

The Other Privacy Crisis:
Informational Privacy, Undermined Norms, and Loss of Control

Richard Warner

Abstract

Informational privacy consists in the ability to control one's personal information. Advances in information processing technology have reduced informational privacy by giving others the power to determine when our personal information is collected, and how it used and distributed. Privacy advocates the sound alarm—in regard to both the governmental and private sectors. This Article focuses entirely on the private sector. Privacy advocates have been remarkably *unconvincing* when arguing that purely private sector reductions in informational privacy pose a serious danger. Their arguments typically consist of examples in which the loss of control over personal information causes harms that—other things being equal—virtually anyone would find unacceptable. "Other things" are rarely "equal." Reducing informational privacy often advances other important goals, and many readily surrender privacy for even relatively minor benefits. The privacy advocates insist we are wrong. They see us as trapped in a "balancing wrongly" crisis in which we systematically undervalue the informational privacy we willingly surrender. They may well be correct; but this Article does not pursue that possibility.

The Article claims that there is *another* privacy crisis, one that has gone largely unnoticed. Technological advances have not only created critical balancing questions; they have also rendered largely useless the scales on which we balance the competing interests. We have lost the customary balancing mechanism at the very time we most need it. This loss is the other privacy crisis. The lost balancing mechanism consists of informational norms—norms that constrain the collection use, and distribution of personal information. The norm-created constraints not only balance competing interests; they also, by virtue of creating that balance, constitute an essential means to achieving a variety of important ends. The technological increase in our ability to process information has undermined the norm-created balance and thereby deprived us of that indispensable means. The solution is to create new informational norms. Legal regulation will not be particularly effective in this regard; however, the very information processing technology that undermined traditional informational norms may provide the means to creating new norms.

Table of Contents

I. Informational Norms Protect Informational Privacy

A. Norms Defined

1. Legally-generated norms
2. Value-justified norms
3. Two claims

B. The Empirical Claim: Role-Specific Informational Norms Exist

C. Shared-Conception, Role-Specific Informational Norms Protect Informational Privacy—If They Are Value-Justified

II. The Normative Claim: Value-Justified, Role-Specific Informational Norms Should Exist

A. We Value Self-Realization

B. Self-Realization Requires Freedom

C. Freedom Requires Informational Privacy

1. Chilling effects
2. Coercive effects

D. Value-Justified Norms Provide The Desirable Degree Of Privacy

III. Norms Undermined

A. The Health Industry Example

1. Greater effectiveness
2. The companies still conform to a norm
3. The norm is no longer value-justified

B. Generalizing from the Health Insurance Example

1. ChoicePoint

2. Google

3. Direct marketing

C. Collaborate Or Resist?

IV. Can We Regain Control Through the Law? Two Dim Prospects

A. Requiring Consent Will Not Return Control

B. Legally-Generated Norms Will Not Return Control

C. A Solution Through Technology?

V. Facebook's Terms of Service Controversy: A Sign of Hope?

The Other Privacy Crisis:
Informational Privacy, Undermined Norms, and Loss of Control

Richard Warner*

Informational privacy is a matter of control.¹ 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.”² We enjoyed a significant degree of control over our personal information into the mid-twentieth century; that control has vanished.³ Dramatic advances in information processing technology put considerable power in the hands of others to determine when our personal information is collected, and how it is

* Professor of Law, Chicago-Kent College of Law; Visiting Foreign Professor, Law Faculty, University of Gdańsk, Poland. I thank Margaret Stewart (once again) for her insightful skepticism, and Robert Sloan (Head of Computer Science, University of Illinois, Chicago), with whom I have discussed informational privacy for the last two years.

¹ James Rule emphasizes this point. JAMES B. RULE, *PRIVACY IN PERIL* 3 (2007) (“Let me define privacy as the exercise of an authentic option to withhold information on oneself”). Michael Froomkin also stresses the point. Michael Froomkin, *The Death of Privacy*, 52 *STAN. L. REV.* 1461, 1462 (2000) (“In this article, I will use ‘informational privacy’ as shorthand for the ability to control the acquisition or release of information about oneself”). Daniel Solove reviews various definitions of informational privacy in terms of control over personal information. DANIEL J. SOLOVE, *UNDERSTANDING PRIVACY* 24 – 29 (2008). Solove treats the various definitions, not as definitions of *informational* privacy, but as definitions of a *general* notion of privacy applicable, not only to concerns about personal information, but also to traditional search and seizure questions, issues of decisional freedom (as in the right of a pregnant woman to opt for an abortion) and a host of other concerns. He contends that there is no single, informative definition of such an expansive concept. *Id.* at 39. I am concerned exclusively with informational privacy and not, as Solove rightly points out, an elusive general concept of “privacy.”

² ALAN WESTIN, *PRIVACY AND FREEDOM* 7 (1967).

³ The erosion of control began in the 1950’s with the development of credit reporting practices. RULE, *supra* note 1, at 99. For a fuller discussion of the history of the loss of control over personal information, see Priscilla M. Regan, *The United States*, in *GLOBAL PRIVACY PROTECTION: THE FIRST GENERATION* 50 (James B. Rule & Graham Greenleaf (eds.) 2008) (also suggesting the breakdown began in the 1950’s).

used and distributed.⁴ As Lawrence Friedman observes, “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.”⁵

Privacy advocates sound the alarm—in regard to both the governmental and private sectors.⁶ I focus entirely on the latter. I do not mean to minimize governmental concerns; however, a strong chorus of concern has forcefully portrayed the increasingly worrisome governmental threat to informational privacy.⁷ The advocates have, however, been remarkably *unconvincing* when arguing that purely private sector reductions in informational privacy pose a serious danger. Their arguments typically

⁴ James B. Rule, *Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions*, 54 UNIV. OF TORONTO LAW J. 183, 183 (2004) (noting that “it has become increasingly rare to deal with any governmental or private-sector organization without generating and relying upon a database of personal information”).

⁵ LAWRENCE M. FRIEDMAN, *GUARDING LIFE’S DARK SECRETS: LEGAL AND SOCIAL CONTROLS OVER REPUTATION, PROPRIETY, AND PRIVACY* 171 (2007).

⁶ Three recent books illustrate tenor of the privacy advocate literature. DANIEL J. SOLOVE, *UNDERSTANDING PRIVACY* (2008) 4 (“[T]he profound proliferation of new information technologies during the twentieth century . . . made privacy erupt into a frontline issue around the world”); JON MILLS, *PRIVACY: THE LOST RIGHT* xi (2008) (comparing contemporary society to the society of *The Brave New World* and insisting that “intrusion is commonplace,” and that “[e]very single individual is at risk”); RULE, *supra* note 1, at 200 (warning of the “endless erosion of privacy” and seeking a solution).

⁷ Solove inveighs against governmental invasions of privacy. SOLOVE, *supra* note 6. Mills is particularly governed with the governmental sector. MILLS, *supra* note 6. Governmental concerns occupy an important place in Rule’s work as well. RULE, *supra* note 6. Other recent examples are Jed Rubenfeld, *The End Of Privacy*, 61 STAN. L. REV. 101 (2008), and Froomkin, note 1. In general, political philosophy, for the last three hundred years, has emphasized the critical role of privacy in limiting the power of the state, and, although we 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.

consist of examples in which the loss of control over personal information causes harms that—other things being equal—virtually anyone would find unacceptable.⁸ The difficulty is that “other things” are rarely “equal.” Reducing informational privacy often advances other important goals,⁹ and, as the staunch privacy advocate Daniel Solove concedes, “abstract incantations of the importance of ‘privacy’ do not fare well when pitted against more concretely stated countervailing interests.”¹⁰ Indeed, most of us readily agree to trade informational privacy for relatively small benefits.¹¹ Privacy advocates insist that we are wrong. They see us as trapped in a “balancing wrongly” crisis in which we systematically undervalue the

⁸ See James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L. J. 1151, 1153 (2004) (noting that “the typical privacy article rests its case precisely on an appeal to its reader’s intuitions and anxieties about the evils of privacy violations”). The committed privacy advocate, James Rule, laments that privacy advocates too often rely on “gut reactions.” RULE, *supra* note 1, at 183. He notes that “[w]e cannot hope to answer [complex balancing questions] until we have a way of ascribing weights to the things being balanced. And, that is exactly where the parties to privacy debates are most dramatically at odds.” *Id.*

⁹ Perhaps the two most frequently cited countervailing interests are economic efficiency and security. Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 CHICAGO L. REV. 75, 86 (2008) (“policy decisions frequently counterpose privacy against two other powerful values: efficiency and security”).

¹⁰ Daniel J. Solove, *A Taxonomy of Privacy*, U. OF PENN. L. REV. 477, 478 (2006).

¹¹ Surveys and studies of Internet users, for example, show that, although “Internet users claim to highly value their privacy; still, they are willing to trade off personal information for small rewards, or are unwilling to change their behavior when privacy threats arise.” Jens Grossklags & Alessandro Acquisti, *When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information* 6, available at <http://www.cl.cam.ac.uk/~rja14/econsec.html>. See also Luc Wathieu & Allan Friedman, *An Empirical Approach to Understanding Privacy Valuation* (noting that consumers trade privacy for economic gain and proposing a model of the tradeoff), available at <http://www.cl.cam.ac.uk/~rja14/econsec.html>; and J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. OF CHI. L. REV. 109 (2008).

informational privacy we willingly surrender.¹² They may well be correct;¹³ I will not pursue that possibility, however.

My claim is that there is *another* privacy crisis, one that has gone largely unnoticed. Technological advances have not only created critical balancing questions; they have also rendered largely useless the scales on which we balance the competing interests. We have lost the customary balancing mechanism at the very time we most need it. This loss is the other privacy crisis. The lost balancing mechanism consists of informational norms—norms that constrain the collection use, and distribution of personal information.¹⁴ The norm-created constraints not only balance competing interests; by virtue of implementing that balance, they also constitute an essential means to achieving a variety of important ends. The technological increase in our ability to process information has undermined the norm-created balance and thereby deprived us of that indispensable means. The solution is to create new norms. Legal regulation will, I argue, not be particularly effective in this regard; however, the very information processing

¹² James Rule sees privacy as constantly eroding as “privacy-protecting Davids . . . mobilize thinly stretched resources against organizational Goliaths, . . . [E]ven the most notable victories appear as provisional non-defeats, subject to rude reversal down the road.” RULE, *supra* note 1, at 144.

