2000

# Examined Lives: Informational Privacy and the Subject as Object

Julie E. Cohen
*Georgetown University Law Center*, jec@law.georgetown.edu



52 Stan. L. Rev. 1373-1438 (2000)

# Examined Lives: Informational Privacy and the Subject as Object

Julie E. Cohen*

*In the United States, proposals for informational privacy protection have proved enormously controversial. On a political level, such proposals threaten powerful data processing interests. On a theoretical level, data processors and other data privacy opponents argue that imposing restrictions on the collection, use, and exchange of personal data would ignore established understandings of property, limit individual freedom of choice, violate principles of rational information use, and infringe data processors' freedom of speech. In this article, Professor Julie Cohen explores these theoretical challenges to informational privacy protection. She concludes that categorical arguments from property, choice, "truth," and speech lack weight, and mask fundamentally political choices about the allocation of power over information, cost, and opportunity. Each debate, although couched in a rhetoric of individual liberty, effectively reduces individuals to objects of choices and trades made by others. Professor Cohen argues, instead, that the debate about data privacy protection should be grounded in an appreciation of the conditions necessary for individuals to develop and exercise autonomy in fact, and that meaningful autonomy requires a degree of freedom from monitoring, scrutiny, and categorization by others. The article concludes by calling for the design of both legal and technological tools for strong data privacy protection.*

I. INTRODUCTION: INFORMATIONAL PRIVACY AS PARADOX ..... 1374
II. OWNING ..... 1377
A. *Why Ownership at All?* ..... 1378
B. *Theories of Ownership* ..... 1380
C. *Ownership, Liberty, and Friction* ..... 1384
III. CHOOSING ..... 1391
A. *Theories and Technologies of Choice* ..... 1392
B. *Choice, Parameters, and Tradeoffs* ..... 1395
IV. KNOWING ..... 1402
A. *Theories of Knowledge* ..... 1402
B. *Knowledge, Persuasion, and Power* ..... 1405
V. SPEAKING ..... 1408

---

* Associate Professor, Georgetown University Law Center. J.D., 1991, Harvard; A.B., 1986, Harvard-Radcliffe. Internet: jec@law.georgetown.edu. I thank C. Edwin Baker, Susan Freiwald, Brett Frischmann, Vicki Jackson, Michael Madison, John Parry, Joel Reidenberg, Marc Rotenberg, Louis Michael Seidman, Marc Spindelman, Lynn Stout, David Vladeck, Phil Weiser, and participants in a faculty workshop at the Georgetown University Law Center for their valuable comments, and Elizabeth Monkus and Erin Roth for research assistance. This article was prepared in part with the support of a summer research grant from the Georgetown University Law Center. All Internet citations were current as of May 22, 2000. 

A. *Theories of (Commercial?) Speech* .....1409
B. *Speech, Property, and Market Institutions*.....1416
VI. BECOMING: TOWARD A DYNAMIC THEORY OF INFORMATIONAL PRIVACY...1423
A. *The Values of Informational Privacy* .....1423
B. *Informational Privacy in Practice* .....1428
VII. CONCLUSION: INFORMATIONAL PRIVACY BY DESIGN .....1436

> [T]he unexamined life is not . . . worth living.[1]
>
> The distinctive discourse of modernity is one of prediction and control. . . . Ironically, there is a profound helplessness in surrendering the future to prediction and control, and there would be even if we could predict and control things at will.[2]

## I. INTRODUCTION: INFORMATIONAL PRIVACY AS PARADOX

Collections of information about, and identified to, individuals have existed for decades. The rise of a networked society, however, has brought with it intense concern about the personal and social implications of such databases—now, in digital form, capable of being rapidly searched, instantly distributed, and seamlessly combined with other data sources to generate ever more comprehensive records of individual attributes and activities.[3] In 1995, with much fanfare, the European Union adopted its Directive on the legal protection of personal identifying information ("European Data Protection Directive").[4] Although the United States has not followed suit—and although powerful interests oppose the recognition of general privacy rights in personal data—public concern about networked databases of personally-identified information is on the rise. Congress is holding hearings[5]; the Federal Trade Commission ("FTC") is conducting investigations[6]; the Admini-

---

1. PLATO, THE APOLOGY (attributing statement to Socrates), *reprinted in* R.E. ALLEN, SOCRATES AND LEGAL OBLIGATION 37, 58 (1980).

2. ALBERT BORGMANN, CROSSING THE POSTMODERN DIVIDE 2 (1992).

3. For a good summary of the sorts of "data mining" that networked databases make possible, see generally A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 479-505 (1996).

4. Council Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L. 281) 31 [hereinafter European Data Protection Directive].

5. *See, e.g.*, 143 CONG. REC. H5809 (daily ed. July 25, 1997) (statement of Rep. Vento) (discussing FTC privacy initiatives led by then-Commissioner Varney); 144 CONG. REC. S3136-37 (daily ed. Apr. 2, 1998) (statement of Sen. Jeffords) (describing congressional efforts to enact comprehensive data privacy legislation). *But see* CENTER FOR PUBLIC INTEGRITY, NOTHING SACRED: THE POLITICS OF PRIVACY 7 (1998) (asserting that whenever Congress actually acts on privacy-related matters, it invariably "turn[s] a privacy bill into a Trojan Horse for corporate privacy invaders").

6. FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS, i-iv (1998) (indicating the need for incentives for self-regulation of privacy online, but also noting a special need for Congress to take action to protect children's online privacy).

stration has hired a "privacy czar"—the first such official in United States history.[7] There is much disagreement about what comes next, but there is also a growing (if still inchoate) consensus that *something* needs to be done.

But privacy theory and privacy rhetoric do not know quite what to do with the notion of "informational privacy."[8] Firms that traffic in personally-identified data argue that the information collected, processed, and exchanged is both their property (because it is valuable) and their constitutionally-protected speech (because it is information). These arguments have a certain intuitive appeal. In contrast, the notion that information about one's ordinary transactions and interactions with others should be secret, or otherwise subject to one's personal control, strains the boundaries of our understanding of what it means for something to be secret, and what it means for something to be owned. On a more theoretical level, meanwhile, the idea that "privacy" might encompass an enforceable right to prevent the sharing of (certain kinds of) personally-identified data seems to conflict with deeply held social values that elevate choice over constraint, freedom of speech over enforced silence, and "sunlight" over shadow.[9]

Or does it? Perhaps these categories—property, choice, speech, and knowledge—are not so straightforward as they seem. In this article, I argue that they are not. Conventional understandings of ownership, liberty, and expression do not easily stretch to accommodate informational privacy rights, but not because of any inherent incompatibility between privacy and ownership, or between privacy and economic or expressive freedom. Rather, the disjunct arises because these understandings are grounded in a theory of self-actualization based on exchange—designed to minimize transaction costs and other obstacles to would-be traders, and thus systematically, inevitably biased toward facilitating trade in personally-identified information. They are grounded, as well, in a theory of the social role of information that conceives information primarily as a lubricant to trade, and that seeks revealed truth about human potential (to be translated into trade advantage) in the rationalized, regularized processing of observed facts.

It is possible to view personally-identified information and individuals' claims to control it quite differently. But to do so requires that we under-

---

7. Robert O'Harrow, Jr., *Clinton Names Counselor on Privacy*, WASH. POST, Mar. 4, 1999, at E2 (noting appointment of Peter Swire as Clinton's chief privacy counselor); *White House Appoints Ohio State Prof. Swire as First Privacy Czar*, WALL ST. J., Mar. 4, 1999, at A6 (discussing Swire's appointment).

8. In this article, I will use the terms "informational privacy" and "data privacy" interchangably.

9. *See* Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 6-7 (1991) ("In general, scholarly analysis of the First Amendment disposes us toward the proposition that more information is better. We esteem 'sunlight' because it illuminates.").

stand how our categories constrain us. Parts II through V undertake that task.

Parts II and III examine the "property" and "choice" objections to strong data privacy rights. These objections rest on claims that data privacy protection would reduce liberty, both by interposing direct constraints on consensual market exchange and by undermining transactional efficiencies that promote such exchange. Yet in both cases, the particular social meanings ascribed to "liberty" and "efficiency" exclude from consideration other kinds of liberty and other kinds of social benefit that data privacy protection might promote. And in both cases, arguments from universal concepts of liberty and efficiency conceal a basic inequality in fact. As a practical matter—that is, given the way existing markets in personally-identified information actually work—the absence of data privacy protection elevates the liberty and efficiency claims of data processors above those of individuals.

Part IV considers the "knowledge" argument against data privacy protection, which asserts that the collection, exchange, and processing of personally-identified data is valuable because it promotes greater scientific and commercial understanding of individual behavior and desires. Without doubt, the study of individual behavior can enhance our understanding of it. Yet the paradigm of knowledge advanced by data privacy opponents rests on a facile equivalence between socially-determined modes of information processing and "truth" in all cases and for all purposes. It systematically privileges one kind of information—static and quantifiable—and one kind of knowledge—rationalizing and objectifying—at the expense of others at least equally important to the human enterprise. And again, the consequence for individuals is a loss, not a gain, in freedom; data-processing practices seek to shape and predict individual behavior according to externally-determined trajectories of opportunity and desire.

