra* note 76, at 1405–06.

buy various products and services.[127] This changed in the 1970s, when the government began selling census data on magnetic tapes.[128] Marketing companies used the data to construct databases divided according to, *inter alia*, "age, income level, race, ethnicity, gender, and geographical location."[129] In the 1980s, marketers supplemented this data with "psychographic" information such as opinions, lifestyles, likes and dislikes, and hobbies.[130] The rich data set, along with advances in database technology and information processing, make direct marketing remarkably effective.[131]

> Such is the sophistication of American direct marketing that . . . [o]ne can reasonably expect to purchase a listing of five thousand women who are both public employees and wear sexy underwear; or business owners who espouse far-right political causes; or registered Republicans who are purchasers of pornography—or, for that matter, of pornography with S-M themes. . . . [You can purchase the] guest list information from a hotel frequented by lesbians . . . [and lists of] women who buy wigs; callers to a romance telephone service; impotent middle-aged men; gamblers; buyers of hair removal products; male buyers of fashion underwear; believers in the feminist political movement, anti-gay movement, and prayer in the public schools movement.[132]

Direct-mail marketing "yields $10 in sales for every $1 in costs—a ratio double that for a television advertisement"[133] and accounts for just over half of all advertising expenditures.[134]

The effectiveness of direct marketing is a boon to businesses.[135] Businesses are not, however, the only beneficiaries of direct marketing.

---

127. *See id.* at 1405 (listing only a 2% success rate for direct marketing).

128. *Id.* at 1406.

129. *Id.*

130. *Id.*

131. Solove, *supra* note 76, at 1407.

132. RULE, *supra* note 3, at 104.

133. Solove, *supra* note 76, at 1407.

134. *Direct Marketing Advertising Expenditures Account for 53% of Total Advertising Expenditures, DMA's 'Power of Direct Marketing' Report Unveils*, DIRECT MKTG. ASS'N (Oct. 13, 2008), http://www.the-dma.org/cgi/disppressrelease?article=1228.

135. It is especially important in the case of new products or services:

> Once a business has developed a new product or service, it must inform potential customers. The cost of alerting consumers about a new product or opportunity can be a major obstacle to the launch of new businesses and prevent innovative products from ever reaching the marketplace. . . . "Target marketing" allows a business to send an offer to a customer specifically identified as likely to be interested. In the absence of information that indicates which consumers are likely customers, businesses must choose between marketing randomly, contacting everyone in an entire geographic community, or relying solely on mass media advertising to reach potential customers.

Fred H. Cate & Michael E. Staten, *The Value of Information Sharing* (Nat'l Retail Fed'n Protecting Privacy in the New Millennium Ser., July 28, 2000), *available at* http://www.bbbonline.org/UnderstandingPrivacy/library/whitepapers/valueofinfosharing.pdf.

Consumers benefit from more efficient businesses, access to new products and services, and from receiving information relevant to their needs and interests.[136] The cost is a loss of informational privacy.[137] The more one loses the ability to control how others process one's personal information, the more one loses informational privacy.[138] The information processing activities that support direct marketing involve a significant loss of control; indeed, direct marketing is a prime example of "mass surveillance"—the use of "[s]ystematically harvested personal information . . . to determine what treatment to mete out to each individual."[139] This "systematic harvesting" is facilitated by the fact that, as noted earlier, "it has become increasingly rare to deal with any . . . private-sector organization without generating and relying upon a database of personal information."[140]

2. The "Retailers as Information Brokers" Norm

Despite the loss of control, the norm is that retailers may act as information brokers for direct marketing purposes.[141] The relevant regularity clearly obtains: retailers do act as information brokers. The regularity is, moreover, sanction-supported. Interacting with businesses typically involves "generating and relying upon a database of personal information,"[142] and the sanction for refusing to generate or rely on such information is typically that one cannot interact with the business or must do so on less favorable terms.[143] Refusal to issue a credit card is, for example, a possible sanction for not agreeing to credit card companies' information brokerage activities, and foregoing discounts and other advantages is the cost for refusing to use retailers' discount cards.[144] In light of the sanctions, most think they ought to conform to the norm. One can forgo having a particular credit card or using a particular discount card, but wholesale avoidance of generating and relying on databases of personal information would mean a wholesale avoidance of a wide range of commercial

136. *Privacy, Current Legislation and DMA Action*, DIRECT MKTG. ASS'N, http://www.the-dma.org/cgi/dispissue?article=129 (last visited Sept. 30, 2010).