¹³ Individual decisions about informational privacy may yield highly objectionable consequences even if each decision seems clearly justified at the time. Hörder V. Haraldsson, Harald U. Sverdrup, Salim Belyazid, Kenneth M. Persson, Johan Holmqvist, *The Tyranny of Small Steps—An Archetypal Behavior in Resource Management*, http://www.systemdynamics.org/conferences/2004/SDS_2004/PAPERS/500HARAL.pdf (noting that a sequence of seemingly well-justified individual decisions can yield highly undesirable consequences).

¹⁴ See *infra* Section I.

technology that undermined traditional informational norms may provide the means to creating new norms.

Section I defines the relevant notion of a norm and introduces the key notion of a value-justified norm (roughly, a norm is value-justified if it is justifiable in light of one's values). The section introduces the concept of *informational* norms and emphasizes that they are *role-specific*; that is: the constraints on the processing of the information are determined by the social roles of the individuals to whom the norm applies. Your pharmacist may, for example, inquire about drugs you are taking in order to prevent undesirable drug interactions, but may not (unless he or she is your friend, or plays some other appropriate role) inquire about whether you are happy in your marriage. Section I makes three key empirical claims. First, value-justified, role-specific informational norms govern a wide range of business interactions. Second, the norms balance informational privacy against competing concerns. Third, by virtue of striking this balance, the norms guarantee a degree of informational privacy.

Section II turns from the empirical claim that value-justified, role-specific informational norms exist to the normative claim that they should. The argument for the latter claim runs in outline as follows: (1) We value self-realization; (2) self-realization requires freedom; (3) freedom requires informational privacy; (4) *only* value-justified, role-specific informational norms provide the requisite degree of informational privacy; hence (5) such norms should exist. Section II defends the first three premises and begins the argument for the fourth by defending the weaker claim that value-

justified role-specific informational norms do in fact provide the requisite degree of informational privacy. I defer to Section IV the argument that *only* such norms can do so.

Section III contends that the technological-driven increase in our ability to process information by ensuring that a wide range of role-specific information norms are no longer value-justified. The consequence is that we have lost the norm-provided control over personal information. Section IV illustrates and argues for these claims by considering the health insurance industry, ChoicePoint, Google, and the practice of direct marketing. The section concludes by arguing that we should try to regain the control we have lost.

Section IV contends that the *only* way we can regain adequate control is by reestablishing value-justified role-specific informational norms, and it argues that the ability of legal regulation to do so is quite limited. Section V suggests that the very technological advances that deprive informational norms of value-justification may also create the conditions under which new value-justified informational norms will emerge.

I. Informational Norms Protect Informational Privacy

Role-specific informational norms balance informational privacy against competing concerns and thereby ensure a degree of control over personal information. The foregoing claim raises four questions. What is a norm? Why think role-specific informational norms exist? How do such norms balance competing concerns? And, how does that norm-created balance

ensure the control over personal information? I take up each question in turn.

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, other things being equal, each group member *ought* to act in accord with that regularity.¹⁵ The “ought” may be purely prudential, justified by a fear of legal and non-legal sanctions; or, it may be justified in light of the values the person accepts. As an example of a norm, imagine you are about to enter an elevator in which several others are already present. Where do you stand? The norm is (roughly) that you should, other things being equal, maximize the distance between you and the person nearest you. Additional examples: you are making a comment during a roundtable discussion. How long should you talk before it is someone else’s turn? The norm is that you should talk only as long as is appropriate (where you and the other participants share roughly the same concept of appropriateness). In a narrow corridor, a lawyer with an oversized briefcase encounters a parent with a baby in a stroller walking in the other direction; in order for one to pass, the other must make room; the norm is that (in most cases at least) the lawyer should make room for the parent.

¹⁵ See Michael Hector & Karl-Dieter Opp, *What Have We Learned About the Emergence of Social Norms?*, in *SOCIAL NORMS* 394, 403 (Michael Hector & Karl-Dieter Opp (eds.), 2001). 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 here.

Two further preliminary points are in order, both of which will be important later. First, legal regulation can account for the fact that we think we ought to conform to a norm. Second, norms divide into two types: those that are, and those that are not, value-justified.

1. Legally-generated norms

The key point is that legal regulation can be the *sole* explanation of why one thinks one ought to conform to a norm. Consider the contractual norm, "Sellers may (within broad limits) disclaim consequential damages." It may seem at first sight that this cannot be a norm. A norm is a sanction-supported regularity *where the regularity exists in part because people think they ought to conform to it*. "Sellers may disclaim consequential damages" does express a sanction-supported regularity: sellers regularly disclaim consequential damages, and courts regularly enforce the disclaimers. Now, *sellers* think they ought to conform to the regularity because such disclaimers reduce their legal liability and make it more predictable. But how can *buyers* think they ought to conform? Most of them do not even know what consequential damages are, let alone realize that they may be disclaimed; so, how can it be true that buyers think they ought to accept and abide by the disclaimers? They think so in this sense: if they became aware of the provision, they would think they ought to conform to it. They would think this because, as empirical studies confirm, people think that they ought

to abide by the law (other things being equal).¹⁶ Since the disclaimer of consequential damages is a legally enforceable provision, buyers who become aware of it will (for the most part) think they ought conform to it.

The distinctive feature of the “disclaim consequential damages” norm is that, for a significantly large group, a commitment to obey the law is the *sole* reason they can be correctly described as thinking they should conform. Call such norms *legally-generated norms*. Legally-generated norms occupy one extreme of a continuum.¹⁷ The other end is home to norms like the etiquette norm, “Do not eat meat with the salad fork.” Those who conform to this norm do not so because they think that their failure to conform would violate a law. Many norms occupy a middle position—for example, the norm, “Drive your car with reasonable care for the safety of others.” People conform in part because unreasonable driving creates potential legal liability, but they would also take steps to avoid exposing others to unreasonable dangers even if the legal liability did not exist (although they might not take such steps as frequently, consistently, and attentively). In general, norms gravitate toward one end or the other on this continuum depending on the extent to which legal or non-legal motivations dominate in the explanation of conformity to the norm.

¹⁶ TOM TYLER, *WHY PEOPLE OBEY THE LAW* 64 (1990) (arguing, based on empirical studies, that people think they ought to obey the law). See also MARK KELMAN, *A GUIDE TO CRITICAL LEGAL STUDIES* 263 - 68 (1987), and David Kairys, *Introduction to THE POLITICS OF LAW* 7 (David Kairys, ed., 1990).

¹⁷ One could define a concept of a norm that did not count such regularities as norms. It might, however, be quite difficult to define just how large a group has to be motivated solely by legally incentives to prevent a regularity from qualifying as a norm. In any case, the notion of a norm relevant here is one that recognizes legally-generated norms.

2. Value-justified norms

Norms divide into those that are, and those that are not, *value-justified*. To see the distinction, consider first 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.” The crucial point to emphasize is that you *could* justify it; you could, that is, if you reflected on the norm *under appropriate ideal conditions* (including having sufficient time, information, lack of bias, and so on). You could justify the balance the norm strikes between the value you place on not feeling crowded, and the value you place on being able to use the elevator when it arrives.¹⁸ In general, with regard to many (but, importantly, not all) norms, we would, given ideal conditions for reflection, regard conformity to the norm as justified in light of our values.¹⁹ Call such norms *value-justified*. Not all norms are value-justified. Imagine a norm which requires selecting men instead of women for police officers. Assume that, even though most unreflectively abide by the norm, they would *not* regard the norm as justified if they were to reflect on it adequately in an unbiased way. It is worth pointing out in passing that legally-generated norms are

¹⁸ Justification comes in degrees, of course: our values may *more or less* justify a norm. I suppress this complication for the sake of simplicity.

¹⁹ The appeal to reasoning under ideal conditions to justify normative conclusions begins (at least) with Aristotle. ARISTOTLE, *NICOMACHEAN ETHICS* (Terrence Irwin, trans., 1985) (2d ed.). For a modern exposition and defense of this approach, see STEPHEN DARWALL, *IMPARTIAL REASON* (1983).

particularly susceptible to lack of value-justification. If courts or legislatures ignore or misinterpret the relevant community values, they may create a legally-generated norm which is not value-justified. Unlike a value-justified norm, such a norm would not reflect our implicit evaluative judgments.

3. Two claims

I advance two claims about value-justified informational norms, one empirical and one normative. The empirical claim is that, for a significant range of important types of interaction, the transfer of information is (or, was in the past at least) in fact governed by value-justified informational norms. The normative claim is that value-justified informational norms should exist across a wide range of transactions whether they do or not.

B. The Empirical Claim: Role-Specific Informational Norms Exist

The communications theorist Helen Nissenbaum defends a sweeping version of the empirical claim; she contends that “there are no arenas of life *not* governed by *norms of information flow*, no information or spheres of life for which ‘anything goes.’”²⁰ A more cautious formulation is sufficient for my purposes: informational norms govern a wide range of important interactions. The empirical claim includes the claim that the norms are *role-specific*, that is: the social roles of the individuals or entities to whom the

²⁰ Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 120 - 121 (2004) [hereinafter, Nissenbaum, *Contextual Integrity*] (calling the claim a “central tenet”). Michael Zimmer also endorses the broad claim. 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 - 118 (2008).

norms apply determine the constraints the norms impose. Nissenbaum emphasizes this point:

Generally, these norms circumscribe the type or nature of information about various individuals that, within a given context, is allowable, expected, or even demanded to be revealed. In medical contexts, it is appropriate to share details of our physical condition or, more specifically, the patient shares information about his or her physical condition with the physician but not vice versa; among friends we may pour over romantic entanglements (our own and those of others); to the bank or our creditors, we reveal financial information; with our professors, we discuss our own grades; at work, it is appropriate to discuss work-related goals and the details and quality of performance.²¹

In general, role-specific informational norms are instances of the following pattern: a business may collect, analyze, and distribute information as is appropriate given the social roles of the business and its customers.²² I will not argue for the empirical claim; I rely on the work Nissenbaum and others.²³ One further observation about the empirical claim is in order, however.