Part V addresses the argument that the collection and exchange of personally-identified data has intrinsic and constitutionally-protected value as "speech." This argument, too, is essentialist. It equates the market exchange of information for value with the highest sort of protected expression, and thus ignores that the relation between personally-identified information and expression is far more complex, and far less direct. Although data privacy protection clearly would affect the First Amendment rights of data processors, this is a strong argument against such protection only if it is assumed that government has no legitimate interest in regulating the non-communicative aspects of information markets, and that individuals have no countervailing property or contractual interests of their own in controlling their personal information. These assumptions, moreover, deny to individuals (but not to data processors) the benefits of arguments from "property" and "choice."

Regardless of the categorical lens through which the legal system views data privacy claims, the result is the same. Our conceptions of property, choice, and information reinforce one another; under all of them, individuals are treated as the natural and appropriate objects of others' trades, others' choices, others' taxonomies, and others' speech. Part VI advances a vision of data privacy protection grounded, instead, in a dynamic theory of individual autonomy. On this theory, one must, if one values the individual as an agent of self-determination and community-building, take seriously a conception of data privacy that returns control over much personal data to the individual. We must carve out protected zones of personal autonomy, so that productive expression and development can have room to flourish. We can do so—constitutionally—by creating a limited right against certain kinds of commercial collection and use of personally-identified information.

I conclude, in Part VII, with some observations about the complementary roles of law and technology in constructing an autonomy-centered regime of informational privacy protection. In a networked world, law alone cannot achieve effective protection of informational privacy, but that does not mean that privacy legislation would be futile. Instead, legal protection for informational privacy can provide (additional) incentives for the development of privacy-protective technologies.

## II. OWNING

The data privacy debate is (in part) a debate about the ownership status of a certain kind of information. The prevailing discourse of property rights, however, lacks a term to describe the particular state of "ownedness" that data privacy advocates seek for personal data. The state of being owned, in our legal culture, means a particular, contingent set of relational attributes thought to denote and promote trade. These are, roughly speaking, a condition of negative liberty for owners, an ethic of self-actualization through market exchange, and an absence of friction. These characteristics are fundamentally irreconcilable with the privacy project as defined by data privacy advocates. On their view, an effective data protection regime is defined by the friction it interposes between would-be trading partners, and the limits it sets on freedom to enter into agreements for the use of personal data.

The first task, then, is to consider whether these characteristics of things "owned" reflect something essential about the nature of "property" in general or personal information in particular. If so, laws imposing data privacy protection invariably will seem arbitrary and artificial, constraints to be evaded by conduct and outpaced by technology. If not, the property lexicon needs expansion to encompass the sort of ownership that the data privacy project seeks to define.

### A. *Why Ownership at All?*

It may be objected, at the outset, that notions of "ownership" are (or should be) irrelevant to the policy debate about data privacy. Within certain sectors of the privacy community, there is a deep-seated resistance to property talk. This reaction is at once visceral and deeply principled. On the one hand, the understanding of ownership that applies to, say, cars or shoes just seems a crabbed and barren way of measuring the importance of information that describes or reveals personality. But there is also a strong conviction that ownership as an intellectual concept doesn't encompass all of the legally relevant interests that an informed privacy policy should consider—that framing the privacy debate in terms of proprietary rights elides something vitally important and conceptually distinct about the interests that the term "privacy" denotes.[10]

Despite this opposition, property rhetoric has crept inexorably into the privacy debate. Opponents of strengthened privacy protection think of collections of personally-identified data as "their" property; as evidence, they point to their investment in compiling the databases and developing algorithms to "mine" them for various purposes.[11] Nor is property talk the exclusive province of privacy opponents. Some privacy advocates argue for "tradable privacy rights"—entitlements that would vest initially in individuals, but then could be freely exchanged for money, preferential service, or other perceived benefits.[12] Others contend, in effect, that individuals already enjoy such rights, and that the data privacy problem can be solved by adopting informed consent procedures that enable individuals to weigh privacy costs accurately when deciding whether and how to surrender "their" information to others.[13]

---

10. *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996); Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, 87 CAL. L. REV. 751 (1999) (reviewing Schwartz and Reidenberg's discussion of European data protection) (book review).

11. *See, e.g.*, Harris S. Gordon, Steven J. Roth, Scott J. Lieberman, Ann Zeller & Anne McConnell, *Customer Relationship Management: A Senior Management Guide to Technology for Creating a Customer-Centric Business* <http://www.the-dma.org/library/publications/customerrelationship.shtml> (discussing the importance of using personally-identified customer information for more effective marketing).

12. *See, e.g.*, James Glave, *The Dawn of the Infomediary*, WIRED NEWS, Feb. 24, 1999 <http://www.wired.com/news/business/0,1367,18094,00.html>; John Hagel III & Jeffrey F. Rayport, *The Coming Battle for Customer Information*, HARV. BUS. REV., Jan.-Feb. 1997, at 53 (discussing the role of intermediaries in data access negotiation and the potential benefits to consumers); Kenneth C. Laudon, *Markets and Privacy*, COMM. ACM, Sept. 1996, at 92 (advocating a regulated national information market).

13. *See, e.g.*, PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 156-70 (1998) (discussing various self-regulatory measures); *see also* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1287-94 (1998) (proposing a statute that would require any-

One answer to the question "Why ownership?" then, is that it seems we simply cannot help ourselves. Property talk is just how we talk about matters of great importance. In particular, it is how we talk about the allocation of rights in things, and personally-identified information seems "thingified" (or detached from self) in ways that other sorts of private matters—intimate privacy, for example—are not. On this view, the "propertization" of the informational privacy debate is a matter of course; it merely testifies to the enormous power of property thinking in shaping the rules and patterns by which we live. The interesting questions, of course, are why this is so, and what consequences follow from it.

On a slightly deeper level, recourse to property talk about privacy in general, and data privacy in particular, seems linguistically determined. "Private," of course, means "not public," in the sense that a secret is not publicly known. But "private" also means "not 'common'"—owned, and set apart from that which is common or owned by others. "Common," moreover, would not suffice to describe the desired characteristics of a strong data privacy regime. In our jurisprudence, things that aren't owned by someone are presumptively accessible to all, and frequently there for the taking by others.[14] Data privacy advocates seek, instead, to guarantee individuals control over their personal data. We lack a word for describing control over things without legal or beneficial ownership of them—a word that signifies that the thing described is both not common and not owned.

To note that privacy talk is embedded in the discourse of property, of course, is to beg the question whether reality is similarly embedded. Some philosophers argue that privacy has meaning only to the extent that it is reducible to a property interest.[15] That may be so—but it may be so because property talk imposes its own cognitive structure on reality. Once personally-identified information is conceived as an object separate from the self, property talk follows naturally; it is how we talk about objects. At the same time, however, it becomes more difficult to think of the information as having other characteristics, simply because property talk does not admit them.[16]

---

one acquiring personally-identified information from a cyberspace transaction to provide clear notice of intended uses of the information and to obtain the individual's prior consent).

14. *See* CAROL M. ROSE, *"Takings" and the Practices of Property: Property as Wealth, Property as "Propriety," in* PROPERTY AND PERSUASION: ESSAYS ON THE HISTORY, THEORY, AND RHETORIC OF OWNERSHIP 49, 53 (1994); Garrett Hardin, *The Tragedy of the Commons*, 162 SCI. 1243 (1968); *cf.* Carol M. Rose, *The Several Futures of Property: Of Cyberspace and Folk Tales, Emission Trades and Ecosystems*, 83 MINN. L. REV. 129, 132-37 (1998) (discussing the concept of "limited common property").

15. *See* JUDITH JARVIS THOMSON, THE REALM OF RIGHTS 285-88 (1990); Judith Jarvis Thomson, *The Right to Privacy*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 272 (Ferdinand David Schoeman ed., 1984).

16. *See generally* GEORGE LAKOFF & MARK JOHNSON, METAPHORS WE LIVE BY (1980) (illustrating how we use metaphors to structure our experiences).

In this sense, property language both describes and determines our experience of reality.

If personally-identified information is not to be considered a "thing" subject to ownership, though, how should we think of it? What, exactly, is conceptually distinct about privacy in general, or data privacy in particular? Philosophers and legal scholars have struggled for decades to articulate a compelling definition of privacy in other terms, as a locus of personal or dignitary interests.[17] Contrasted with property talk, this language seems fuzzy; the boundaries of things seem evident, but it's harder to know where the boundaries of dignity begin. A third explanation for property talk about privacy, then, is that property talk reflects a preference for boundedness, even at the risk of oversimplification.

Which view is right? Is privacy only about assigning property interests (in things), or is it about something more, or different, than ownership? And does it matter—that is, does ceding privacy to the seductively crisp discourse of property rights dictate a clear winner in the data privacy debate? How large, in other words, is the risk? The questions cannot be answered without a fuller exploration of what "property" means.

### B. *Theories of Ownership*

Mainstream property theorists recognize two main theoretical justifications for ownership: Lockean labor-desert theory, and a more explicitly utilitarian theory that focuses on economic efficiency. As currently interpreted, these theories converge on a vision of property as constituted by and defined through market exchange. This vision cannot support a broad conception of data privacy protection. Yet other strands of property theory pose a progressive challenge to the prevailing understanding of property. Together, these alternative approaches might supply the building blocks for a reconceptualization of personally-identified data as differently proprietary.