137. MILLS, *supra* note 7, at 271.

138. *Id.*

139. *See* RULE, *supra* note 3, at 14 (defining mass surveillance).

140. Rule, *supra* note 4, at 183.

141. *See id.* at 196 (describing how information is shifted from one sphere to another).

142. *Id.* at 183.

143. *See, e.g.*, *MasterCard Worldwide-Global Privacy Policy*, MASTERCARD (June 1, 2010), http://www.mastercard.com/us/personal/en/general/global-privacy-notice.html (predicating access to some services on consent to information dispersal).

144. *Id.*

interactions,[145] and for most, that sanction is unacceptable. As Hal Abelson, Ken Ledeen, and Harry Lewis note:

> [W]e give up data about ourselves because we don't have the time, patience, or single-mindedness about privacy that would be required to live our daily lives in another way. In the U.S., the number of credit, debit, and bank cards is in the billions. Every time one is used, an electronic handshake records a few bits of information about who is using it, when, where, and for what. It is now virtually unheard of for people to make large purchases of ordinary consumer goods with cash. Personal checks are going the way of cassette tape drives, rendered irrelevant by newer technologies. Even if you could pay cash for everything you buy, the tax authorities would have you in their databases anyway.[146]

Consumers might choose to bear the sanctions temporarily in a general consumer revolt; however, *unilateral* non-conformance by any one consumer carries sanctions that make non-conformity a choice each consumer avoids. Most, therefore, decide that on prudential grounds they ought to conform (or would after adequate reflection, so decide).[147]

3. The Norm is Not Value-Justified

The norm is nonetheless not value-justified. Consumers conform to the "retailers as information brokers" norm in order to avoid the sanctions of non-conformity, but—I contend—they do not regard the "retailers as information brokers" norm as at least as well-justified as any alternative. Consumers instead regard an alternative in which they have more control over their personal information as better justified. This is the most plausible interpretation of over twenty years of studies and surveys about consumer attitudes toward privacy.[148] A typical study found that 89% of consumers had either a "high concern" (53.7%) or a "medium concern" (35.5%) about "general privacy."[149] Table 1 reproduces the results of that study.

---

145. Posner, *supra* note 6, at 248 ("[A] person would have to be a hermit to be able to function in our society without voluntarily disclosing a vast amount of personal information to a vast array of public and private demanders.").

146. ABELSON ET AL., *supra* note 112, at 41–42. Indeed, it is nearly impossible in practice to avoid all data collection. "Regardless of how cautious and informationally conservative a consumer is, they do not have the ability to live a modern life and avoid being systemically profiled. Consumer profiling is currently unavoidable by the majority of consumers." Letter from Pam Dixon, Exec. Dir., World Policy Forum, to Fed. Trade Comm. 10 (Nov. 6, 2009), *available at* http://www.worldprivacyforum.org/pdf/WPF_Comments_FTC_110609fs.pdf.

147. *See supra* note 68 and accompanying text.

148. There is an excellent collection of relevant studies in an online database maintained by Alessandro Acquisti. *See* Alessandro Acquisti, *The Economics of Privacy*, http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm (last visited Sept. 30, 2010).

149. Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, IEEE SEC. & PRIVACY, Jan./Feb. 2005, at 26, 28 tbl.1.

Table 1[150]

	General privacy concern (%)	Data about offline identity (%)	Data about online identity (%)	Data about personal profile (%)	Data about professional profile (%)	Data about sexual and political identity (%)
High Concern	53.7	39.6	25.2	0.9	11.9	12.1
Medium Concern	35.5	48.3	41.2	16.8	50.8	25.8
Low Concern	10.7	12.1	33.6	82.3	37.3	62.1

Of course, finding that consumers are "concerned" does not mean that they are concerned *about the loss of control* over their private information, but why else would consumers be concerned? The concern is surely that others will do something unacceptable with the information.[151] It would be strange if this were not true. In general, control is an important consideration in determining whether to enter into or continue a relationship.[152] One may, for example, refuse to associate with someone because he or she is too controlling. In commercial relationships, conformity to the "retailers as information brokers" norm entails a significant loss of control over personal information; direct marketing is, as noted earlier, an example *par excellence* of mass surveillance. Why would one not be seriously concerned about such a loss of control? As the privacy advocates remind us, a significant degree of control is essential to "intimacy, friendship, dignity, individuality, human relationships, autonomy, freedom, self-development, creativity, independence, imagination, counterculture, eccentricity, freedom of thought, democracy, reputation, and psychological well-being."[153] Anyone—and that is virtually everyone—who values at least some of the items in this list values informational privacy and is, therefore, concerned with retaining an appropriate degree of control over personal information.