²¹ Nissenbaum, *Contextual Integrity*, *supra* note 20, at 120 - 121.

²² Michael Zimmer argues that “[w]ithin each context, the relevant *agents*, *types of information*, and *transmissions principles* combine to shape the governing informational norms.” Zimmer, *supra* note 20, at 115 (citing A. Barth, A. Datta, J.C. Mitchell, and H. Nissenbaum, *Privacy and Contextual Integrity: Framework and Applications*, PROCEEDINGS OF THE IEEE SYMPOSIUM ON SECURITY AND PRIVACY, MAY 2006, <http://www.nyu.edu/projects/nissenbaum>). For simplicity, I have combined into a single concept of “appropriateness” Zimmer’s appeal to agents, types of information, and transmissions principles.

²³ Nissenbaum, *Contextual Integrity* *supra* note 20 cites the following sources in support of the empirical claim: PIERRE BOURDIEU & L OIC J.D. W ACQUANT, AN INVITATION TO REFLEXIVE SOCIOLOGY 95–115 (1992) (discussing Bourdieu’s concept of fields); *id.* at 97 (“In highly differentiated societies, the social cosmos is made up of a number of such relatively autonomous social microcosms For instance, the artistic field, or the religious field, or the economic field all follow specific logics”); MICHAEL PHILLIPS, BETWEEN UNIVERSALISM AND SKEPTICISM: ETHICS AS SOCIAL ARTIFACT (1994); MICHAEL WALZER, SPHERES OF JUSTICE: A DEFENSE OF PLURALISM AND EQUALITY (1983); Roger Friedland & Robert R. Alford, *Bringing Society Back In: Symbolic Practices, and Institutional Contradictions*, in THE NEW INSTITUTIONALISM IN ORGANIZATIONAL

The theorists typically assume that all parties to an informational norm agree on what counts as appropriate.²⁴ The assumption is not required. The norm in one's family may be that it is appropriate to share the intimate details of one's marriage with one's siblings; one may conform in order to preserve congenial sibling relationships even though one regards as extremely inappropriate to divulge marital details. The assumption is not only not required, it is also (for the most part) false. It holds only for (a sufficiently distant) past. In the present, the range of information businesses now regard it as appropriate to collect, analyze, and distribute often extends far beyond what consumers would agree is appropriate. I will nonetheless temporarily assume that all parties to an informational norm agree on what counts as appropriate. The point is to begin by characterizing what (to a considerably extent) we no longer have: role-specific informational norms incorporating a shared conception of appropriateness. Only such norms

ANALYSIS 232, 253 (Walter W. Powell & Paul J. DiMaggio (eds.), 1991) (noting that "society is composed of multiple institutional logics"); Jeroen van den Hoven, *Privacy and the Varieties of Informational Wrongdoing*, in READINGS IN CYBER ETHICS 430 (Richard A. Spinello & Herman T. Tavani (eds.), 2001). In addition these sources cited by Nissenbaum, see Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW AND PHILOSOPHY 559-596, (1998); James Rachels, *Why Privacy Is Important*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 290, 294 (Ferdinand David Schoeman ed., 1984); Robert Post, *Social Foundations of Privacy: Community and the Self in the Common Law Tort*, 77 CAL. L. REV. 957 (1989); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject As Object*, 52 STAN. L. REV. 1373 (2000); and, Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999).

²⁴ The claim is generally both left implicit and taken for granted. Consider, for example, James Rachels observation that "the 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 it is appropriate for them to have." James Rachels, *Why Privacy Is Important*, 4 PHILOSOPHY AND PUBLIC AFFAIRS 323, 328 (1975). It is clear from the context that Rachel thinks of the conception of appropriateness as one the parties share, and know they share.

balance informational privacy against competing concerns in a way that ensures adequate control over personal information. Understanding how they do so provides the background for understanding what we have lost through the technology-driven undermining of informational norms.

An example is helpful. Consider a typical consumer purchase. Vicky enters a wine store. Assume the store conforms to the following norm: collect information only for purposes appropriately related to the store's role as a seller of wine, where Vicky and the store share roughly the same conception of appropriateness. That conception permits the store to process certain information—and for good reason. Processing of the information benefits both businesses and consumers. Collecting and processing the information increases efficiency;²⁵ increases the relevant information businesses send consumers while decreasing the irrelevant;²⁶ decreases fraud;²⁷ and generally allows both the businesses and consumers to reap whatever other benefits may be available in the circumstances from the businesses ability to "predicate dealings with [consumers] on the cumulative . . . record of past acquaintance with them."²⁸

²⁵ See Jerry Kang, *Information Privacy In Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1216-17 (1998).

²⁶ See *Id.* at 1218

²⁷ See *Id.* at 1218 -19

²⁸ RULE, *supra* note 1, at 8. Rule notes that

Throughout life, we constantly predicate dealings with those around us on the cumulative—if unsystematic—record of past acquaintance with them. As the jurist Richard Posner would remind us, such impressions make it possible to adjust our actions to those who appear as reliable or undependable, restrained or impulsive, honest or devious. It is very difficult to imagine how

The wine store will almost certainly avail itself of information processing the norm permits. The reason: information is power. The more relevant information one has in regard to an end, the more effective one is, other things being equal, in achieving it. "Other things" may not be "equal," of course. For example, information overload decreases effectiveness and relevant but incomplete information can create a misleading picture. Such exceptions aside, however, more relevant information means more power. Relevant information empowers businesses by enabling them to discriminate among types of consumers in order to treat the different types in ways most likely to yield the results the business desires. This is why

the logic . . . of surveillance systems is to grow. Given that the efficient pursuit of discrimination among persons is their *raison d'être*, we should hardly be surprised that they tend to grow in *depth*—that is, in the total amount of information collected on the average individual with whom they deal. But surveillance systems also tend to grow *laterally*—to broaden the *variety* of sources of personal data they rely on in making those discriminations, especially through symbiotic exchanges with similar systems.²⁹

Market competition reinforces this tendency. To remain competitive, companies increase their customer surveillance in response to increases by competitors. Indeed, as a recent Privacy International report notes,

We 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

we could go about everyday life without sufficient "invasion of privacy" to afford some basis for such judgments.

Id. at 8 – 9.

²⁹ RULE, *supra* note 1, at 18.

some cases to find new and more innovative ways to become even more surveillance-intensive.³⁰

Shared-conception, role-specific informational norms limit the tendency of surveillance to become ever more intensive. Consider the collection of information first. Both customers and wine retailers would, for example, agree (even at the present time) that it is not appropriate for a wine retailer to collect information about a customer's liver function; the kind of clothes the customer wears; or whether the customer is in the store with his or her spouse or another companion. Similar remarks hold for the analysis and distribution of information. *Analysis*: imagine that researchers have discovered correlations between patterns of wine selection and sexual orientation (lest this seem too fanciful, consider the direct marketing "discovery in recent presidential campaign that buyers of a particular car-washing product proved enormously susceptible to Republican campaign appeals"³¹). Most consumers and wine retailers find it inappropriate for the retailer to analyze buying patterns to determine customers' sexual orientation. *Distribution*: suppose Vicky consults the wine store on wine selections for a dinner party he is giving; Vicky discusses their wine preferences of his guests, identifying some by name. It would be inappropriate for the store to publish the details about the party on its web site.

³⁰ Privacy International, *A Race to the Bottom—Privacy Ranking of Internet Service Companies*, <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-553961>.

³¹ RULE, *supra* note 1, at 104.

As the examples illustrate, the notion of appropriateness in a shared-conception, role-specific informational norm balances informational privacy against competing concerns. The next—and essential—point is that, by virtue of creating this balance, the norms also ensure a degree of control over personal information.

C. Shared-Conception, Role-Specific Informational Norms Protect Informational Privacy—If They Are Value-Justified

It may seem obvious that shared-conception, role-specific norms ensure a degree of control over personal information. Just imagine Vicky entering the wine store. She knows that the norm-conforming store will only process information in ways *he* regards as appropriate. Is that not enough to see her as having control over his personal information? The answer is “no.” Shared-conception role-specific informational norms provide genuine control over personal information *only when they are value-justified*. The following example reveals why.

Imagine businesses and consumers adhere to a role-specific informational norm under a shared conception of appropriateness; however, suppose also that the norm is *not* value-justified. Consumers nonetheless sincerely believe that (by and large) business process information only in ways that the customers see as appropriate; however, they believe this only because they have not adequately reflected on the business practices. If they did so, they would reject the balance the norm strikes between informational privacy and competing concerns as unjustifiably biased in favor

of the businesses. They would conclude that conformity to the norm requires them to reveal information they would prefer to withhold. Thus, conformity to the norm actually *deprives* them of effective control.

To summarize: to the extent shared-conception, role-specific norms are value-justified, they protect informational privacy by providing a degree of control over personal information. Section III argues that advances in information processing technology have resulted in norms that are no longer value-justified, and hence that we have lost the control that such norms ensure. How should we respond? Section IV concludes that we should try to reestablish value-justified, shared-conception, role-specific norms. That conclusion rests on the normative claim that value-justified role-specific informational norms should exist. The next section begins the defense of that claim.

II. The Normative Claim: Value-Justified, Role-Specific Informational Norms Should Exist

The normative claim is that value-justified role-specific informational norms exist across a wide range of transactions. The argument for the claim in outline: (1) We value self-realization; (2) self-realization requires freedom; (3) freedom requires informational privacy; (4) *only* value-justified shared-conception role-specific informational norms provide the requisite degree of informational privacy; hence (5) such norms should exist.