Labor-desert theory focuses on the right of self-determination and the acquisition of property through the investment of labor.[18] On this theory, I

---

17. *See* JULIE C. INNESS, PRIVACY, INTIMACY AND ISOLATION 102-15 (1992); FERDINAND DAVID SCHOEMAN, PRIVACY AND SOCIAL FREEDOM 14-23, 137 (1992); Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, *in* NOMOS XIII: PRIVACY 1, 3-16 (J. Roland Pennock & John W. Chapman eds., 1971) (discussing privacy in terms of respect for persons); John M. Roberts & Thomas Gregor, *Privacy: A Cultural View*, *in* NOMOS XIII: PRIVACY, *supra*, at 199, 208 (exploring privacy within an indigenous community and its effect on village relationships and individual self-esteem); Ferdinand David Schoeman, *Privacy: Philosophical Dimensions*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY, *supra* note 15, at 1, 14-17; Arnold Simmel, *Privacy Is Not an Isolated Freedom*, *in* NOMOS XIII: PRIVACY, *supra*, at 71, 71-74 (identifying privacy as a cornerstone of the entire structure of human interaction).

18. *See generally* JOHN LOCKE, TWO TREATISES OF GOVERNMENT (Peter Laslett ed., Cambridge Univ. Press 1988) (1690); Wendy J. Gordon, *A Property Right in Self-Expression: Equality*

might "own" the data generated by my actions, and therefore the right to prohibit or condition its use by others. It is hard to see, though, how I would have the right to control what another gathers through his or her own diligence, even if what is gathered is information about me. If the criterion of ownership is effort, I will not always, or even most often, have the superior claim.

Utilitarian theory, meanwhile, takes as its primary purpose maximizing human satisfaction or benefit.[19] Right away, this approach confronts the thorny problem of what constitutes benefit and how to measure it. Latter-day utilitarianism strives mightily to be agnostic on this matter, by defining satisfaction as whatever people choose to pursue, measured in terms of what they are willing to pay.[20] The role of law, and especially property law, is simply to promulgate rules that will facilitate wealth-maximizing transactions.[21] A thing becomes "property"—and appropriately so—when it can be fenced and traded relatively costlessly.[22] On this view, personally-identified information is properly the subject of trade in markets, and I might plausibly claim a right to control the use and disclosure of information about me only to the extent that I can outbid interested third parties.

In practice, labor and utilitarian theories of value overlap substantially to support a vision of human self-determination as bound up with the consensual exchange of property for value. For utilitarians, this conclusion follows straightforwardly from the account of preferences as revealed by behavior. If what people do is the measure of what they want, then mutually-agreed exchanges are definitionally utility-enhancing.[23] For Lockeans, the self-actualization value of trade follows from the investment of property with self. The investment confers a presumptively unlimited right to control the property's disposition; what limits the right devalues the investment.[24] Under either theory, restrictions on the exchange of personally-identified data make little sense.

---

*and Individualism in the Natural Law of Intellectual Property*, 102 YALE L.J. 1533 (1993) (applying Lockean theory to intellectual property).

19. *See generally* Jeremy Bentham, *Principles of Morals and Legislations*, *in* 1 THE WORKS OF JEREMY BENTHAM 1, 1-4, 11-12 (Thoemmes Press 1995) (1843).

20. *See* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 12-15, 568 (4th ed. 1988) [hereinafter POSNER, ECONOMIC ANALYSIS]; RICHARD A. POSNER, THE PROBLEMS OF JURISPRUDENCE 353–92 (1990) [hereinafter POSNER, PROBLEMS].

21. *See* POSNER, ECONOMIC ANALYSIS, *supra* note 20, at 36-39, 271-89; POSNER, PROBLEMS, *supra* note 20, at 357.

22. The classic statement of this approach is Harold Demsetz, *Toward a Theory of Property Rights*, 57 AM. ECON. REV. 347 (1967).

23. *See, e.g.*, C. Edwin Baker, *The Ideology of the Economic Analysis of Law*, 5 PHIL. & PUB. AFF. 3, 32-41 (1975); Margaret Jane Radin, *Market-Inalienability*, 100 HARV. L. REV. 1849 (1987) (describing a vision of universal commodification through market exchange and developing an opposing theory based on the premise that noncommodification serves important human values).

24. *See* Radin, *supra* note 23, at 1888-90.

Coexisting with the dominant liberal market-based understanding of property, however, are a variety of critiques based on an understanding of "property" as fundamentally relational. Under these theories, things deemed property are not defined solely or even primarily by their exchange value, but rather by the ways in which they shape the social relations between and among persons.[25] Several of these more recent strands of property theory offer alternative visions of ownership that might inform the data privacy debate.

Margaret Jane Radin's theory of property for personhood introduces two crucial innovations.[26] The first is the idea that noneconomic or dignitary interests—say, those of a residential tenant—might preclude or restrict the transfer of property by its nominal owner.[27] The second, and far more revolutionary, is that if we think of these possessory interests as "property," we acknowledge the possibility of a wholly new kind of concurrent estate, characterized by overlapping yet ontologically and functionally distinct interests in things owned. Thus, personhood theory might support a dignity-based claim to ownership of one's personal data. Personhood theory, though, seems an odd way of talking about my control over data that others already possess. In this respect information seems fundamentally different than, for example, housing, or wedding rings, or biological organs. Personally-identified information is profligate; it casually escapes direct control. The question is not how to allocate it given its scarcity, but how (or whether) to regulate its abundance.

Here, the respective work of C. Edwin Baker and Joseph Singer complements Radin's approach. Baker carefully disaggregates property into exchange, use, and other values, and argues that not all values or social functions of property deserve the same degree of legal protection.[28] In particular, he singles out the exchange value of property as an appropriate subject of regulation, because control over exchange implicates power over people.[29] Singer, meanwhile, focuses on explicating property's interdependence with social structures of authority and hierarchy.[30] Together, Baker's

---

25. This insight derives, initially, from the work of the Legal Realists. *See* Morris R. Cohen, *Property and Sovereignty*, 13 CORNELL L.Q. 8 (1927); Felix S. Cohen, *Transcendental Nonsense and the Functional Approach*, 35 COLUM. L. REV. 809 (1935).

26. *See* Margaret Jane Radin, *Property and Personhood*, 34 STAN. L. REV. 957 (1982).

27. *See id.* at 992-1002.

28. *See* C. Edwin Baker, *Property and Its Relation to Constitutionally Protected Liberty*, 134 U. PA. L. REV. 741, 762 (1986).

29. *See id.* at 772.

30. *See* Joseph William Singer, *Legal Theory: Sovereignty and Property*, 86 NW. U.L. REV. 1 (1991); Joseph William Singer, *No Right to Exclude: Public Accommodations and Private Property*, 90 NW. U.L. REV. 1283 (1996) [hereinafter Singer, *No Right to Exclude*]; Joseph William Singer, *Re-Reading Property*, 26 NEW ENG. L. REV. 711 (1992). For Singer, the "bundle of rights" approach overlooks these questions. *See* Singer, *No Right to Exclude*, *supra*, at 1301. Yet Baker's

and Singer's approaches suggest a way out of the difficulty generated by an exclusive focus on things possessed by the party claiming a personhood interest. A relational approach to personally-identified data might, but need not, assign "ownership" or control of exchange based on possession. Instead, it might focus on some other consideration, such as (for example) ensuring that the individuals who are data subjects have greater power to control third parties' access to their transactional histories.

Neither Baker's nor Singer's work, however, tells us how we should decide whether personally-identified data (or any other "property") warrants such treatment. Liberal property theory's answer to this question, of course, is that this is precisely what we cannot and should not decide. To divide entitlements formerly perceived as unitary, and to hold nonexchange interests privileged even in transactions between other, consenting parties, smacks of a pernicious collectivism. Impediments to self-interested trade endanger liberty; conversely, a property regime that would promote liberty must facilitate trade.

A different possible answer, though, lies in the work of scholars who have advanced visions of property as facilitating the development of human potential. Frank Michelman, Joan Williams and others articulate an essentially republican vision that emphasizes property's role in ensuring an egalitarian distribution of political power and participation.[31] In addition, Williams identifies a strain of (largely intuitive) theorizing about property that she calls the "liberal dignity" vision. On this view, property rights may not interfere with the basic respect due all persons.[32] Finally, Radin writes more generally of "human flourishing," in terms that encompass both individual and collective goals.[33] Under any of these theories, property is a means to a larger end; it constitutes the individual's stake in society and undergirds society's vision of itself. These theories of property might support restrictions on the exchange of personally-identified data if such restrictions are judged important to the development of community and/or of individuality.

Where does this exploration of property theory leave us? Does a property-theoretic approach to privacy dictate, or privilege, a particular outcome in the data privacy debate? Yes—but not necessarily. Equating "privacy"

---

work, which is explicitly about unbundling, drives toward very similar ends. *See* Baker, *supra* note 28, at 742-43 (arguing that different "sticks" in the bundle have different relational implications).

31. *See* Frank I. Michelman, *Property, Utility, and Fairness: Comments on the Ethical Foundations of "Just Compensation" Law*, 80 HARV. L. REV. 1165 (1967); Joan Williams, *The Rhetoric of Property*, 83 IOWA L. REV. 277 (1998).

32. *See* Williams, *supra* note 31, at 343-52.