The conclusion would seem unavoidable that the "retailers as information brokers" norm is not value-justified. It is value-justified only if, in light of consumers' values, it is at least as well justified as any alternative.[154] But, it seems clear that consumers regard as better justified alternatives that allow

150. *Id.*

151. Alessandro Acquisti seems to take it for granted that this is the explanation. *See* Alessandro Acquisti, *Privacy and Security of Personal Information: Economic Incentives and Technological Solutions*, *in* ECONOMICS OF INFORMATION SECURITY 179, 182 (L. Jean Camp & Stephen Lewis eds., Kluwer Int'l Ser. on Advances in Info. Sec., 2004).

152. Acquisti & Grossklags, *supra* note 149, at 27.

153. SOLOVE, *supra* note 7, at 98.

154. *See* Warner, *supra* note 21, at 8–9.

them to retain more control over their personal information.[155] There is, however, a seemingly serious objection: the studies referred to above actually contain conflicting results. Although a large number of studies show consumers are concerned about losing control over personal information, there is evidence that individuals value privacy less than they may claim; in fact, "many are willing to trade off personal information for small rewards."[156] The "retailers as information brokers" norm would seem to be a case in point. If consumers find the loss of control objectionable, why do they conform when the cost of non-conformity is mere inconvenience and loss of some minor advantages such as discounts?

This point does not disconfirm the claim that the norm is not value-justified; it confirms it. The point is precisely what one should expect if consumers are trapped in conformity to a norm that is not value-justified. The hockey players' "no helmet" norm illustrates the point.[157] The hockey players did not wear helmets even though their values made "all players wear helmets" a far better-justified alternative. The sanctions were sufficient to ensure players did not *unilaterally* decide to violate the norm. Similarly, consumers conform to the "retailers as information brokers" norm even though their values make "consumers have more control" a much better-justified alternative. The sanctions are sufficient to discourage *unilateral* non-conformity.[158] Like the no-helmet-norm hockey players, consumers are trapped in conformity to a norm that is not value-justified.

As noted earlier, conformity to informational norms counts as free consent to norm-implemented tradeoffs only if the norms are value-justified.[159] Sanction-compelled conformity to norms that are not value-justified is

155. For a sketch of a system that would provide more control, see Daniel J. Weitzner et al., *Information Accountability*, 51 COMM. OF THE ACM, June 2008, at 82, 86. For discussion and criticism, see Robert H. Sloan & Richard Warner, *Developing Foundations for Accountability Systems: Informational Norms and Context-Sensitive Judgments*, *in* 2010 ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE, at 21, *available at* http://www.acsac.org/2010/workshop/p21-sloan.pdf.

156. Jens Grossklags & Alessandro Acquisti, *When 25 Cents Is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information*, *available at* http://weis2007.econinfosec.org/papers/66.pdf. *See also* Acquisti & Grossklags, *supra* note 149, at 26, 31 (finding consumers to have misconceptions regarding loss of privacy); Beales & Muris, *supra* note 14, at 114 ("Judging by behavior in the marketplace, most consumers have better things to do with their time than read privacy notices."); Luc Wathieu & Allan Friedman, *An Empirical Approach to Understanding Privacy Valuation* 1–3 (Harvard Bus. Sch., Working Paper No. 07-075, 2007), *available at* http://www.hbs.edu/research/pdf/07-075.pdf (noting that consumers trade privacy for economic gain and proposing a model of the tradeoff).

157. *See supra* notes 47–52 and accompanying text.

158. *See* Acquisti & Grossklags, *supra* note 149, at 31 (discussing how cost may discourage a consumer from adopting a privacy technology).

159. *See supra* Part I.A.2.

compelled conformity to an alternative inconsistent with one's values and should not count as free consent to the norm-implemented tradeoff. It follows that consumers do not give free and informed consent to the tradeoff implemented by the norm, and hence, they do not have an adequate degree of informational privacy.

C. *Information Aggregators*

Information aggregators are businesses that collect and resell personal information.[160] ChoicePoint, one of the largest, obtains 40,000 new records daily for its ever-growing database of more than 19 billion records.[161] ChoicePoint's clients include government agencies, insurance companies, employers doing background checks, direct marketers, and potentially anyone with an interest in obtaining information about others.[162] I contend that it is a norm that information aggregators may process and resell any type of information (within legal limits) and that the norm is not value-justified.