Before beginning the argument, the focus on self-realization requires some comment. The first three steps offer the following answer to the question of why we value privacy: we value it primarily as an essential

means to self-realization.³² This emphasis on self-realization may appear to overlook the fact that privacy advocates offer surprisingly diverse answers to the question of why privacy matters. As Daniel Solove notes, “theorists have proclaimed the value of privacy to be protecting intimacy, friendship, individuality, human relationships, autonomy, freedom, self-development, creativity, independence, imagination, counterculture, eccentricity, creativity, thought, democracy, reputation, and psychological well-being.”³³ I by no means deny the diversity; however, the theme of self-realization unifies the otherwise disparate activities, attitudes, and relationships privacy advocates identify as served by informational privacy. I am not suggesting that we value these activities, attitudes, and relationships solely for their contribution to self-realization. We also value them for their own sake. It is just that their role in self-realization is primarily what matters here.

A. We Value Self-Realization

³² Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 300, 314 (Ferdinand David Schoeman ed. 1984) (“The right to privacy protects the individual’s interest in becoming, being, and remaining a person”). Daniel Solove reviews the theories that see privacy as of value because of its relation to personhood in SOLOVE, *supra* note 6, at 29 - 34. Solove criticizes these theories for “failing to articulate an adequate definition of personhood.” *Id.*, at 31. He also finds the theories both over- and under-inclusive. *Id.* at 31 - 32. The connection I draw between self-realization and informational privacy is immune to the first criticism as it rests on uncontroversial insights that have long formed a part of political philosophy. See *infra* text accompanying notes 35 -38. The connection I draw is also immune to the second criticism. That criticism is leveled at attempts to explain the scope of certain privacy laws entirely or primarily by appeal to considerations about personhood. I make no such attempt.

³³ SOLOVE, *supra* note 6, at 98.

The first premise in the argument for the normative claim is that we value self-realization. I not will argue for this claim by deriving it from something yet even more fundamental; instead, I will describe self-realization in a way that reveals it as something which we do indeed regard as fundamentally important.

William James concisely captures the relevant concept of self-realization. "I am," James writes,

often confronted by the necessity of standing by one of my . . . selves and relinquishing the rest. Not that I would not, if I could, be both handsome and fat and well dressed, and a great athlete, and make a million a year, be a wit, a *bon vivant*, and a lady killer, as well as a philosopher, and a philanthropist, statesman, warrior, and African explorer, as well as a "tone poet" and saint. But the thing is simply impossible. The millionaire's work would run counter to the saint's; the *bon vivant* and the philanthropist would trip each other; the philosopher and the lady killer could not well keep house in the same tenement of clay. Such characters may at the outset of life be alike *possible* to a man. But to make anyone of them actual, the rest must be more or less suppressed. So the seeker of his truest, strongest, deepest self must review the list carefully, and pick out the one on which to stake his salvation. All other selves thereupon become unreal, but the fortunes of this self are real, its failures are real failures, its triumphs real triumphs, carrying shame and gladness with them.³⁴

You realize your self—make yourself the person you are--by what you "stand by," by the commitments you strive to realize. Self-realization in this sense figures importantly in moral and political philosophy from Hegel³⁵ and Mill³⁶

³⁴ WILLIAM JAMES, 1 THE PRINCIPLES OF PSYCHOLOGY 309 - 10 (1980).

³⁵ See generally GEORG W. F. HEGEL, THE PHILOSOPHY OF RIGHT (T. M. Knox, trans., 1967).

³⁶ See generally JOHN STUART MILL, ON LIBERTY (David Bromwich & George Kateb eds., Yale University Press 2003) (1859).

to Rawls³⁷ and Raz,³⁸ and I assume that it is clear that we not only value self-realization so for its own sake, but that we also regard it as of great importance. James's picture of self-realization requires one emendation, however.

James exaggerates when he suggests that "the seeker of his truest, strongest, deepest self must review the list carefully, and pick out the one on which to stake his salvation."³⁹ Our identities are composed of multiple roles: spouse, parent, professor, friend, applicant for insurance, heir to this or that religious tradition, product of southern Californian culture, and so on. In general,

[w]e are none of us defined by membership in a single community or form of moral life. We are . . . heirs of many distinct, sometimes conflicting, intellectual and moral traditions. . . . The complexity and contradictions of our cultural inheritance give to our identities an aspect of complexity and even of plurality which is not accidental, but (if we may use such a term) essential to them. For us . . . the power to conceive of ourselves in different ways, to harbour dissonant projects and perspectives, to inform our thoughts and lives with divergent categories and concepts, is integral to our identity as reflective beings.⁴⁰

We spread out along a continuum: the harmonious occupy one extreme; the conflict-ridden, the other. Most of us most likely occupy a position somewhere in the middle.

³⁷ See generally JOHN RAWLS, *A THEORY OF JUSTICE* (1971); JOHN RAWLS, *POLITICAL LIBERALISM* (1993).

³⁸ See generally JOSEPH RAZ, *THE MORALITY OF FREEDOM* (1986).

³⁹ JAMES, *supra* note 34, at 310.

⁴⁰ JOHN GRAY, *POST-LIBERALISM: STUDIES IN POLITICAL THOUGHT* 262 - 63 (1993).

Our “middle-position” commitments typically include commitments to the activities, attitudes, and relationships privacy advocates identify when explaining why we value privacy. Consider Solove’s list: “intimacy, friendship, individuality, human relationships, self-development, creativity, independence, imagination, counterculture, eccentricity, creativity, thought, democracy, reputation, and psychological well-being.”⁴¹ We typically seek self-realization through intimacy, friendship, and human relationships; our self-realizing activities are instances of individuality, self-development, and independence, and can be instances of thought, creativity, eccentricity, counterculture, and democratic participation; finally, our psychological well-being depends in part on achieving our self-realizing goals.

B. Self-Realization Requires Freedom

The second premise in the argument for the normative claim is that self-realization requires freedom. An essential preliminary is clarifying the relevant notion of freedom. For our purposes, freedom is best conceived as an ideal: the ideally free person chooses his or her actions on the basis of principles adopted as the result of critical reflection. This will suffice for our purposes; controversy erupts as soon as one tries to clarify key terms in this definition, but there is no need for further clarification in this Article.

Self-realization requires freedom this sense. This is not to deny that many of our commitments are partly—perhaps largely—the product of upbringing, education, culture, and myriad other influences. Self-realization

⁴¹ SOLOVE, *supra* note 6, at 98.

nonetheless requires approximating the ideal of freedom to *some* degree. Imagine that the total mind control of some future Orwellian government denies you any choice in your commitments; not a single one is what you would choose if the mind control were absent. You are not realizing *your* self, you are realizing the government's vision of who you should be. We do not realize *our* selves unless we approximate to some considerable degree the ideal of the free individual. In short: self-realization requires some degree of freedom.

C. Freedom Requires Informational Privacy

The degree of freedom adequate for self-realization requires a corresponding degree of informational privacy. Reductions in informational privacy can reduce freedom by creating chilling or coercive effects. Chilling effects prevent you from acting in ways you would otherwise choose; coercive effects compel you to act in ways you would otherwise not choose.⁴²

1. Chilling Effects

*McVeigh v. Cohen*⁴³ illustrates the chilling effect. Timothy McVeigh, a decorated seventeen-year gay veteran, sought to enjoin the Navy from discharging him for a violation of the "Don't Ask, Don't Tell" policy. Up to that time, McVeigh had complied with the military's "Don't Ask, Don't Tell"

⁴² Jerry Kang, *Information Privacy In Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1215 - 16 (1998).

⁴³ 983 F. Supp. 215 (D.D.C. 1998).

policy and therefore—in an illustration of the chilling effect—did not say or do things he would otherwise have said and done. In general, as Jerry Kang emphasizes, lack of informational privacy

chills individuals from engaging in unpopular or out-of-the-mainstream behavior. While uniform obedience to criminal and tort laws may deserve praise, not criticism, excessive inhibition—not only of illegal activity but also of legal, but unpopular, activity—can corrode private experimentation, deliberation, and reflection. The end result may be bland, unoriginal thinking or excessive conformity to unwarranted social norms. Worse, the self-repression of activity and communication could undermine the self-critical capacities of a polity. This is why totalitarian regimes have maligned a desire for privacy as deviant, in part to sap an individual's ability to question the status quo and to experiment with alternate conceptions of the good life.⁴⁴

2. Coercive effects

McVeigh v. Cohen also illustrates the coercive effect. McVeigh's alleged violation of the "Don't Ask, Don't Tell" policy occurred when McVeigh accidentally responded to a toy drive on his ship with an email account which bore the alias "boysrch." The person conducting the toy drive searched the AOL member profiles and discovered that the account was owned by a person named "Tim," who was in the military, lived in Hawaii, and identified himself as gay. At her request, AOL identified the owner of the account as Tim McVeigh, and the litigation ensued. After the court enjoined the discharge, McVeigh commented:

⁴⁴ Kang, *supra* note 42, at 1216 - 1217. See also RULE, *supra* note 1, at 186 - 188; Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY, 223, 241 (Ferdinand David Schoeman ed., 1984) ("We act differently if we believe we are being observed. If we can never be sure whether or not we are being watched and listened to, all our actions will be altered and our very character will change"); Rainer Böhme, *Conformity or Diversity: Social Implications of Transparency in Personal Data Processing*, at <http://weis2008.econinfosec.org/papers/Bohme.pdf> (reporting empirical findings suggesting that others knowledge of personal information breeds conformity).