33. *See* MARGARET JANE RADIN, CONTESTED COMMODITIES 62-75 (1996); *see also* Martha Nussbaum, *Aristotelian Social Democracy*, *in* LIBERALISM AND THE GOOD 203 (R. Bruce Douglass, Gerald M. Mara & Henry S. Richardson eds., 1990).

with "property" disfavors strong data privacy protection only to the extent that our sense of what can be owned is limited by a platonic ideal of frictionless tradability. Other insights point the way toward a more nuanced understanding of the social and institutional roles of things deemed "property." In particular, they suggest that in some circumstances property might plausibly be defined as a constellation of characteristics to which the mainstream vision gives short shrift: a nonexchange value; a prohibition on trade in "things" too closely intertwined with self; and a sense of property as a requisite for both individual and collective development. I turn now to the question whether it would be good policy to do so.

### C. *Ownership, Liberty, and Friction*

To offer encumbrance as a model for twenty-first century information policy is to risk ridicule on two fronts. To data privacy opponents, such an approach seems laughably retrograde. The prevailing view is that doctrinally as well as theoretically, the modern law of property frowns on encumbrances to trade, and that such restrictions invariably undermine both liberty and efficiency. In fact, though, the argument that property law categorically disfavors encumbrance is far too simple. Legal scholars have catalogued numerous situations in which property law recognizes and enforces such restrictions.[34] In particular, intellectual property law supplies strong precedent for an encumbrance-based model of ownership in personally-identified data. Intellectual property scholars, however, fear that the creation of property rights in personally-identified data may lend support to more general arguments for new intellectual property rights in uncopyrightable facts.[35] But the parallels between intellectual property rights and strong data privacy protection do not require this result. Conceptual similarities between intellectual property and data privacy protection demonstrate, instead, that "liberty" and "efficiency" are not absolutes. The meanings we ascribe to them depend on which burdens we choose to recognize as "costs" and which freedoms we seek to promote.[36]

Within property law generally, intellectual property is the paradigmatic example of encumbered transfer based on substantive policy. One may buy a

---

34. *See* Williams, *supra* note 31, at 329-36, 356-58.

35. *See* Rochelle Cooper Dreyfuss, *Warren and Brandeis Redux: Finding (More) Privacy Protection in Intellectual Property Lore*, 1999 STAN. TECH. L. REV. VS 8 <http://stlr.stanford.edu/STLR/Symposia/Privacy/99_VS_8>; Jessica Litman**,** *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1294-95 (2000); Samuelson, *supra* note 10, at 769-72; Pamela Samuelson, *Privacy As Intellectual Property?*, 52 STAN. L. REV. 1125, 1140-42 (2000); *see also* David G. Post, *Plugging In: Privacy, Property, and Cyberspace*, AM. LAW., Nov. 1997, at 98-99.

36. *Cf.* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 162-63 (1999) ("The difference is in the underlying values that inform, or that should inform, information in each context."). I am indebted to the members of the CyberProf listserv, especially Dan Burk, Peter Swire, and Eugene Volokh, for a colloquy that suggested the analysis developed in this section).

copy of a patented, copyrighted, or trademarked article, but the owner of the intangible asset has rights that travel with the good and restrict its use.[37] This is so for reasons that are explicitly utilitarian (in the more diffuse sense of that term): According creators and inventors these rights promotes progress, and also promotes wider public distribution of intellectual goods.[38] In the case of copyright, these reasons are thought to justify granting authors a substantial degree of "dead hand" control of works.[39]

The trend in intellectual property law and policy, moreover, appears to be toward ever-greater usage restrictions. These restrictions are couched in the language of liberal property theory—they are "licenses" based on preexisting property rights, which confer the greater power of absolute control.[40] Their practical effect, though, is to diminish the freedom of purchasers to use intellectual products as they wish. Indeed, they are valued precisely because they do so, and justified in ways that seem to turn liberal property theory on its head. Thus, for example, we are told that protecting the liberty interests of users of intellectual goods would undermine social welfare,[41] and that it

---

37. *See* 15 U.S.C. § 1114 (1994 & Supp. IV 1998) (providing remedies for trademark infringement); 17 U.S.C. § 106 (1994 & Supp. IV 1998) (delineating exclusive rights in copyrighted works); 35 U.S.C. § 271 (1994 & Supp. III 1997) (providing remedies for patent infringement).

38. *See* Eyal H. Barash, *Experimental Uses, Patents, and Scientific Progress*, 91 NW. U. L. REV. 667, 667-70 (1997); Margaret Chon, *Postmodern "Progress": Reconsidering the Copyright and Patent Power*, 43 DEPAUL L. REV. 97, 98, 104-08 (1993); Niva Elkin-Koren, *Copyright Policy and the Limits of Freedom of Contract*, 12 BERKELEY TECH. L.J. 93, 98-101 (1997); Joseph Fischer, *Harmonization of Federal Patent and Trademark Laws After the* Vornado, Zip Dee *and* Betts *Decisions: An Economic Analysis*, 8 FED. CIRCUIT B.J., Summer 1998, at 29, 43-44; Robert A. Kreiss, *Accessibility and Commercialization in Copyright Theory*, 43 UCLA L. REV. 1, 10-21 (1995); William M. Landes & Richard A. Posner, *An Economic Analysis of Copyright Law*, 18 J. LEGAL STUD. 325, 326-27 (1989); Mark A. Lemley, *The Economics of Improvement in Intellectual Property Law*, 75 TEX. L. REV. 989, 993-99 (1997); Jessica Litman, *The Public Domain*, 39 EMORY L.J. 965 (1990); Albert C. Smith & John W. Burns, *Unethical or Essential*, 8 J. PROPRIETARY RTS. (Oct. 1996). *But see* Glynn S. Lunney, Jr., *Reexamining Copyright's Incentives-Access Paradigm*, 49 VAND. L. REV. 483 (1996) (arguing that society also should consider the opportunity cost created by the copyright regime, measured in terms of other, noncreative activities that might produce greater social welfare); A. Samuel Oddi, *Beyond Obviousness: Invention Protection in the Twenty-First Century*, 38 AM. U.L. REV. 1097 (1989) (arguing that patents should issue only for inventions that would not otherwise be produced).

39. *See* 17 U.S.C. § 302(a) (1994 and Supp. IV 1998) (setting the term of copyright at life of the author plus seventy years); Copyright Term Extension Act, Pub. L. No. 105-298, 112 Stat. 2827, 2827-29 (codified at 17 U.S.C. §§ 301-304 (Supp. IV 1998) (extending certain copyrights by twenty years); *Copyright Term Extension Act of 1995: Hearing on S.483 Before the Senate Comm. on the Judiciary*, 104th Cong. (1995) (statements of Pat Alger, Nashville Songwriters Association International; Shana Alexander; Ginny Mancini; Robert Lissauer; Carlos Santana; Mike Stoller) (arguing that incentives rationale for copyright supported a twenty-year extension of copyright term).

40. *See* Robert W. Gomulkiewicz, *The License Is the Product: Comments on the Promise of Article 2B for Software and Information Licensing*, 13 BERKELEY TECH. L.J. 891 (1998); Raymond T. Nimmer, *Breaking Barriers: The Relation Between Contract and Intellectual Property Law*, 13 BERKELEY TECH. L.J. 827 (1998).

41. *See* PAUL GOLDSTEIN, COPYRIGHT'S HIGHWAY: THE LAW AND LORE OF COPYRIGHT FROM GUTENBERG TO THE CELESTIAL JUKEBOX (1994); Tom W. Bell, *Fair Use vs. Fared Use:*

would be inefficient to require an intellectual property owner to outbid all third parties who wish to use an intellectual product.[42]

The vitality of encumbrance-based models within intellectual property law complicates the account of ownership as negative liberty that is central to liberal property theory. These models remind us that defining the bounds of a property interest always requires choices between liberty claims. The question is not one of freedom versus unfreedom, but of whose freedom to prefer.[43]

In particular, if (some) restrictions on use are good policy in the case of intangible intellectual goods,[44] it is fair to ask why we should presume that restrictions on use of personally-identified data can never be good policy. Certainly, one can posit policy goals that strong data privacy protection might promote. These might include, for example, protection of individual dignity, promotion of personal autonomy, and development of the capacity for meaningful participation in the social and political life of the community. In Part VI, I argue that we should treat these goals as important, and that strong data privacy rights are the best way to promote them. For now, the point is simply that the relative merits of encumbrance and tradability must be assessed in context.

In the case of intellectual property, economic theory supplies a justification for choosing between liberty claims in a manner that imposes (at least some) usage restrictions on recipients of intellectual goods. Intellectual

---

*The Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557 (1998); Jane C. Ginsburg, *Authors and Users in Copyright*, 45 J. COPYRIGHT SOC'Y 1 (1997).

42. *See* Robert P. Merges, *Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations*, 84 CAL. L. REV. 1293, 1306-07 (1996).

43. It is worth remembering that even "dead hand" control of land originally was seen as safeguarding freedom, namely, that of landowners to keep ancestral lands within the family. But the practice interfered with the freedom of heirs to use and transfer land as they pleased. As land came to be valued more and more for its exchange value, a consensus emerged that the balance of freedoms favored the heirs. *See* JESSE DUKEMINIER & JAMES E. KRIER, PROPERTY 282-84 (4th ed. 1998). The enforcement of restrictive covenants, however, cuts the other way: Such covenants disfavor subsequent owners at the expense of original ones, and do so precisely to preserve their intent that land remain dedicated to its original (typically residential) uses. *See* Williams, *supra* note 31, at 284. As Williams demonstrates, the prevailing theory of property as conferring unrestricted rights of use and exchange cannot explain the cases, which seem to rest on a substantive preference for certain uses above others. *See id*.