The relevant regularity clearly exists: information aggregators do process and resell a wide variety information. The sanction for non-conformity is the same as in the case of the "retailers as information brokers" norm: wholesale avoidance of generating and relying on databases of personal information would mean a wholesale avoidance of a wide range of commercial interactions.[163] For most consumers, the considerable inconvenience and loss of various advantages and privileges is unacceptable.[164] Most, therefore, decide on prudential grounds that they ought to conform.[165] The norm is nonetheless not value-justified. The argument is again the same as in the case of the "retailers as information brokers" norm. Consumers value privacy in ways that lead them to better justify an alternative in which they have greater control over information processing practices.[166] The lack of value-justification means that consumers do not give free and informed consent to

160. Beales & Muris, *supra* note 14, at 109–10.

161. Duane D. Stanford, *All our Lives are on File for Sale*, ATLANTA J. CONST., Mar. 21, 2004, at A1.

162. For information about ChoicePoint, see ROBERT O'HARROW, JR., NO PLACE TO HIDE 2 (paperback ed. 2006).

163. *See supra* note 145 and accompanying text.

164. ChoicePoint collects information from two sources: public records and private sources, and one can attempt to foil ChoicePoint's processing by not disclosing information to the latter, or by providing misrepresentations in what one does disclose. *See* O'HARROW, *supra* note 162, at 2. Public records may arise from mandatory disclosure (recording property transactions, for example), or voluntary disclosures under penalty of perjury (as in court proceedings); failure to disclose and misrepresentation risk legal and non-legal sanctions.

165. *See id.* at 7 (discussing the American desire to trade freedom for security, in the wake of the United States Patriot Act).

166. *See supra* Part IV.B.3.

the tradeoff implemented by the norm, and hence, they do not have an adequate degree of informational privacy.

The exact parallels with the "retailers as information brokers" norm do not deprive the "information aggregator" norm of interest. On the contrary, one of the hallmarks of contemporary personal-information processing is the flow of information from various businesses and other sources to information aggregators.[167] Unlike collecting information *exclusively* for purposes of direct marketing, the practices of information aggregators ensure that information collected on one occasion for one purpose is retained, analyzed, and distributed for a variety of purposes to anyone who may lawfully obtain the information.[168] One critical concern is that bits and pieces of personal information, innocuous when taken separately, can be aggregated into a permanently available and highly revealing profile.[169] Privacy advocates paint disturbing pictures of the possible consequences. Daniel Solove, for example, contends:

> We're heading toward a world where an extensive trail of information fragments about us will be forever preserved on the Internet, displayed instantly in a Google search. We will be forced to live with a detailed record beginning with childhood that will stay with us for life wherever we go, searchable and accessible from anywhere in the world. This data can often be of dubious reliability; it can be false and defamatory; or it can be true but deeply humiliating or discrediting. We may find it increasingly difficult to have a fresh start, a second chance, or a clean slate. We might find it harder to engage in self-exploration if every false step and foolish act is chronicled forever in a permanent record. This record will affect our ability to define our identities, to obtain jobs, to participate in public life, and more.[170]

Solove is merely describing *possibilities*, but these possibilities highlight a *fact*: data aggregation entails a significant lost control over our personal information.[171] The connection possibilities and fact is hardly unique to personal information. The possibility of having to make an emergency stop,

---

167. O'HARROW, *supra* note 162, at 2.

168. *Id.*

169. Solove, *supra* note 76, at 1452.

170. DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 17 (2007).

171. Privacy advocates are often criticized for merely describing possibilities. The possibilities may be illustrated by actual cases, but the essential point is that the same thing *might* happen to us. *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1154 (2004) ("[T]he typical privacy article rests its case precisely on an appeal to its reader's intuitions and anxieties about the evils of privacy violations."). The criticism is certainly just. James Rule laments that privacy advocates too often rely on "gut reactions." RULE, *supra* note 3, at 183. However, merely to make this criticism misses one underlying point of the describing the possibilities: they demonstrate the *fact* of loss of control.

for example, highlights the fact that driving a car at 80 miles per hour involves a significantly greater chance for loss of control when compared to driving at 50 miles per hour. Similarly, the degree and significance of our loss of control over our personal information is illustrated by the possible outcomes to which it exposes us.

As important as the loss of control is, it is not the only reason one should be concerned about a loss of informational privacy. As the next example illustrates, technologically-enhanced information process can lead to objectionable outcomes that do not consist just in a loss of control.