I'm very glad to be able to stay in the military. Probably a double feeling. One, of course, I'm extremely happy with the judge's ruling and that I get to maintain my military career and continue on. The other side of that is that the Navy is not particularly good losers... I've experienced some of that since my returning to work here, which has been addressed back to Washington, DC. As far as going on with my career, I think that will work out fine. My only concern is with regards to the advancement board. If I was still on board my ship and in charge of my command, I feel I certainly would be advanced on when I come up later this year. But now that my name has become "INTERNATIONAL", it's going to be hard for an advancement board NOT to know who I am, so I have to rely that the board will remain impartial, and I don't know how likely that is. So that will be the first look at whether the Navy, I don't want to say, retaliates. Because it would be hard to prove that this was the reason.. but if, for some reason, they don't recommend me for Master Chief, with the reviews I've received and the commendations I've gotten before this, I most certainly would have probably gotten Master Chief had this not have happened. So time will tell."⁴⁵

McVeigh was compelled to face a number of consequences he would certainly have chosen to avoid, and, to that extent, his freedom was abrogated.

Chilling and coercive effects are unavoidable. This is true even though shared-conception, role-specific informational norms provide some protection against chilling and coercive effects by ensuring a degree of control over personal information.⁴⁶ Indeed, the very norms that provide *some* protection also ensure that chilling and coercive effects will occur. They do so because they only prohibit the processing of *inappropriate* information. The disclosure of information (possible and actual) inevitably creates chilling and coercive effects; indeed, the fact that our identities typically incorporate multiple roles makes us particularly susceptible to them. The expectations

⁴⁵ Carlin Langley, *Up Close and Personal with Sr. Chief Petty Officer Tim Mcveigh of the U.S. Navy*, at <http://www.bearchub4u.com/mcveigh.html>.

⁴⁶ See *supra* Section I.

we create in others when we are in one role (chief petty officer in McVeigh's case) may be deeply disappointed when they find us in what they regard as an incompatible role (gay man); the consequences can range from disapproval and dislike to loss of employment and ostracization.

The fact that informational norms provide only *some* degree of control raises the question of whether they provide *right* degree. Should it be more? Or, less? The answer is that value-justified, shared-conception, role-specific norms provide precisely the degree of control we regard as desirable. The explanation is brief but sufficiently important that it merits its own subsection.

D. Value-Justified Norms Provide The Desirable Degree Of Privacy

Consider the norm in the wine store example: Process information only for purposes appropriately related to the store's role as a seller of wine. The norm balances informational privacy against competing concerns, and it is value-justified only if, on adequate reflection, we would find that balance justified in light of our values. One of the factors we would consider would be the extent to which processing information would create chilling and coercive effects. Seeing the norm as justified in light of our values would include seeing those effects as an acceptable price to pay for the gains from processing information. We would see the norm as implementing tradeoffs we regard as desirable and hence as providing a desirable, even if merely partial, degree of control over personal information. Thus, if a norm is value-

justified, it provides the degree of control over personal information that we regard as desirable.

The next section, Section IV, argues that businesses now often process information in ways that render the relevant norms no longer value-justified. The loss of value-justification entails a loss of control: informational norms that are not value-justified provide only the illusion of control over personal information. Section V argues that the only way we can regain the control businesses have taken from us is by reestablishing shared-conception, role-specific informational norms that are value-justified.

IV. Norms Undermined

Why do businesses now process information in ways that result in loss of value-justification? The answer lies in a point that James Rule emphasizes: increased information processing abilities make businesses far more effective in determining that a specific individual meets whatever standard businesses wish to impose.⁴⁷ An analogy illustrates the connection between increased effectiveness and the loss value-justification. Imagine two elementary school friends adhere to the norm, "Throw as hard as you

⁴⁷ James Rule emphasizes that contemporary information processing systems

share a distinctive and sociologically crucial quality: they not only *collect and record* details of personal information; they are also 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. I call such operations systems of *mass surveillance*. Mass surveillance is the distinctive and consequential feature of our times. Whether carried out by government agencies or private-sector organizations, it shapes the ways we approach major institutions and our treatment at their hands.

RULE, *supra* note 1, at 14.

can,” when they play catch. One of the friends then moves away and to 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. The other answers, “We never meant *that* hard!” There are two possible interpretations of the complaint. The most natural perhaps is that the thrower violated the old norm (interpreted as, “Throw as hard as we—as elementary school children—can”). There is an alternative, however: the thrower adheres to the old norm (interpreted as, “Throw as hard as you can, however hard that may be”), but the norm is no longer value-justified. If the friends were to consider the norm now, in light of their current physical abilities and values, they would not find it justified.

The same two interpretative possibilities arise for businesses which are now, thanks to technological advances, able to “throw harder”—to enforce their policies with greater effectiveness. While it may be difficult to decide between the two alternatives in the case of the friends, the “no longer value-justified” option is clearly the correct in the case of businesses.

A. The Health Insurance Industry

The health insurance industry is an excellent example of how the increased ability to enforce policies renders an informational norm no longer value-justified. There are three steps in the argument. (1) Information processing technologies allow health insurance companies to pursue their policies with much greater effectiveness; (2) the companies nonetheless

conform to the applicable role-specific informational norm; (3) the norm is, however, not value-justified.

1. Greater effectiveness

Health insurance companies provide insurance in exchange for a premium. To remain in business, they must charge premiums appropriate for the risk against which they insure; doing so requires collecting and analyzing information relevant to predicting insurance applicants' morbidity and mortality. In the past, an insurance company's ability to enforce its policies regarding granting insurance and setting premiums was significantly limited by what applicants were willing to disclose about their medical histories. For example, after his wife dies, Jones's doctor prescribes Prozac until Jones' temporary depression passes. 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. In the (sufficiently distant) past, Jones could prevent his new insurance company from finding out the diagnosis and prescription by not noting it on his application for insurance. Something he might well wish to do so as the diagnosis of depression and the prescription of Prozac could lead to the denial of insurance or higher premiums.⁴⁸

⁴⁸ *How a history of mental illness can affect your life insurance costs*, at <http://www.insure.com/articles/lifeinsurance/mental-illness.html> (noting that roughly 90% of applicants in less-than-perfect health were unable to buy individual policies at standard rates, while 37% were rejected outright).

In the present, the health insurance industry use of data aggregation services makes it unlikely that Jones can prevent the company from finding out the facts.⁴⁹ The Medical Information Bureau (MIB) illustrates the point.⁵⁰ MIB is a trade association whose insurance company members share information in the form of MIB records. MIB records consist of codes indicating medical conditions which affect morbidity or mortality. The MIB website 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. The MIB Checking Service protects your company against the cost of early claims and helps you rate and rider policies commensurate with risk.⁵¹

MIB, along with other data collection and aggregation services, enable health insurance companies to "throw harder," to enforce their policies with much greater effectiveness.

⁴⁹ Services specifically targeting the health insurance industry include Milliman IntelliScript, at <http://www.rxhistories.com> ("Insurers use Milliman IntelliScript to gather prescription information in real time and then review an easy-to-read online report"), and the Medical Information Bureau, at <http://www.mib.com>, which collects, analyzes, and distributes information from health insurance applications. For a discussion of prescription reporting, see Martha R. Gore, *Prescription Insurance Tool Evaluates Consumers Prescription Insurance Tool Evaluates Consumers*, SUITE101.COM, Sept. 22, 2008, at http://generalmedicine.suite101.com/article.cfm/health_and_insurance_database_evaluate_consumers. For a discussion of the Medical Information Bureau, see *Milliman Protective Value Study*, at <http://www.mib.com/html/pvs.html>.

⁵⁰ See RENÉE 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).

⁵¹ MIB website, at <http://www.mib.com/html/health.html>.

2. The companies still conform to a norm

Despite the insurance companies' ability to "throw harder," they still conform to the following norm: process information only in ways appropriate to a health insurer. This claim will seem obviously false if one interprets the norm this way: "Companies should process information only in ways—*pre-MIB and other data aggregation ways*—appropriate to a health insurer."⁵²

The difficulty with this interpretation is that norms are dynamic; they change and evolve over time,⁵³ and there is no reason to think that the health insurance company norm is somehow unalterably anchored to the particular technology and practices of a particular time. Indeed, in using MIB and similar services, the companies are just doing what has always qualified as appropriate: collecting information relevant to assessing morbidity and mortality. So why not interpret the norm this way: "Companies should process information only in ways appropriate to a health insurer—where appropriate ways include any legal ways of assessing applicants' morbidity and mortality."

Even this broadly interpreted, however, it may appear that the companies still do not conform to the norm. A norm, after all, is a sanction-

⁵² Nissenbaum arguably holds such a view. She proposes "a presumption in favor of the status quo; common practices are understood to reflect norms of appropriateness and flow, and breaches of these norms are held to be violations of privacy." Nissenbaum. *Contextual Integrity*, *supra* note 20, at 127. It is not clear what Nissenbaum includes in her "status quo." Does it include existing technology and the limitations it imposes? If it would seem—implausibly—that taking advantage of any technological advance entails a violation of the norm. I think focusing on loss of value-justification instead of violation actually better captures the point Nissenbaum is after.

⁵³ See Gary Alan Fine, *Enacting Norms: Mushrooming and the Culture of Expectations and Explanations*, in Hector & Opp, *supra* note 15, at 139.

supported behavioral regularity *to which we think we ought to conform*. It may appear obvious that we do not think we should conform. Surely to claim that we think we ought to conform is just to ignore the intense controversy sparked by the health insurance industry's use of data aggregation services. I briefly review the controversy before returning to the question of whether it shows there is no norm.

The basic complaint is that “[i]n a country without universal health care coverage, individuals seeking to secure health insurance face market-driven industry efforts to avoid insuring those likely to generate claims.”⁵⁴ There are two objections to distinguish. The first is about process; the second, about substance. The process objection is that health care is such an important good that its distribution should not be so extensively determined by profit-motive-driven corporations seeking to avoid insuring those who may most need medical treatment. *Individuals*, as opposed to health insurance companies, should have a greater role in determining how health care is distributed. In the past, they did. Simply withholding information on an insurance application provided some control over what an insurance company knew and hence some control over the distribution of health care. The second objection is that health-insurance-industry-determined distribution of health care is deeply flawed: the system is too

⁵⁴ RULE, *supra* note 1, at 110.

costly, and many who ought to have health care do not receive it.⁵⁵ It does not matter for our purposes whether these objections are correct.