44. I have argued that, past a certain point, they are not. *See* Julie E. Cohen, Lochner *in Cyberspace: The New Economic Orthodoxy of "Rights Management,"* 97 MICH. L. REV. 462, 538-59 (1998). For purposes of this article, though, whether that is correct is beside the point. The point is that we matter-of-factly invoke the property rights of some to limit the liberty interests of others, and that we do so to effectuate social policy choices. It does not necessarily follow, in other words, that intellectual property and data privacy should be treated the same way. *Cf.* LESSIG, *supra* note 36, at 161-63 (explaining why a particular data management architecture might address societal concerns about data privacy even though it would not address parallel concerns about access to intellectual property). The example of intellectual property shows the plasticity of arguments from liberty and efficiency, not their inevitability.

products have strong public good characteristics, and (at least in theory) would be underproduced without the additional incentives that intellectual property law supplies.[45] Economic theory also indicates, though, that these entitlements should be limited. Copyright's public access and use privileges, for example, play an important role in stimulating further creative efforts, and so produce important social benefits that in turn would be underproduced if authors were granted more complete control.[46] Intellectual property law, in short, seeks the balance of rights and limitations that will best promote the twin goals of progress and widespread public distribution of intellectual goods.[47]

In the case of personally-identified data, economic theory similarly favors allocating ownership rights to the individuals who are in some sense the "creators" of the data, but for very different reasons. Incentives play little role in the analysis; personally-identified data is not scarce.[48] Instead, because bargaining over initial entitlements is not costless, economic theory indicates that the property right should be assigned initially to individuals, who would incur higher costs to bargain for it.[49] Nor is there a compelling need to encourage the production of *collections* of personally-identified data. Unlike traditional intellectual goods, these databases have no significant public good characteristics. Instead, they are the paradigmatic example of a good whose entire value is privately appropriable, and whose creation therefore requires no additional public subsidy.[50]

---

45. *See, e.g.*, Elkin-Koren, *supra* note 38, at 98-100; William W. Fisher III, *Reconstructing the Fair Use Doctrine*, 101 HARV. L. REV. 1659, 1700-04 (1988); Landes & Posner, *supra* note 38, at 326-33. *But see* Stephen Breyer, *The Uneasy Case for Copyright: A Study of Copyright in Books, Photocopies, and Computer Programs*, 84 HARV. L. REV. 281 (1970) (arguing that abolishing copyright law would not substantially affect incentives for book production); Gillian K. Hadfield, *The Economics of Copyright: An Historical Perspective*, 38 COPYRIGHT L. SYMP. (ASCAP) 1, 14 (1988) (suggesting that "much of the perceived need for protection in early analyses in fact arose from or was reinforced by the fact of large 'economies of scale' in publishing (augmented by high levels of uncertainty) rather than the 'public goods' problem . . . .").

46. *See* Cohen, *supra* note 44, at 542-51; Landes & Posner, *supra* note 38, at 332-33, 347-53; Lemley, *supra* note 38, at 1056-58; Lydia Pallas Loren, *Redefining the Market Failure Approach to Fair Use in an Era of Copyright Permission Systems*, 5 J. INTELL. PROP. L. 1, 49-56 (1997).

47. *See* U.S. CONST. art. I, § 8, cl. 8; Cohen, *supra* note 44, at 542-51; Elkin-Koren, *supra* note 38, at 98-101; Kreiss, *supra* note 38; Landes & Posner, *supra* note 38, at 326-37; Lemley, *supra* note 38, at 993-99; Litman, *supra* note 38.

48. Without question, the possibility of monitoring or profiling may affect incentives to engage in certain *types* of transactions or activities. *See* notes 188-230 *infra* and accompanying text. But with the possible (though apocryphal) exception of the hermit on the mountaintop, everyone transacts.

49. *See* Ronald Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960); *see also* DANIEL W. BROMLEY, ECONOMIC INTERESTS AND INSTITUTIONS: THE CONCEPTUAL FOUNDATIONS OF PUBLIC POLICY 118-21, 134-43, 165-81 (1989) (illustrating that different initial entitlement structures lead to different equilibrium points).

50. *See* Jack Hirshleifer, *The Private and Social Value of Information and the Reward to Inventive Activity*, 61 AM. ECON. REV. 561 (1971). Arguably, collections of personally-identified data have public-good characteristics to the extent that they enable vendors to allocate goods and

Here, the liberal property rights tradition offers a different efficiency-based objection to proposals for granting individuals *ongoing* ownership rights in personally-identified information. Citing the cost of negotiating and enforcing ongoing data protection provisions, data privacy opponents argue that increased protection would impose unreasonable costs on routine consumer transactions—costs that consumers themselves ultimately will have to bear.[51] Thus, even assuming that greater data privacy protection is desirable for reasons related to personal dignity, they contend that the social costs of enhanced privacy would be too great. Implicitly, this argument rests on a liberty claim as well. "Unnecessary" transaction costs are a species of indirect restraint on liberty; imposing them would offend the principle that laws about "property" should facilitate trade.

Again, though, the example of intellectual property shows that the relationships between friction and social benefit, and between friction and liberty, are more complicated than mainstream property theory suggests.[52] Current trends in copyright law and theory favor the adoption of digital tech-

---

services to those consumers who want them (and are able to pay) the most. As Part III B discusses, though, targeted marketing doesn't just seek to satisfy existing desires; it seeks to create new ones. To a substantial degree, these desires are "relative preferences"—preferences for the satisfaction gained by improving one's (consumptive) lot relative to others. Fulfillment of relative preferences generates no net increase in social utility; if anything, it decreases social utility by fueling zero-sum spending races and by diverting resources from the satisfaction of other wants. *See* Viet D. Dinh, *Forming and Reforming Wants*, 85 GEO. L.J. 2121, 2130 (1997).

Collections of data gathered from individuals also may have public good characteristics when they are generated and used to support socially valuable research. These cases, however, are distinguishable from those in which the databases are pure private goods by the fact that the data gathered and disseminated purely for research need not remain personally-identifiable. At most, then, the public goods argument would support drafting a privacy rule that treats the two sorts of databased differently. *See* text accompanying notes 207-215 *infra*. In addition, there are other ways to encourage the creation of databases for research. *See generally* Brett Frischmann, *Innovation and Institutions: Rethinking the Economics of U.S. Science and Technology Policy*, 24 VT. L. REV. 347 (2000) (discussing grant funding and tax incentives). Whether data processors should be entitled to any legal protection for existing, already-created databases is a separate question, which this article does not address.

51. *See* SOLVEIG SINGLETON, PRIVACY AS CENSORSHIP: A SKEPTICAL VIEW OF PROPOSALS TO REGULATE PRIVACY IN THE PRIVATE SECTOR (Cato Inst. Policy Analysis No. 295, 1998); *see also* Simon G. Davies, *Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 143, 161 (Philip E. Agre & Marc Rotenberg eds., 1997) ("The cost factor is a powerful weapon in the armory of privacy invaders because it implies that a few 'fundamentalists' will force a rise in the production cost of an item of a service."). *But see* Laudon, *supra* note 12, at 102-03 (noting and rejecting this argument).

52. It is equally clear that traditional property law is comfortable imposing heightened transaction costs in some contexts. Again, restrictive covenants supply an easy example; allowing initial landowners to impose use restrictions creates substantial information and renegotiation costs for subsequent owners. The cases largely avoid consideration of costs by relying on the fiction of notice implied from the circumstances, even though the range of circumstances recognized as legally sufficient is so great as to give even the most savvy purchaser pause. *See* Williams, *supra* note 31, at 356-58.

nologies that enforce usage restrictions for digital works.[53] From a technological standpoint, personal data encumbered with usage restrictions are no different than digital works similarly encumbered. Yet digital "rights management" technologies have not encountered transaction cost objections; indeed, quite the opposite is true. Intellectual property owners and many legal commentators argue that rights management technologies will reduce the transaction costs that attend the licensing of intellectual products.[54]

Library, educational, and consumer groups, meanwhile, have objected that technologically-enforced usage restrictions impose new and unwarranted burdens on users of copyrighted works.[55] This objection to digital rights management technologies is not perceived (or presented) as an objection to costs. But plainly it is; the new technologies are designed to impose new transactional barriers to uses formerly available without negotiation or charge.[56] Plainly too, the objection is about more than costs: Opponents of digital rights management technologies argue that allocating the "costs" of privileged uses to authors, and through them to society at large, serves important social values—values that would not be served to the same extent by requiring all would-be users to pay for all uses.[57] It is hard to escape the conclusion that the identification of particular costs as "friction" to be eliminated depends on other, normative considerations.

And so, in one sense, the intellectual property and data privacy debates are not inconsistent at all. A world with ongoing usage restrictions for intellectual property, but not for personally-identified data, is a world in which the liberty claims of individuals count for less than those of publishers and data processors, and in which the social benefits (or efficiencies) arising

---

53. *See* Digital Millennium Copyright Act, Pub. L. No. 105-304 (1998) (codified as amended at 17 U.S.C. §§ 1201-05 (1999)); CHRISTOPHER BURNS, INC., COPYRIGHT MANAGEMENT AND THE NII: REPORT TO THE ENABLING TECHNOLOGIES COMMITTEE OF THE ASSOCIATION OF AMERICAN PUBLISHERS (1995); INFORMATION INFRASTRUCTURE TASK FORCE, UNITED STATES, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, 230-34 (1995); PETER WAYNER, DIGITAL COPYRIGHT PROTECTION (1997); Bell, *supra* note 41; Mark Stefik, *Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing*, 12 BERKELEY TECH. L.J. 137 (1997); IMPRIMATUR, *Project Documents* <http://www.imprimatur.alcs.co.uk/final/>.