D. The Health Insurance Industry

Health insurers make money by collecting more in premiums than they pay out in compensation; to do so, they must correlate premiums with risks.[172] This requires processing personal information about morbidity and mortality, in order to identify high risk individuals.[173] They can then control the ratio of compensation to premiums by refusing to insure high-risk applicants, discontinuing insuring current high-risk customers, or charging high-risk applicants and customers higher premiums.[174] Keeping insurance companies in business benefits both the companies and the consumers who pay for their health care through insurance.[175] One cost is a loss of informational privacy. Consumers lose control over personal information pertaining to mortality and morbidity. I contend that it is a norm that health insurance companies may process any legally obtained personal information relevant to determining risks of morbidity and mortality and that the norm is not value-justified.

Insurance companies do routinely process such health information, and this regularity is sanction-supported.[176] To illustrate the sanctions, suppose that after his wife dies, Jones' doctor prescribes Prozac for Jones' temporary depression. Jones' insurance pays both for the office visit and for the Prozac. Five years later, Jones leaves his employment—and his employer-provided health insurance—to open his own business. Fearing that the diagnosis of depression and the prescription of Prozac could lead to the denial of insurance or higher premiums,[177] he omits noting the depression diagnosis and corresponding prescription on his application for insurance. If the insurance

172. Jeffrey Manns, Note, *Insuring Against Terror?*, 112 YALE L.J. 2509, 2515 (2002).

173. *See id.*

174. Manns, *supra* note 172, at 2515.

175. In addition, it has the benefits typically associated with allowing a business to collect information. *See supra* note 1 and accompanying text.

176. *See* Lawrence Gostin, *Health Care Information and the Protection of Personal Privacy: Ethical and Legal Considerations*, 127 ANNALS OF INTERNAL MED. 683, 685 (1997).

177. *See How a History of mental Illness Affects Your Life Insurance Rates*, INSURE.COM, http://www.insure.com/articles/lifeinsurance/mental-illness.html (last visited Sept. 30, 2010).

company discovers the omission, sanctions include the denial of coverage and liability for fraud.[178]

It is highly likely that the company will discover the omission. The health insurance industry's use of information aggregation services makes it quite difficult to conceal medical history.[179] The industry uses both general information aggregators like ChoicePoint and specialized ones like the Medical Information Bureau (MIB).[180] MIB is a trade association whose insurance company members share information in the form of MIB records.[181] MIB claims that the "MIB Checking Service is the fastest, most effective way to prevent omissions and material misrepresentations on insurance applications. It's the only method available during underwriting to help you immediately confirm whether the information applicants provide is accurate and complete."[182] Such information aggregators allow health insurance companies to effectively detect and sanction those who fail to conform to the regularity of allowing the companies to process personal information concerning morbidity and mortality.

In light of the sanctions, most consumers think they ought to conform. One may occasionally succeed in concealing information about morbidity and mortality, but on the whole, health insurance companies are likely to acquire such information despite attempts at concealment, and the likely sanction—

178. *See, e.g.*, ANTHEM, MISSOURI: INDIVIDUAL ENROLLMENT APPLICATION 8 (2011), *available at* http://docs.anthem.com/wellpoint/docs/viewDocument?mcItemNbr=AMO-103C-ER. Courts uphold the right to collect the information, either because the information is publicly available or because consumers have contractually agreed to the companies' data collection activities.

179. Services specifically targeting the health insurance industry include MIB Group, Inc., http://www.mib.com (last visited Apr. 10, 2011), which collects, uses, and distributes information from health insurance applications, and *Milliman IntelliScript*, MILLIMAN, http://www.milliman.com/expertise/healthcare/products-tools/intelliscript (last visited Apr. 10, 2011). Insurers can use Milliman IntelliScript to gather prescription information in real time and then review an easy-to-read online report. *Id.*

180. *See* RENEE MARLIN-BENNETT, KNOWLEDGE POWER: INTELLECTUAL PROPERTY, INFORMATION, AND PRIVACY 194 (2004) (noting that MIB has existed since 1902 but that technology has greatly increased its power to process information).

181. *Actuarial and Statistical Research Group*, MIB GROUP, INC., http://www.mibsolutions.com/risk_analytics (last visited Apr. 11, 2011). MIB records consist of codes indicating medical conditions which affect morbidity or mortality. JON SHREVE, MILLIMAN PROTECTIVE VALUE STUDY: THE IMPACT OF THE MIB CHECKING SERVICE ON HEALTH INSURANCE UNDERWRITING (2006), *available at* http://www.mibsolutions.com/pdf/20060310 20MILLIMAN 20HEALTH 20PV 20SUMMARY.pdf.