What does the controversy show? Does it show that many do *not* think that we think we ought not to go along with the health insurance industry's practice of processing information in any legal way appropriate to a health insurer? The answer is that there is still an important sense in which we think we ought to conform to the practice. An analogy is helpful. The current norm in standard form, merchant-consumer contracts is for the parties to abide by the arbitration clauses those contracts routinely contain. Some commentators and consumers object to the clauses; assume, for the sake of argument, that *most* commentators consumers object and—in *that sense*—think they ought not to conform to the norm. As long as the courts continue to enforce such clauses, they still have no choice other than to conform to them, *and* they think they ought to (assuming they think they should obey the law⁵⁶). In this case, the norm persists as a *legally-generated* norm. There is a similar argument in the case of the health insurance companies. The reason is that in entering insurance contracts we have consented to the companies' data collection activities⁵⁷ and hence they

⁵⁵ See, e. g., JONATHAN COHN, *SICK: THE UNTOLD STORY OF AMERICA'S HEALTH CARE CRISIS* (2007); and, Bob Roehr, *Health Care in the US Ranks Lowest Among Developed Countries*, 337 *BMJ* a889 (2008), available at http://www.bmj.com/cgi/content/extract/337/jul21_1/a889.

⁵⁶ See *supra* note 16 and accompanying text.

⁵⁷ In regard to MIB, see MIB Privacy Policy, at http://www.mib.com/html/mib_privacy_policy.html (MIB records collected and distributed only with the insured's consent); in regard to IntelliScript, see *What Is An Authorized Request*, Frequently Asked Questions,

have the legal right to collect and use that information. We (most of us) think we ought to obey the law, so we think we ought to conform to insurance industry's practice of processing information only in ways appropriate to a health insurer—where appropriate ways include any legal ways of assessing applicants' morbidity and mortality. The norm persists as a legally-generated norm—even though consumers do not agree that appropriate ways include all legal ways of assessing applicants' morbidity and mortality.

What the controversy over the role of the health insurance industry in determining the distribution of health care *does* show is that the health insurance company informational norm is no longer value-justified.

3. The norm is no longer value-justified

A role-specific informational norm is value-justified when, in light our values, we can justify balance it strikes between informational privacy and competing concerns. In this case the balance is between ensuring a sufficient citizen voice in the just distribution of health care, and allowing health insurance companies to effectively pursue their policies. The current norm strongly favors the insurance companies. If consumers were to reflect adequately on the balance the norm strikes, it is highly unlikely that they would conclude that, the balance is justified. As the controversy shows, most of those who have carefully reflected on the balancing conclude the

<http://www.rxhistories.com/faq.html> (prescription history requests collected and shared only with the insured's consent).

opposite. Note that this does not mean that we know what the balance should be. We just know what it should *not* be.

B. Generalizing from the Health Insurance Example

The health insurance example illustrates the following pattern. Increased information processing power ensures the far more effective enforcement of business policies and thereby creates controversial balancing questions. As a result, although insurers conform to the relevant role-specific informational, norm that norm is no longer value-justified. The pattern appears in a variety of contexts, including innovative businesses that, as part of their business plan, process a vast amount of different types of information. In this regard, I discuss ChoicePoint, Google, and the contemporary practice of direct marketing. Other contexts in which the same pattern appears include the extension of credit,⁵⁸ employment decisions,⁵⁹ news reporting,⁶⁰ and the practice of price discrimination.⁶¹ My

⁵⁸ James Rule discusses the greatly enhanced ability of creditors to determine whether their criteria of credit worthiness are fulfilled. RULE, *supra* note 1, at _____. Controversy surrounds these practices, which are in part responsible for global financial crisis of the early twenty-first century. Creditors are conforming to the norm of collecting information appropriate to determining credit-worthiness, but the norm is no longer value-justified.

⁵⁹ Data aggregation services provide employers with a wealth of information about their potential hires. Few would deny that employers should have *some* information; the question is how much. See *infra* text accompanying note 66. Employers are conforming to the norm of collecting information appropriate to determining the qualifications of potential employees, but the norm is no longer value-justified.

⁶⁰ Technology has both expanded reporters access to information and their ability to report it through non-traditional means such as blogs. See *infra* Section V (discussing the impact of the Consumerist blog posting on Facebook). The depth to which reporters can penetrate into people's lives is highly controversial. The reporters are conforming to the norm of collecting information appropriate to news

discussion of ChoicePoint, Google, and direct marketing will be extremely brief; my intent is merely to illustrate how the same pattern emerges in seemingly disparate contexts.

1. ChoicePoint

ChoicePoint is one of the largest companies in the multi-billion-dollar information aggregation business, the business of collecting and reselling personal information.⁶² ChoicePoint exploits the information processing power of computers and the Internet to obtain 40,000 new public records daily for its ever-growing database of more than 19 billion records.⁶³ Access to this information allows employers, credit agencies, insurance companies, or anyone else interested in whether someone conforms to a certain standard to

reporting--at least arguably. One might well think there is simply a norm-violation here. But even if they do conform, the norm is no longer value-justified.

⁶¹ Price discrimination is simply charging different buyers different prices for essentially the same product or service. Hal Varian, *Differential Pricing and Efficiency*, at <http://www.firstmonday.org/issues/issue2/different>. 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*, at <http://www.dtc.umn.edu/~odlyzko/doc/networks.html>. 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 that they can collect and use the necessary information. *Id.* Price discrimination and its data collection practices are controversial. See Andrew Odlyzko, *Privacy and the clandestine evolution of ecommerce*, at <http://www.dtc.umn.edu/~odlyzko/doc/networks.html>. Price discriminators are nonetheless conforming to the norm of collecting information appropriate to determining willingness to pay, but the norm is no longer value-justified.

⁶² Beales & Muris, *supra* note 11, at 109 - 110.

⁶³ Duane D. Stanford, *All our lives are on file for sale*, ATLANTA J. CONST., Mar. 21, 2004 at 1A. For information about ChoicePoint, see Robert O'Harrow, *No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society* (Free Press Jan. 2005).

make that determination with far more effectiveness than would have been thought possible prior to the advent of information aggregators.

The availability of this wealth of information generates controversial questions about how to balance the benefits of access against the impact on informational privacy. The benefits include increased efficiency; increased relevant information and decreased irrelevant information for consumers; and decreased fraud.⁶⁴ Critics counterpose two harms. The first is the creation of chilling and coercive effects.⁶⁵ The ChoicePoint records "contain a great deal of information about individuals, often very sensitive information."⁶⁶ The information includes: social security numbers; financial account numbers; information about children as well as allegations of wrongdoing in regard to them (from family law files); details of medical conditions and other highly personal information about the effect of conditions, preexisting conditions, or information relevant to supporting an allegation that the claims are exaggerated (from insurance litigation files); allegations about lifestyle and sexual history (from sexual harassment files); and a variety of very sensitive personal information pertaining to alleged criminal activities (from criminal files).⁶⁷ Critics complain that

⁶⁴ See *infra* text accompanying note 44.

⁶⁵ Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 560 (1995) (noting how data processing "creates a potential for suppressing a capacity for free choice: the more that is known about an individual, the easier it is to force his obedience"). See also *supra* note 44 and accompanying text.

⁶⁶ Beth Givens, *Public Records on the Internet: The Privacy Dilemma* (Apr. 19, 2002), at <http://www.privacyrights.org/ar/onlinepubrecs.htm>.

⁶⁷ *Id.*

our 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. I believe, sadly, we will be contacted by many more.⁶⁸

The second objection is that aggregation creates pernicious stereotypes. Ann Bartow, for example, argues that businesses are aggregating data to construct a profile of the typical female consumer; “[d]atum by datum, woman by woman, the cyber-definition of “female” is being constructed. . . . Derivative e-stereotypes, braced by a plenitude of personal information, will appear scientific and incontrovertible.”⁶⁹ She worries that men and women will understand women through a business-constructed stereotype that distorts perceptions and limits possibilities.⁷⁰ Joel Reidenberg also complains of “invidious stereotyping.”⁷¹ He contends that Acxiom,⁷² another major information aggregator, “offered a comprehensive ethnicity coding

⁶⁸ *Id.*

⁶⁹ Ann Bartow, *Our Data, Ourselves: Privacy, Propertization, and Gender*, 34 U.S.F. L. Rev. 633, 653 – 54 (2000).

⁷⁰ *Id.* at 655 - 58.

⁷¹ Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 883 (2003).

⁷² Acxiom describes its services at <http://www.acxiom.com/>.

system . . . [and] also proposed to clients coding that resembled Nazi Germany's Nuremberg laws."⁷³

The controversy does *not* show that ChoicePoint fails to conform to the following norm: process information only in ways appropriate to the role as an information aggregator. This norm licenses ChoicePoint to collect, analyze, and distribute *any* information insofar as it does so legally. The role of an information aggregator *just is* to collect, analyze, and distribute information. The objection to recognizing this norm is the same as the objection to recognizing the analogous norm in the case of the health insurance industry: namely, the controversy shows that we, most consumers at least, do not think that we ought to acquiesce in ChoicePoint's informational processing activities. The answer is also the same: ChoicePoint's information processing activities are legal, and, since we think we ought to comply with the law we think—in *this* sense—that we ought to acquiesce in ChoicePoint's informational processing activities.