54. *See, e.g.*, GOLDSTEIN, *supra* note 41, at 170, 224; Bell, *supra* note 41, at 581-84; Robert P. Merges, *The End of Friction? Property Rights and Contract in the "Newtonian" World of On-Line Commerce*, 12 BERKELEY TECH. L.J. 115, 130-34 (1997); Stefik, *supra* note 53, at 146-47.

55. *See Hearing on H.R. 2281 & 2280 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong. (1997) (statement of Douglas Bennett, President, Earlham College, on behalf of the Digital Future Coalition); Digital Future Coalition, *Collected Position Papers, Letters, and Press Releases* <http://www.dfc.org/>.

56. *See* Cohen, *supra* note 44, at 471-73.

57. Proponents of digital rights management technologies argue that costs placed on authors and publishers will be passed through to consumers. This is clearly right—but it does not follow that costs will be borne by the same people, in the same proportions. *See id.* at 498-504, 542-51, 556-59.

from market-encumbrance are deemed less valuable than those arising from trade. But the inequality that flows from the data privacy debate is even more profound. Even absent ongoing usage restrictions, an initial allocation of entitlements in personally-identified information to data processors shifts enormous wealth away from individuals, and does so without even acknowledging the shift, much less offering any tenable justification.[58]

Juxtaposing the data privacy debate with the politics of intellectual property thus exposes an ideological fault line within the transaction costs approach to designating property interests. The designation as "transaction cost" has political valence. Decisions to retain (or increase) some costs and eliminate others may be decisions about cost (and wealth) allocation as well. Moreover, some costs may have instrumental or production value that outweighs the short-term loss they impose.[59] In the case of data privacy, we might conclude, for example, that placing some cost burden on processors and users of personally-identified data promotes greater respect for individual dignity than requiring individuals to purchase their privacy against a default rule of no-privacy. Under one allocation, the costs of privacy are borne by society generally; under the other, the costs are borne by those individuals who both desire privacy and can afford it (and the costs of no-privacy are borne by everyone else). The two outcomes are not equivalent, and we cannot choose between them based on an abstract injunction to "minimize costs."

The point sharpens where digital information systems are concerned. As the example of intellectual property suggests, the belief that encumbrance inevitably trades against efficiency is simplistic. Transaction costs are a function of system design, and system design, in turn, is based on socially-determined conceptions of efficiency.[60] Thus far, whether deliberately or by oversight, we have constructed data processing systems that do not involve the individual in decisionmaking about the uses of data collected by the system.[61] Yet the same technologies that enable distributed rights-management functionality might enable the creation of privacy protection that travels with data—obviating the need for continual negotiation of terms, but at the same time redistributing "costs" away from the individuals who are data subjects.

---

58. *See* Paul Farhi, *Me Inc.: Getting the Goods on Consumers*, WASH. POST, Feb. 14, 1999, at H1 (arguing that marketing researchers doing phone surveys are getting "something for nothing"); Laudon, *supra* note 12, at 99.

59. *See* Cohen, *supra* note 44, at 542-51, 559-59; Pierre Schlag, *The Problem of Transaction Costs*, 62 S. CAL. L. REV. 1661 (1989).

60. *See* Philip E. Agre, *Beyond the Mirror World: Privacy and the Representational Practices of Computing*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE, *supra* note 51, at 29; Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE, *supra* note 51, at 125.

61. *See* Burkert, *supra* note 60, at 137.

Whether we should do so depends on whether this allocation of costs is the best one.

* * * *

Property talk about data privacy creates both risk and opportunity. Property rights effectuate policy choices; at the same time, though, property rhetoric may seem to privilege certain choices above others. Recognizing property rights in personally-identified data risks enabling more, not less, trade and producing less, not more, privacy. But defining these rights, instead, in terms of encumbrance, along the general lines suggested by the intellectual property model, offers the possibility of a privacy paradigm that returns fine-grained, ongoing control to the individual. The perceived opposition between strong data privacy and property is part ideology and part technological artifact. Current systems for processing transactions are designed to facilitate a one-time surrender of control over personal information, but they need not be. Within particular system parameters—which are in turn a function of social parameters that define acceptable information policy—ownership can be both "sticky" and efficient. The design of such systems is a matter of choice. Next to consider, then, is how we should choose.

## III. CHOOSING

The data privacy debate is also a debate about freedom of choice and its necessary preconditions. The prevailing approach to this question is closely aligned with the position that personally-identified data becomes "property" when, and because, it becomes tradable: A successful data privacy regime is precisely one that guarantees individuals the right to trade their personal information for perceived benefits, and that places the lowest transaction cost barriers in the way of consensual trades. If individuals choose to trade their personal data away without placing restrictions on secondary or tertiary uses, surely it is their business.[62] On this view, choice rather than ownership is (or should be) the engine of privacy policy. What matters most is that personal data is owned at the end of the day in the manner the parties have agreed.

Theories of privacy-as-choice, however, do not seem to contemplate the exercise of this freedom in nonmarket realms. "Choice" is something that occurs within existing constraints but not about them. This Part considers whether that is necessarily so—whether, in other words, there is something about that sort of choice that makes it the freest.

---

62. *See* SWIRE & LITAN, *supra* note 13; Peter P. Swire, *Markets, Self-Regulation and Government Enforcement in the Protection of Personal Information*, *in* U.S. DEPT. OF COMMERCE, PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (1997) [hereinafter Swire, *Markets*] <http://www.osu.edu/units/law/swire.htm>.

### A. *Theories and Technologies of Choice*

Adherents of the privacy-as-choice model contemplate that as data privacy becomes more important to consumers, privacy preferences and practices will become specified contractual terms in most ordinary online interactions.[63] To make this a concrete possibility, technology companies have invested heavily in the development of technologies for managing data privacy preferences. In theory, these technologies, most notably the World Wide Web Consortium's Platform for Privacy Preferences ("P3P"), will allow individuals to create tailored profiles that specify permitted and prohibited uses of their personal data.[64] The profiles will act as digital passports that negotiate privacy terms with vendors' websites. If the vendor offers less privacy protection than the individual wants, the profile will alert the individual and offer the option to transact on the vendor's terms.[65]

Like the justifications for property ownership discussed in Part II.B,[66] the theoretical antecedents of a data privacy regime based on "freedom of choice" mingle strands of Lockean and utilitarian libertarianism. Under utilitarian theory—especially in its economic incarnation—market exchanges reflect the expression and satisfaction of preferences.[67] Definitionally, market exchange makes people better off; it follows that the law should seek to maximize opportunities to make data privacy practices the subject of exchange. From Lockean theory, meanwhile, comes an emphasis on self-determination through freedom from limits on the accumulation and disposition of property. The disposition right is inseparably linked with the accumulation right.[68] Conversely, then, interference with exchange reduces the

---

63. *See* LESSIG, *supra* note 36, at 159-63.

64. *See* Joseph Reagle & Lorrie Faith Cranor, *The Platform for Privacy Preferences*, COMM. ACM, Feb. 1999, at 48, 48 (arguing that websites can bolster users' confidence by clarifying their privacy policies upfront and allowing visitors to become active participants in the decisionmaking process). For websites providing customers with information about tools for construction of their own privacy profiles see, e.g., W3C, *The Platform for Privacy Preferences 1.0 (P3P 1.0) Specification* <http://www.w3.org/TR/P3P>; SuperProfile, *What Is a Superprofile* <http://www.superprofile.com/sprofile.html>; Privaseek, *Privacy Tools* <http://www.privaseek.com>. In fact, as privacy experts have documented, the P3P project has experienced numerous delays, in part because industry sponsors have been unable to reach consensus on the level of privacy protection to enable. *See* Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 778-79 (1999); Marc Rotenberg, *What Larry Doesn't Get: Fair Information Practices and the Architecture of Privacy*, 2000 STAN. TECH. L. REV. ¶¶ 63-66 (2000) <http://stlr.stanford.edu/STLR/Working_Papers/00_Rotenberg_1>.

65. *See* Reagle & Cranor, *supra* note 64, at 49; *see also Online Privacy Alliance*, (Sept. 20, 1999) <http://www.privacyalliance.com/resources/rulesntools.shtml> (discussing different types of privacy tools and privacy "infomediaries").

66. *See* notes 18-33 *supra* and accompanying text.

67. *See* NICHOLAS MERCURO & STEVEN G. MEDEMA, ECONOMICS AND THE LAW: FROM POSNER TO POST-MODERNISM 13-18, 57-60 (1997).

68. Locke himself recognized two sorts of limits on the freedom to accumulate: One must not accumulate property only to waste it, and one must leave "enough, and as good . . . for others."

accumulation incentive; it follows that the law should not prevent individuals from managing their own wealth.