182. *MIB Checking Service-Issue with Confidence*, MIB GROUP, INC, http://www.mibsolutions.com/health (last visited Apr. 11, 2011).

denial of coverage[183]—is a disaster in a market economy in which one pays for health care through health insurance. The loss of coverage is thus a risk most think they should avoid. Hence, on the whole, the only reasonable option is to conform to the norm by not attempting to conceal information about morbidity and mortality.[184]

The norm is, however, not value-justified. As in the previous two examples, one reason the norm is not value-justified is that consumers regard an alternative in which they have more control over their personal information as better justified. In this case, however, there is an additional reason the norm is not value-justified: consumers also regard as better justified an alternative that *differently distributes health care.* To see why, consider that the distribution of health care in the United States is determined, in large part, by the distribution of private health insurance.[185] The vast majority of those who have carefully reflected on the problem without bias or prejudice have concluded that the distribution is seriously flawed; many who ought to have health care go without.[186] Thus, if we—people in general—were to reflect adequately on the issue, it is highly likely we would regard an alternative distribution as better justified. The conclusion remains the same as before: consumers do not give free and informed consent to the tradeoff implemented by the norm, and hence, they do not have an adequate degree of informational privacy.

E. Further Examples

The foregoing examples are not isolated instances. One could make the similar claims about lack of value-justification in a number of cases, including: employer use of information in hiring and retention decisions,[187] the extension

183. *See, e.g.*, ANTHEM, *supra* note 178, at 8 ("If we issue coverage to you and then discover an act, practice, or omission that constitutes fraud or intentional misrepresentation of material fact, we may rescind your coverage, even after it has been issued.").

184. One might object that this is not true of someone who, for example, thinks it is always morally wrong to lie (even to an insurance company) and who would thus not attempt to conceal information through deceit. That person would conform *because* he or she thinks lying is wrong. But this just shows that the person has two reasons to conform: lying is always wrong; and, there is no other reasonable option.

185. Laura D. Hermer, *Private Health Insurance in the United States: A Proposal for a More Functional System*, 6 HOUS. J. HEALTH L. & POL'Y 1, 2 (2005).

186. *See* ASSISTANT SEC'Y FOR PLANNING & EDUC., U.S. DEP'T OF HEALTH & HUMAN SERVS., OVERVIEW OF THE UNINSURED IN THE UNITED STATES: AN ANALYSIS OF THE 2005 CURRENT POPULATION SURVEY (2005), *available at* http://aspe.hhs.gov/health/reports/05/uninsured-cps (displaying demographics of the uninsured).

187. Employer use of information aggregators allows employers to acquire a wide range of personal information including information applicants or employees attempt to conceal. The sanction for concealment is typically denial of employment and possible legal liability; such sanctions are so severe that, for most, the only reasonable option is not to attempt to conceal

of credit,[188] news reporting,[189] and the practice of price discrimination.[190] Let us continue, however, to focus on the direct marketing, information aggregator, and health insurance examples. In each case, we—like the pre-1979 hockey players[191]—are trapped in conformity to a norm inconsistent with our values. I contend that individuals should respond by seeking to create relevant value-justified norms. The task is by no means easy. To see why, consider one critical difference between the examples and the hockey players. It was easy for the hockey players to specify a NHL-mandated helmet requirement as an alternative to the no-helmet norm.[192] It is far more difficult to specify alternatives to the norms in the previous examples. People want more control and a better distribution of health care, but describing how best to achieve that requires explaining how to balance a variety of competing concerns, and it is by no means clear how to strike the balance. But doesn't this overlook an obvious and much simpler solution: require consent?

---

information they employer may regard as relevant. Privacy advocates warn that information aggregators have given employers such an extensive power to peer into the lives of applicants and employees that:

> [O]ur society will see a growing number of individuals who are disenfranchised for life. Large numbers will not be able to find employment because of negative information . . . —whether true or not—from years gone by. Or they will be relegated to lower-paying jobs in the service industries, unable to bring their true abilities into the employment marketplace. We [www.privacyrights.org] have been contacted by many such individuals in our ten-year history.

Beth Givens, *Public Records on the Internet: The Privacy Dilemma*, PRIVATE RIGHTS CLEARINGHOUSE (Apr. 19, 2002), http://www.privacyrights.org/ar/onlinepubrecs.htm.