What the controversy shows is that the norm is not value-justified. The norm is value-justified if, in light our values, we could, on adequate reflection, justify the balance it strikes between informational privacy and competing concerns. It seems highly unlikely that consumers in general would regard the balance as justified. The critics and commentators who have carefully considered the question have raised sufficient doubts about the wisdom of ChoicePoint's practices that it is difficult to see how, on

⁷³ *Id.* (quoting ACXIOM PRODUCT CATALOG 5 (1999)).

reflection, the majority of us would conclude that it is clearly justified in light of our values.⁷⁴

2. Google

Google offers a variety of services, including a search engine, email, social networking, and a browser.⁷⁵ In the pursuit of these activities, it collects, analyzes, and distributes an astonishing amount and variety of information.⁷⁶ A contrast with both the health insurance industry and ChoicePoint is instructive. The health insurance companies have a long established practice of processing information relevant to assessing morbidity and mortality. There is no such established practice in the case of ChoicePoint. Information aggregation (on the scale of ChoicePoint at least⁷⁷) is a relatively new business. ChoicePoint's role as an information aggregator nonetheless defines the range of information processing relevant to pursuing that role: within legal limits, process any information for which there is sufficient market demand. Google's business activities do not as clearly define the range of information relevant to pursuing those activities. There is no ready answer to the question of what information is especially relevant to

⁷⁴ As in the case of the health insurance industry, this does not mean we know what the balance should be; we just know is what it should *not* be.

⁷⁵ Zimmer, *supra* note 20, at 109 – 110.

⁷⁶ Zimmer, *supra* note 20, at 115 – 126 (summarizing Google's information processing practices).

⁷⁷ Data aggregation is actually a long established practice. Traditional mail order selling requires a database of addresses. In 1917, for example, the total mail order business in the United States was approximately \$1.5 billion. *History of Direct Mail*, DirectMail.org, <http://www.direct-mail.org/history3.htm>.

providing a search engine, email services, social networking services, and a browser. Perhaps in part for this reason, Google's information processing activities have ignited controversy.⁷⁸ The critics express concern about a dramatic reduction in freedom. Daniel Solove, for example, contends that we are

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. Ironically, the unconstrained flow of information on the Internet might impede our freedom.⁷⁹

Google nonetheless conforms to the following norm: Collect information only insofar as it is appropriate to its business activities, where Google itself determines what is appropriate. It is nonetheless clear that the norm exists as a legally-generated norm. The argument is the by now familiar one: Google's customers consent to its information processing

⁷⁸ "Anxieties [about search engine information processing practices] led news organizations to investigate and report on the information search engines routinely collect from their users, which led to criticism by various advocacy groups, which, in turn, has led to inquiries and investigations by European and U. S. government regulators, all with Google as the primary target." Zimmer, *supra* note 20, at 113 (citations omitted).

⁷⁹ DANIEL J. SOLOVE, *THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET* 17 (2007).

activities;⁸⁰ hence Google has the legal right to collect and use that information; we ought to obey the law,⁸¹ so we think we ought to conform to Google's information processing practices. What the controversy shows is that the norm is not value-justified. Critics have raised sufficient doubts about Google's practices that it is highly unlikely that the majority of us would conclude, after adequate reflection, that Google's information processing activities are clearly justified in light of our values.

3. Direct marketing

Direct marketing sorts buyers into groups according to their willingness to purchase certain products and services.⁸² Technology has greatly increased its power to make such discriminations:

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

⁸⁰ Google provides its services under a terms of service agreement. http://www.google.com/privacy_terms.html. Under section 7.2 of the agreement ("You agree to the use of your data in accordance with Google's privacy policies"), users agree to be bound by the various privacy policies that define how Google may process information related to the use of the services it offers.

⁸¹ See *supra* note 16 and accompanying text.

⁸² "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." Carol Scovotti & Lisa Spiller, *Revisiting the Conceptual Definition of Direct Marketing: Perspectives from Scholars and Practitioners*, at <http://www.the-dma.org/dmef/proceedings05/Revisitingthe-Spiller.pdf>.

products; male buyers of fashion underwear; believers in the feminist political movement, anti-gay movement, and prayer in the public schools.⁸³

The contemporary, technologically-enhanced practice of direct marketing has the power to make an incredibly wide range of correlations between types of people and the willingness to buy various products and services. The result is an across the board expansion of the types of information is appropriate for a business to process under applicable role-specific norms. Imagine, for example, that direct marketers discovered that people who dress a certain way, or who have certain liver functions, are likely to purchase certain wines. The wine store—or the direct marketing firm it has engaged—could collect that information while nonetheless conforming to the following norm: collect information only in ways appropriate to direct marketing. The information processing activities of direct marketers have proven highly controversial.⁸⁴ Nonetheless, for the same reasons as in the case of the health insurance industry, ChoicePoint, and Google, the norm persists as a legally-generated but not value-justified norm.

C. Collaborate Or Resist?

To summarize: the increased ability to process information increases the ability of businesses to discriminate among types of consumers. This results (across a wide range of cases) in informational norms that are not value-justified. Loss of value-justification means loss of control: we have

⁸³ RULE, *supra* note 1, at 104.

⁸⁴ RULE, *supra* note 1, at 102 – 105.

lost the control over personal information that value-justified norms provide. The loss puts freedom and hence self-realization at risk. The privacy advocates capture this vision in the metaphor of the panopticon. As Jon Mills explains,

totality of current technology and the demand for information creates what can be termed a “panopticon effect.” In the late 1700’s, Jeremy Bentham embarked on a wide campaign of prison reform. He championed the concept of “the Panopticon,” . . . a circular prison structure with . . . an observation tower in the center. Prison cells are stacked and arranged around the perimeter such that they constitute the entire thickness of the structure’s walls . . . [E]ach and every cell is visible from the central tower. The windows of the tower . . . block all visibility from without, allowing the guards to monitor the prisoners, but preventing the prisoners from seeing the guards . . . This design creates a round-the-clock surveillance machine. Prisoners never know whether they are being watched at any point in time . . . Because of psychological pressure, prisoners are forced to conform their behavior to acceptable standards at all times, effectively becoming their own wardens.⁸⁵

The metaphor is an effective reminder that the “round-the-clock surveillance machine” of private surveillance puts freedom and self-realization at risk.

How should we respond?

We could collaborate. We could accept—or at least not resist—routine mass surveillance. The likely outcome would be that controversy over the power of businesses to enforce policies would eventually die down; and, as our values adjusted, we would come to regard such power as acceptable. In light the adjusted values, we would be able once again to justify role-specific informational norms, and the once-again-value-justified norms would provide us with control over personal information. But it would be a very different “control.” It would be a far more circumscribed control than we

⁸⁵ MILLS, *supra* note 6, at 70 – 72.

enjoyed before the rise of routine mass surveillance, before “the world of the all-seeing eye.”⁸⁶ Businesses would enforce their policies with an effectiveness that channeled consumers along the specified lines. The degree of freedom we once enjoyed would be gone—and, with it, opportunities for self-realization that once lay open before us. Life in a business surveillance panopticon would have arrived. Any even relatively close approximation to life in a panopticon is inconsistent with the value we place on freedom and self-realization—at least with the value many, perhaps most of us, place thereon.

For those with such values, the question is how we can regain the lost control over our personal information. In the next section I consider whether we can regain control through legal regulation; in Section V, I consider non-legal means.

IV. Can We Regain Control Through the Law? Two Dim Prospects

The solution may seem obvious: require consent. More fully, why not simply require by statute that businesses to obtain consent before they collect certain types of information?⁸⁷ Doing so would appear to return to us the control that technology has removed. Unfortunately, a consent requirement fails to return to us the desired control.

⁸⁶ FRIEDMAN, *supra* note 3.

⁸⁷ Joel Reidenberg is among the many who suggest this approach. Reidenberg, *supra* note 71. James Rule also suggests a consent requirement. RULE, *supra* note 1, 196.

A. Requiring Consent Will Not Return Control

The inadequacy of a consent requirement becomes clear as soon as one focuses on the mechanism that would be used to obtain consent: a standard form, no-negotiation agreement. Both businesses and consumers will insist on this. Businesses will insist because they want to benefit of using standard form agreements to manage their legal risks effectively without costly one-on-one negotiation.⁸⁸ Consumers will insist because they do not take the time and trouble to read privacy policies.⁸⁹ As J. Howard Beales and Timothy Muris note,

Judging by behavior in the marketplace, most consumers have better things to do with their time than read privacy notices. The point is not that transaction costs are particularly high, because it does not take long to process a privacy notice. Rather, processing privacy notices is a cost that most consumers apparently do not believe is worth incurring. The perceived benefits are simply too low. Simpler notices

⁸⁸ See, e. g., E. ALLAN FARNSWORTH, *CONTRACT* § 4.26 (2004) (explaining how standardization leads to cost reduction); Batya Goodman, Note, *Honey, I Shrink-Wrapped the Consumer: The Shrink-Wrap Agreement as an Adhesion Contract*, 21 *CARDOZO L. REV.* 319, 325 (1999) (explaining universal benefit of cost reduction); John J.A. Burke, *Contracts as a Commodity: A Nonfiction Approach*, 24 *SETON HALL LEGIS. J.* 285, 286-90 (2000) (observing that "universal" use of standard-form contracts is "unquestioned" as efficient business practice).

⁸⁹ See Kang, *supra* note 44, at 1248 (stating that "[f]or 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"). Many have observed that buyers do not as a rule read standard form contracts. See, e. g., Robert A. Hillman, *On-line Consumer Standard-Form Contracting Practices: A Survey and Discussion of Legal Implications*, in *CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY'* (Jane Winn (ed.), 2006) (reporting survey results supporting the claim that online buyers do not read contracts); Melvin Aron Eisenberg, *The Limits of Cognition and the Limits of Contract*, 47 *STAN. L. REV.* 211, 240-41 (1995) ("[C]onsumers who are faced with the dense text of form contracts characteristically respond by refusing to read"); Michael I. Meyerson, *The Reunification of Contract Law: The Objective Theory of Consumer Form Contracts*, 47 *U. MIAMI L. REV.* 1263, 1269-70, 1275 (1993) ("It is no secret that consumers neither read nor understand standard form contracts"); Melvin Aron Eisenberg, *Text Anxiety*, 59 *S. CAL. L. REV.* 305, 309 (1986) (dense form contract language discourages consumers from reading terms).

are always possible, but 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.⁹⁰

Beales and Muris emphasize the complexity of privacy policies that attempt to convey meaningful information: "Everyone who has received a financial privacy notice (and has actually perused it) is aware that the notices are often long, complex, and filled with legal jargon."⁹¹

The difficulty of conveying sufficient information to make a consumer's choice adequately informed is even more severe than they suggest. It is, as practical matter, impossible to do so. The problem is that information is collected on one occasion for one purpose is typically retained, analyzed, and distributed for a variety of other purposes in unpredictable ways. 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. It is the totality of information about a person and how it is used that poses the greatest threat to privacy. . . . 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.⁹²

Improper valuation deprives consumers of adequate control over their information. To the extent that consumers mistakenly impart information

⁹⁰ Beales & Muris, *supra* note 11, at 109 - 110. Beales was the Director of the Federal Trade Commission's Bureau of Consumer Protection, 2001 - 2004; Muris was the Chairman of the Federal Trade Commission 2001 - 2004.