The privacy-as-choice model differs in some respects from the property-rights approach explored in Part II.C above.[69] The model implicitly concedes initial ownership to individuals. At the same time, however, it presumes both the ability and the desire to alienate personal information (on the right terms), and thus devalues the argument that ownership necessarily includes the right to assert ongoing control. Ongoing control exists only as a matter of contract, and only to the extent that the data processor is willing to agree. Nor is there any serious discussion of digitally self-enforcing access and usage rights, which might create ongoing control on a de facto basis. (One suspects that it is no coincidence that the "transaction cost" objection to data privacy management plays a much less significant role in discussions of privacy-as-choice.) Instead, the contract model relies on self-enforcement of privacy practices by vendors themselves. Dishonest vendors, the reasoning goes, will lose credibility and market share.[70]

The theory of privacy-as-choice predicts that, eventually, the technologically-mediated market for a given product or service will reach an equilibrium based on the privacy practices that most consumers prefer.[71] If, for example, most consumers prefer that their credit card companies or magazine publishers make their names and addresses available to "selected" purveyors of other products and services, the status quo will remain the norm. If most consumers prefer no data-sharing, then that practice will prevail. If enough consumers, or enough profitable consumers, prefer something different, a smaller market will evolve to serve them as well.

It seems churlish to contest this rosy vision of a market for privacy, or to argue that we should expect more choice, or different kinds of choice, than the market will provide. Economic and political theorists, however, recognize that choice is both more constrained and more complicated than theories of privacy-as-choice would suggest. Choice occurs within parameters. Some of these parameters, such as the fact that we need gravity to walk and oxygen to breathe, are relatively fixed. Others, such as the design of legal

---

LOCKE, *supra* note 18, at §§ 27, 31. He resolved both limits by positing freedom of exchange. Trading perishable commodities for imperishable currency avoids waste, and transfers perishables to those who need them. *See id.* at §§ 46-48. The background conditions that supported this reasoning have changed substantially since Locke's day, but the belief that markets cure distributional inequities has not. For a persuasive critique of the linkage between accumulation and disposition of property, see Baker, *supra* note 28.

69. *See* notes 34-61 *supra* and accompanying text.

70. *See* Swire, *Markets*, *supra* note 62; *cf.* Paola Benassi, *TRUSTe: An Online Privacy Seal Program*, COMM. ACM, Feb. 1999, at 56. Swire distinguishes between two versions of this model: "pure market" and "self-regulation" by formal and informal industry associations. Under either version, though, the discipline is supplied by market entities rather than by law.

71. *See* LESSIG, *supra* note 36, at 159-63.

institutions and technological tools, are slightly more malleable; they are, in other words, themselves the subject of choices.[72] The debate about privacy and freedom of choice is, in fact, two debates—one about the conditions of choice within a given set of institutions or parameters (here, the evolving, relatively unregulated market for personally-identified data), and one about the parameters themselves. And if "freedom of choice" includes the freedom of self-determination writ large, then it necessarily includes the freedom to use nonmarket means to change the parameters within which markets operate. The question is whether it would be desirable to do so.

Economic and political markets offer different constraints. Adherents of market choice argue that nonmarket choices constrain nonsubscribers, while market choices do not. One may be bound by a choice inconsistent with one's own vote and, presumably, with one's own preferences or views about self-determination. In markets, by contrast, one may trade or not trade as one pleases. Thus, some argue that substantive regulation of transaction terms is inherently freedom-destroying.[73] But of course third-party constraints do obtain in markets—if one has unusual tastes or belongs to a customer group perceived as fickle or unprofitable, one may be limited to product offerings designed for others' preferences.[74] One constraint is no more neutral than the other; they are simply different. Social policy generally reflects some combination of the two. In our culture, for example, it is usually unacceptable to impose nonmarket constraints on speech—but that decision was and is a political one.

Economic and political markets also offer different freedoms. Economic markets are, generally speaking, a good forum for the expression and satisfaction of purely consumption-related preferences. They are, however, a much poorer forum for expression and satisfaction of second-order preferences about the sorts of behavior the law should encourage or discourage.[75] They are also a poor forum for the resolution of issues that we as a society believe, either for reasons of market failure or for normative reasons, should

---

72. *See* BROMLEY, *supra* note 49; LESSIG, *supra* note 36; *see also* Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661 (1998).

73. *See* SINGLETON, *supra* note 51; Solveig Singleton, *Reviving a First Amendment Absolutism for the Internet*, 3 TEX. REV. L. & POL'Y. 279 (1999) [hereinafter Singleton, *Reviving*]; *cf.* Bell, *supra* note 41, at 607-08 (arguing that copyright fair use doctrine resembles a contract of adhesion if it constrains private contracts).

74. *See* BROMLEY, *supra* note 49, at 65-66.

75. *See* G. PETER PENZ, CONSUMER SOVEREIGNTY AND HUMAN INTERESTS 41-58 (1986); Cass R. Sunstein, *Disrupting Voluntary Transactions*, *in* NOMOS XXXI: MARKETS AND JUSTICE 279, 285-87 (John W. Chapman & J. Roland Pennock eds., 1989); Cass R. Sunstein, *Legal Interference with Private Preferences*, 53 U. CHI. L. REV. 1129, 1133-35, 1140-45 (1986).

be decided based on votes rather than dollars.[76] Political markets perform precisely this function.

Finally, economic and political markets suffer from different dysfunctions. Market failure may arise from disparities of power, from high or unevenly distributed bargaining costs, from failure to absorb negative externalities (or to reproduce positive ones), or from information asymmetries that preclude the exercise of informed choice.[77] The mechanisms for exercising freedom of choice in political markets, in turn, are subject to collective action problems and interest group corruption.[78] Public choice theory tells us that there will be substantial overlap between economic and political outcomes, and plainly this is correct. Plainly too, though, there are occasions when the different bases for decisionmaking in economic and political markets may translate into different results.[79]

Inescapably, then, selection of the forum for choice about data privacy depends (at least in part) on the nature of the policy sought to be implemented. A substantive preference for trade in personally-identified information is more easily implemented in economic markets. A substantive preference for durable privacy, or for privacy as to certain items of information, may be more easily or effectively implemented in political ones. Before we can decide (or even decide how to decide), we must assess whether privacy-as-choice will guarantee durable privacy for those who prefer it.

### B. *Choice, Parameters, and Tradeoffs*

The privacy-as-choice model is conceived as empowering individuals.[80] Whether that is true, however, depends on the baseline for comparison.

---

76. *See* Cohen, *supra* note 44, at 552-55; Victor P. Goldberg, *Institutional Change and the Quasi-Invisible Hand*, 17 J.L. & ECON. 461, 481 (1974); Herbert Hovenkamp, *Legislation, Well-Being, and Public Choice*, 57 U. CHI. L. REV. 63 (1990); Richard H. Pildes & Elizabeth S. Anderson, *Slinging Arrows at Democracy: Social Choice Theory, Value Pluralism, and Democratic Politics*, 90 COLUM. L. REV. 2121 (1990); Maxwell L. Stearns, *The Misguided Renaissance of Social Choice*, 103 YALE L.J. 1219 (1994).

77. *Cf.* ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 38-41 (3d ed. 2000). The differences between my formulation and the textbook definition are deliberate. Elsewhere, I have shown that "market power" is not the only kind of power that matters in markets, and that the expansion of markets to absorb formerly uncompensated positive externalities may decrease overall social utility rather than enhancing it. *See* Cohen, *supra* note 44, at 517-51.

78. *See* MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS 2 (1965) (arguing that rational self-interested individuals will not act to achieve their common group interets); JAMES M. BUCHANAN & GORDON TULLOCK, THE CALCULUS OF CONSENT: LOGICAL FOUNDATIONS OF CONSTITUTIONAL DEMOCRACY (1962); THE POLITICAL ECONOMY OF RENT-SEEKING (Charles K. Rowley, Robert O. Tollison & Gordon Tullock eds., 1988).

79. *See* DANIEL A. FARBER & PHILIP P. FRICKEY, LAW AND PUBLIC CHOICE: A CRITICAL INTRODUCTION (1991); DONALD P. GREEN & IAN SHAPIRO, PATHOLOGIES OF RATIONAL CHOICE THEORY: A CRITIQUE OF APPLICATIONS IN POLITICAL SCIENCE (1994).

80. *See* LESSIG, *supra* note 36, at 159-63.

Plainly, the model would give individuals more power over uses of their personal data than they currently enjoy. At the very least, P3P and similar technologies might supply a reliable, automatic means of communicating privacy preferences to vendors, where none now exists. It seems difficult to dispute that a system based on accurate information and routinized use of P3P-type profiles would offer some advantages compared with current commercial practice, which affords individuals no enforceable data privacy protection. If we are serious about choice, though, we also must consider the structural choices that privacy-as-choice forecloses. In addition, we must consider the economic and political consequences of a choice to restrict choice about data privacy to the marketplace.

Freedom of choice in markets requires accurate information about choices and their consequences, and enough power—in terms of wealth, numbers, or control over resources—to have choices.[81] The privacy-as-choice model reinforces persistent inequalities on both counts.

First, to assess the benefits and costs of a trade accurately, individuals must understand the uses contemplated for the information they are asked to disclose.[82] Proponents of "choice" as the basis for privacy policy differ on exactly how this is best accomplished. Some advocate greater regulation of privacy disclosures; others argue that the same market principles that produce privacy also will foster disclosure.[83] All agree, though, that digital network technologies enable easy disclosure of privacy policies and practices at a far greater level of detail than feasible in off-line transactions.

In reality, individuals face enormous difficulty assessing how their personal information will be used.[84] The decision about how much information a privacy policy should provide is hotly contested. The problem is especially acute for secondary and tertiary uses of personally-identified information. Routine practice is to specify these classes of recipients only in the most

---

81. In theory, choice exists as long as the individual can refuse the transaction. I am concerned here, however, with options beyond the choice to accept or reject the lowest-priced, most privacy-invasive offer.