188. James Rule discusses the greatly enhanced ability of creditors to determine whether their criteria of credit worthiness are fulfilled. *See* RULE, *supra* note 3, at 102; Charles Duhigg, *What Does Your Credit-Card Company Know About You?*, N.Y. TIMES MAG., May 17, 2009, at 40.

189. Technology has both expanded reporters access to information and their ability to report it through non-traditional means such as blogs. The greatly increased depth to which reporters can penetrate into people's lives is highly controversial. *See* MILLS, *supra* note 7, at 287.

190. Price discrimination is "[t]he practice of offering identical or similar goods to different buyers at different prices when the costs of producing the goods are the same." BLACK'S LAW DICTIONARY 1227 (8th ed. 2004). It is a long-established practice that has greatly increased in frequency as the result of technological advances. *See* Andrew Odlyzko, *Privacy, Economics, and Price Discrimination on the Internet*, *in* ICEC2003: FIFTH INTERNATIONAL CONFERENCE ON ELECTRONIC COMMERCE 355–66 (N. Sadeh ed., 2003), *reprinted in* ECONOMICS OF INFORMATION SECURITY, *supra* note 151, at 187. Price discrimination requires sorting buyers into groups according to their willingness to pay, and that requires a significant amount of information. Consequently, sellers structure their interactions so they can collect and use the necessary information. *Id.* at 355. Price discrimination and its data collection practices are controversial. *See generally* Douglas M. Kochelek, Note, *Data Mining and Antitrust*, 22 HARV. J.L. & TECH. 515 (2009).

191. *See supra* notes 47–52 and accompanying text.

192. *See supra* notes 47–52 and accompanying text.

V. A CONSENT REQUIREMENT IS NOT A SOLUTION

A consent requirement will not ensure an adequate degree of informational privacy. First, individuals simply do not invest the time, attention, and effort needed to read the privacy notices.[193] Second, even if they did, it would be practically impossible to devote enough time to obtain and understand all the relevant information.[194] Third, even if they could obtain and understand all the relevant information, they would, in a wide range of cases, make an undesirable tradeoff between informational privacy and competing concerns.[195] I consider each objection in turn.

A. Consumers Do Not Read Privacy Notices

It is commonplace to note that consumers typically do not take the time to read privacy provisions in contracts or privacy polices.[196] "Judging by behavior in the marketplace, most consumers have better things to do with their time than read privacy notices. . . . [P]rocessing privacy notices is a cost that most consumers apparently do not believe is worth incurring. The perceived benefits are simply too low."[197] There is good reason for consumers to adopt this attitude. To begin with, reading and understanding a privacy notice requires reading and understanding a considerable amount of information, some of which is couched in legalese.[198] Imagine, for example: George downloads the latest version of Adobe Reader®. Three accompanying documents address Adobe's rights to use personal information related to the Reader's download and use: the privacy policy (approximately 3 single-space pages); the terms of use agreement (21 numbered paragraphs); and the license

193. *See* Robert A. Hillman, *Online Consumer Standard Form Contracting Practices: A Survey and Discussion of Legal Implications*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 283, 283 (Jane K. Winn ed., Markets and the Law Ser., 2006).

194. Melvin Aron Eisenberg, *The Limits of Cognition and the Limits of Contract*, 47 STAN. L. REV. 211, 241 (1995).

195. Beales & Muris, *supra* note 14, at 116–17.

196. *See* Kang, *supra* note 12, at 1248 ("For numerous reasons, such as transaction costs, individuals and information collectors do not generally negotiate and conclude express privacy contracts before engaging in each and every cyberspace transaction."). The failure to read privacy policies is hardly surprising given the well-documented fact that consumers do not read standard form contracts in general. *See, e.g.*, Melvin Aron Eisenberg, Commentary, *Text Anxiety*, 59 S. CAL. L. REV. 305, 305 (1986) ("[C]onsumers who are faced with the dense text of form contracts characteristically respond by refusing to read."). *See also* Hillman, *supra* note 193, at 289 (reporting survey results in which 44% of respondents did not read standard form contracts); Michael I. Meyerson, *The Reunification of Contract Law: The Objective Theory of Consumer Form Contracts*, 47 U. MIAMI L. REV. 1263, 1269 (1993) ("It is no secret that consumers neither read nor understand standard form contracts.").