⁹¹ *Id.* at 113.

⁹² Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1452 (2001).

that they would withhold were they better informed, they impair their informational privacy. To the extent that they mistakenly withhold information that they would impart were they better informed, they forego the gains of disclosing the information.

A consent requirement cannot return the control we have lost through the undermining of informational norms. If we wish to regain such control, we must reestablish value-justified, role-specific informational norms. Why not do so with *legally-generated* norms? Why not pass statutes that create the necessary norms?

B. Legally-Generated Norms Will Not Return Control

One difficulty is achieving sufficient legislative agreement on highly controversial matters like health care insurance. I will put that problem aside in order to focus on another difficulty, one that remains even if legislative agreement is achieved. The problem is that, to return to us the norm-created control we have lost, it is not sufficient merely to create a legally-generated norm; one must also ensure that there is widespread knowledge of it. I argue first that widespread knowledge is required and then contend that the law's ability to meet this requirement is limited.

Why is it a problem that the legally-generated norm be widely known? How can a norm exist and not be known? In fact, this is common in the case of legally-generated norms. Recall the contractual norm, "Sellers may (within broad limits) disclaim consequential damages."⁹³ As noted earlier,

⁹³ See *supra* note 16 and accompanying text.

the vast majority of buyers do not even know what consequential damages are, let alone realize that sellers are allowed to disclaim them. Their relation to the norm is hypothetical: if they were aware of it, they would think they ought to conform to it.⁹⁴ Such a hypothetical relation to a legally-generated norm is insufficient to return to us the control we have lost. That control rests on actual knowledge.

The earlier wine store example illustrates the point. Vicky and the store share—and know they share—the conception of appropriateness incorporated in the relevant role-specific informational norm. Thus, when she enters the store, Vicky *knows* what information will, and what information will not be collected and processed. As a result, she knows that she need not fear chilling or coercive effects from the disclosure of certain information, and she is on notice that such effects may arise from the information that is disclosed. This is precisely what Vicky does *not* know if she enters the store knowing only that the law regulates the processing of information, but not knowing what that regulation is. She is exposed to unknown chilling and coercive effects. *Known* value-justified norms guarantee action based on knowledge; lack of knowledge condemns to action under uncertainty. If we want the control we once had, the new norms we create must be widely known.

The law's ability to create the necessary knowledge is quite limited, as the "disclaim consequential damages" norm illustrates. Sellers routinely disclaim such damages, and their ability to do so is asserted in the Uniform

⁹⁴ *Id.*

Commercial Code, and in every state which has enacted a statutory version of the Code; however, as any first-year Contracts professor can testify, non-lawyers are generally unaware, not only of the relevant law, but of the meaning of “consequential damages.” This is just one illustration of the obvious fact that passing a statute is one thing while it is quite another to create general public awareness and understanding of it.

C. A Solution Through Technology?

The prospects for reestablishing control over personal information through the legal creation of informational norms appear dim. But the law is not the only way to generate norms. It did not create the norms governing where you stand in an elevator, or how long you talk at a roundtable. They arose out of patterns of social interaction. Are there patterns of interaction that might give rise to new value-justified informational norms? There may be some reason to think so. The very information processing technology that currently deprives norms of value-justification may also create the context in which new norms will emerge. It may do so because the technology can make businesses more transparent and hence more accountable.⁹⁵ Esther Dyson emphasizes this point:

In the networked world, you cannot—and cannot expect to—control your company's image; the best you can do is influence it. Anything

⁹⁵ See DAVID BRIN, *THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM?* (1998); and Jeffrey M. Aresty & Richard Warner, *Reinventing Law in Cyberspace: A Social Contract for the Digital Age and International Business Negotiations*, ABA GUIDE TO INTERNATIONAL BUSINESS NEGOTIATIONS, (James Silkenat, Jeffery Aresty & Jacqueline Klosek, (eds.), forthcoming) (discussing the effects of Internet-created transparency).

and everything about a company can be known—every slipup, every policy, every practice. You can't control what people say about your company. On the Internet, they'll say anything they like, which may be a mixture of fact, fiction, and opinion. Living with this transparency requires executives to change their thinking fundamentally: they have to learn that their company is what people see it to be and that they must figure out how to turn that visibility to their advantage.⁹⁶

Will more transparent—and hence more accountable—businesses interact with their customers in ways that led to the emergence of value-justified shared-conception role-specific informational norms? The recent controversy over Facebook's Terms of Service agreement suggests that answer may be "yes"—or, at least that it is not obviously "no."

V. Facebook's Terms of Service Controversy: A Sign of Hope?

Controversy erupted in February 2009 when Facebook revised its Terms of Service agreement. The original agreement contained the following grant of a license:

You hereby grant Facebook an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to (a) use, copy, publish, stream, store, retain, publicly perform or display, transmit, scan, reformat, modify, edit, frame, translate, excerpt, adapt, create derivative works and distribute (through multiple tiers), any User Content you (i) Post on or in connection with the Facebook Service or the promotion thereof subject only to your privacy settings or (ii) enable a user to Post, including by offering a Share Link on your website and (b) to use your name, likeness and image for any purpose, including commercial or advertising, each of (a) and (b) on or in connection with the Facebook Service or the promotion thereof.⁹⁷

⁹⁶ Esther Dyson, *Mirror, Mirror on the Wall*, HARVARD BUSINESS REVIEW, 24 (Sept.-Oct. 1997).

⁹⁷ Chris Walters, *Facebook's New Terms Of Service: "We Can Do Anything We Want With Your Content. Forever."*, THE CONSUMERIST, Feb. 15, 2009, at <http://consumerist.com/5150175/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever>.

Facebook made two changes that altered the duration of this grant.

First, it deleted this provision: “You may remove your User Content from the Site at any time. If you choose to remove your User Content, the license granted above will automatically expire, however you acknowledge that the Company may retain archived copies of your User Content.”⁹⁸ It then substituted a provision that asserted that the license would *not* expire after the user removed content (content still retained in the archived copies).⁹⁹

The changes were short-lived. An immediate outcry from its members compelled Facebook to return temporarily to the original agreement¹⁰⁰ and to institute “a new approach that will allow all users to have a voice in shaping the policies that govern the Facebook service.”¹⁰¹ The

new approach to site governance . . . offers its users around the world an unprecedented role in determining the future policies governing the service. Facebook released the first proposals subject to these new procedures – The Facebook Principles, a set of values that will guide the development of the service, and Statement of Rights and Responsibilities that make clear Facebook’s and users’ commitments related to the service. Over the coming weeks, users will have the opportunity to review, comment and vote on these documents. An update to the Privacy Policy is also planned and this change will be subject to similar input.¹⁰²

Two points bear emphasis.

⁹⁸ *Id.*

⁹⁹ *Id.*

¹⁰⁰ Mark Zuckerberg, *Update on Terms*, FACEBOOK, February 17, 2009, at <http://blog.facebook.com/blog.php?post=54746167130>. Mark Zuckerberg is the founder of Facebook.

¹⁰¹ FACEBOOK, at <http://www.facebook.com/group.php?gid=69048030774>.

¹⁰² At <http://www.facebook.com/press/releases.php?p=85587>.

First, the result of the new approach could be a value-justified, shared-conception, role-specific informational norm. If Facebook's members have sufficient input, and if they can reach sufficiently widespread agreement on a new Terms of Service agreement, then it is reasonable to assume that the agreed on terms will express a value-justified sanction-supported regularity to which Facebook members think they ought to conform. It will be a sanction-supported regularity because Facebook and its members will conform to the terms, which are enforceable under the Terms of Use agreement. Members will think that they ought to conform—and not merely because they think they should conform to legally enforceable agreements. They will think they should conform because the regularity incorporates a shared conception of appropriate information processing, a conception balancing competing interests in ways the members see as justifiable.

Second, should this happen, part of the explanation will be the increased businesses transparency created by the very information processing technology that currently undermines informational norms. Facebook's new approach is the outcome of a controversy ignited and spread with great rapidity as a result of a blog entry. When a blog entry on The Consumerist noted the change in the agreement, comments immediately proliferated.¹⁰³ There could be no better example of Dyson's observation that

¹⁰³ Brad Stone & Brian Seltzer, *Facebook Withdraws Changes in Data Use*, THE NEW YORK TIMES, Feb. 18, 2009, <http://www.nytimes.com/2009/02/19/technology/internet/19facebook.html> (noting that The Consumerist blog "entry set off an explosion of activity that overwhelmed Facebook's own attempts to quickly clarify the matter," and that after "three days of pressure from angry users and the threat of a formal legal complaint by a coalition of consumer advocacy groups, the company reversed changes to its contract").

in “the networked world, you cannot—and cannot expect to—control your company's image; the best you can do is influence it. Anything and everything about a company can be known—every slipup, every policy, every practice.”¹⁰⁴

Is the Facebook controversy an isolated incident, or a harbinger of processes that will reestablish value-justified shared-conception informational norms? We might put the question this way: will we escape imprisonment in the business surveillance panopticon because we can see the guards? Perhaps it is not unreasonable to hope so.

¹⁰⁴ Dyson, *supra* note 96.