197. Beales & Muris, *supra* note 14, at 114.

198. Eisenberg, *supra* note 194, at 241.

agreement (5 single-space pages).[199] The latter two contain a number of terms that require a significant knowledge of contract and intellectual property law to fully interpret and understand.[200] Reading these documents requires a significant amount of time, and reading with full understanding is simply beyond the capacity of those without the relevant legal knowledge. Simplifying the notices to make reading them faster and easier will not yield *informed* consent. Notices that attempt to provide enough information for consent to be informed tend to be like the financial privacy notices one receives from one's bank—"long, complex, and filled with legal jargon."[201] In general, "any notice that provides meaningful information about the actual uses of information in the modern economy will necessarily impose costs on consumers who must read and process the information."[202]

B. Informed Consent as a Practical Matter is Impossible

Even if consumers did read and understand privacy notices, they would not obtain all the information necessary to give informed consent. The problem is that information collected on one occasion for one purpose is typically retained, analyzed, and distributed for a variety of other purposes in unpredictable ways.[203] The unpredictability of future uses makes informed consent a practical impossibility.[204] Daniel Solove emphasizes this point:

> An individual may give out bits of information in different contexts, each transfer appearing innocuous. However, the information can be aggregated and could prove to be invasive of the private life when combined with other information.... From the standpoint of each particular information transaction, individuals will not have enough facts to make a truly informed decision. The potential future uses of that information are too vast and unknown to enable individuals to make the appropriate valuation.[205]

C. The Overall Pattern of Free and Informed Consent Would Yield Undesirable Tradeoffs

Suppose consumers could obtain and understand all relevant information. The resulting overall pattern of consent would determine a tradeoff between

---

199. ADOBE READER, http://get.adobe.com/reader/ (last visited Sept. 29, 2010).

200. *See, e.g., id.* Such clauses include a dispute resolution process, disclaimers that "Adobe may change the Terms from time to time at its sole discretion," and reserved rights: "You may not assign (or grant a sublicense of) your rights to use the Software, grant a security interest in or over your rights to use the Software, or otherwise transfer any part of your rights to use the Software." *Id.*

201. Beales & Muris, *supra* note 14, at 113.

202. *Id.* at 114.

203. Solove, *supra* note 76, at 1452.

204. *See id.* at 1426–27.

205. *Id.* at 1452.

privacy and competing concerns. Is there any reason to think the tradeoff will result in the socially optimal balance between informational privacy and competing concerns? There would be reason to think if: 1) the giving or withholding of consent signaled consumers' preferences with regard to consent to sellers; 2) sellers responded to these signals by altering their offerings to reflect these values; 3) buyers responded by preferring products and services consistent with their preference about consent to those inconsistent; 4) this feedback mechanism yielded the socially optimal allocation of information. But even if (1) through (3) are true, there is no reason to think (4) is. To take a simple example, consider telephone books. Telephone books usefully facilitate communication—the more so, the more numbers they contain. Suppose, however, while most of us prefer telephone books with most other people's numbers in them, a majority of us also prefer not to have our individual numbers listed. If consent was required before a number could be listed, reasonably comprehensive telephone books would not exist, and we would lose the aid to communication that most of us prefer. Similar suboptimal results are likely in reality. "[T]here is often little individual incentive to participate in the aggregation of information about people, [yet] an important collective good results from the default participation of most people."[206]

VI. COLLABORATE OR RESIST?

There are two ways to remedy a situation in which a norm lacks value-justification: collaborate (retain the norm and change one's values to make the norm value-justified);[207] or resist (replace the norm with a value-justified one).[208] Privacy advocates make a strong case against collaboration. They emphasize that a significant degree of informational privacy is essential to "intimacy, friendship, dignity, individuality, human relationships, autonomy, freedom, self-development, creativity, independence, imagination, counterculture, eccentricity, freedom of thought, democracy, reputation, and psychological well-being."[209] For anyone who assumes that a significant degree of informational privacy is a necessary means to these ends, resistance (creating value-justified norms) is the only reasonable option. The critical question is what combination of these factors will most likely produce the necessary value-justified informational norms. I leave this question unanswered. My goal has been to define the target, not explain how to hit it. How to do so is a complex question requiring a detailed examination of how best to approximate the four conditions defining ideal transaction conditions.

206. Kent Walker, *The Costs of Privacy*, 25 HARV. J.L. & PUB. POL'Y 87, 95 (2001).

207. *See supra* pp. 1070–72.

208. Warner, *supra* note 21, at 14.

209. SOLOVE, *supra* note 7, at 98.