82. *See* COOTER & ULEN, *supra* note 77, at 38-41 (listing information asymmetry among the causes of market failure).

83. *Compare* Kang, *supra* note 13 (advocating statutorily required disclosures), *with* SWIRE & LITAN, *supra* note 62 (advocating industry self-regulation), Swire, *Markets*, *supra* note 62 (same), and Individual Reference Service Group, *White Paper* (Dec. 1997) <http://www.irsg.org/html/white_paper.htm> (same).

84. For a thorough and illuminating exploration of the information problems and other costs that confront individuals seeking to protect their privacy, see Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033 (1999); *see also* Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 47-51 (1997) (discussing information problems that confront health care consumers).

general terms.[85] Yet without information about the nature and identity of secondary and tertiary users, individuals cannot easily determine what information to provide or withhold.

Even assuming perfect information about all contemplated reuses of data, however, consumer freedom is relative. Individual consumers are free to accept or reject the terms offered, but it is the vendor who is free to decide what terms to offer in the first place.[86] Thus, consumers may discover that the surrender of personal information is nonnegotiable or prohibitively priced. At this point, the P3P model simply assumes the transaction will fail. But to the extent that individuals need or want the goods or services and cannot obtain them elsewhere—to the extent, that is, that all vendors serving a given market believe collecting consumer data is a competitive necessity—one suspects that individuals may simply concede, and convince themselves that the loss of privacy associated with this particular transaction is not too great.

The present valuation placed on any given surrender of personally-identified information is, of course, also a matter of personal choice. Yet it is difficult to assess the future significance of a loss of privacy, much less to compare that future harm with a currently offered benefit. In part, this is due to the information problems discussed above. In part, though, the disability is cognitive. Estimating probability-weighted future value and discounting for present value are hard, and people are demonstrably bad at it.[87] The valuation problem is compounded by the fact that the trivial and incremental character of each loss—information about a grocery purchase here, a magazine subscription there—tends to minimize its ultimate effect.[88] A comprehensive collection of data about an individual is vastly more than the sum of its parts.

---

85. *See, e.g.*, *Clickrewards* <http://www.clickrewards.com/>; *Disney.com* <http://www.disney.go.com/>; *FTD.com* <http://www.ftd.com/>; *Sony.com* <http://www.sony.com/>; *Travelcity.com* <http://www.travelocity.com>; *Varsitybooks.com* <http://www.varsitybooks.com/>; *1-800-flowers.com* <http://www.1800flowers.com/>.

86. *See* BROMLEY, *supra* note 49, at 65-66; Cohen, *supra* note 44, at 518-33; Goldberg, *supra* note 76, at 483-91 (discussing institutional advantages enjoyed by firms in setting standardized contract terms); *cf.* Kenneth Lee & Gabriel Speyer, *White Paper: Platform for Privacy Preferences Project (P3P) & Citibank* (1998) <http://www.w3.org/P3P/Lee_Speyer.html> (noting problems that P3P-enforced variety of user preferences may pose for organization accustomed to standardized practices).

87. For a good summary of the cognitive phenomena that distort assessment of risk in commercial transactions, see Larry T. Garvin, *Adequate Assurance of Performance: Of Risk, Duress, and Cognition*, 69 U. COLO. L. REV. 71, 140-70 (1998).

88. *Cf.* Froomkin, *supra* note 3, at 492 ("[A]s long as in each individual transaction the cost of not providing the information is disproportionate to the loss (which is a function of the cumulation of the transactions, not any single transaction) a property rights approach appears unlikely to have much real influence on database creation.").

More fundamentally, the privacy-as-choice model assumes that data privacy can be valued using market measures. But monetary measures of value do not capture the very real incommensurabilities that the choice presents. Privacy, like other dignity-related goods, has inherently nonmonetizable dimensions.[89] These dimensions may be lost or distorted beyond recognition in the translation to dollars and cents.

A final set of objections to the privacy-as-choice model is based on distributive justice concerns. Self-evidently, an important determinant of choice within markets is wealth. If data privacy costs money—or, conversely, if surrendering privacy saves money—access to privacy will be more unequal than if it did not. Under a regime of tradable privacy rights, "privacy" simply will become a status that can be chosen (and paid for) the way one might choose a neighborhood, a health club, or a brand of automobile.

Of course, it isn't quite that simple—marketers would rather have your data if you're rich than if you're poor. Thus, marketers are likely to spend extra money to identify wealthier customers and recruit them to loyalty programs that offer incentives for repeat shoppers.[90] A perverse consequence of a purely market-based approach to data privacy rights, then, may be more discounts for the rich. If so, then the poor will lose twice over. They will have less privacy, and they will also pay more for goods and services than more desirable customers. Privacy in markets, then, is more than a luxury. Personally-identified data is the wedge that enables "scientific," market-driven, and increasingly precise separation of "haves" from "have-nots."[91]

Relatedly, the privacy-as-choice model ignores that some (perhaps most) uses of personally-identified data do not involve offers of discounts. Consumer data can be used for many purposes to which consumers might not so blithely agree: employment decisions and classifications by health insurance providers that exclude or disadvantage genetic or medical "have-nots"; employment or housing decisions based on perceived personality risks; employment or housing decisions based on sexual or religious preferences; and so on.[92] Data processors have no particular interest in disclosing these uses, precisely because individuals are likely to find them so objectionable. And even many privileged individuals might not wish to trade their own privacy

---

89. *See* MARGARET JANE RADIN, CONTESTED COMMODITIES 74-94 (1996).

90. *See, e.g.*, Pamela Klein, *Malls Market Customer Base*, CHI. TRIB., Nov. 11, 1998, sec. 3, at 1 (discussing the willingness of credit card companies like Visa USA to pay large sums of money to talk to shoppers in malls); John Schwartz, *The Price We Pay: When Everything's up for Grabs, True Value Is Hard to Find*, WASH. POST, June 27, 1999, at B1 (describing how Home Depot identifies wealthy customers based on demographics and zip code and sends those customers coupons directly by mail).

91. *See* OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION 53-94 (1993).

92. *See* Schwartz, *supra* note 84, at 25-41; GANDY, *supra* note 91, at 75-76.

for the supposed advantages that privilege would confer; who knows, after all, to what uses seemingly innocuous information might be put in the future?

To a substantial degree, then, the rhetoric of "choice" obfuscates the political choice that current data privacy policy represents. The data privacy debate is not merely, or even mostly, about the satisfaction of consumer preferences as expressed in the direct market for goods and services. Like the rhetoric of "transaction costs," the emphasis on "choice" conceals the degree to which the model predetermines who chooses.[93] In particular, with respect to secondary uses of personally-identified data, the "choice" that the model protects is not choice by individuals. It is the choice of data processors about how to classify individuals, and for what purposes.

To object that these structural inequalities—the reactive nature of consumer freedom, income disparities, and the like—are beyond the scope of the problem is to miss the point. In any serious discussion of what constitutes choice about privacy, perceived failures of markets are precisely the issue. The design of markets, and whether to delegate resolution of particular questions to them, are themselves choices.[94]

The elusiveness of this point within the mainstream data privacy debate suggests that, like "property," "choice" has become a category with a specific, culturally determined meaning. "Freedom of choice" means "choice in markets," and means only that. In a provocative essay on the evolution of governance structures, Larry Lessig observes that we have lost faith in other, more traditional institutions of governance.[95] But it seems to me that the phenomenon is cognitive as much as existential: We conceive of "freedom" in literal, almost physical terms, as a function of direct or subjective constraints on behavior.[96] Law, of course, does not directly constrain in most instances; nor, I would argue, does it constrain more directly than price in many cases. Yet law operates in terms of prohibition, while markets operate in terms of possibility. And so liberty has come to mean freedom from laws (other than economic ones) rather than freedom that laws might guarantee.

It was not always thus. As Eric Foner shows, liberty has meant many things at different times in our history.[97] At times, it has meant a simple,

---

93. *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1660-62 (1999) (characterizing this aspect of the privacy-as-choice model as the "autonomy" trap).

94. *See* Jean Braucher, *Contract Versus Contractarianism: The Regulatory Role of Contract Law*, 47 WASH. & LEE L. REV. 697 (1990); Cohen, *supra* note 44, at 549-55; Goldberg, *supra* note 76, at 468 n.15, 484-91; *cf.* BROMLEY, *supra* note 49, at 118-21, 134-43, 165-81 (demonstrating that the efficient equilibrium point in an economic system depends on the initial choice of entitlement structure).

95. *See* Lawrence Lessig, *Governance* (1998) (draft 3.01) <http://cyber.law.harvard.edu/works/lessig/cpsr.pdf>.

96. *Cf.* Lessig, *supra* note 72, at 677-80 (discussing the difference between subjective, or perceived, constraints and objective ones).

97. *See* ERIC FONER, THE STORY OF AMERICAN FREEDOM (1998).

literal "libertarianism"; at other times, though, it has meant the freedom to strive toward shared moral or existential ideals.[98] As I will argue in Part VI.A,[99] data privacy protection furthers still another sort of liberty—that of self-determination, expressed through the power to define oneself to the world in the way one wishes. The conventional wisdom is that such affirmative liberty claims are weaker and less principled than negative liberty claims.[100] Yet assuming this is so, the affirmative formulation is easily reframed in the negative: Data privacy ensures liberty to preclude certain types of probabilistic judgments about one's inclinations, abilities, or shortcomings. And thus reframed, it is difficult to see why this sort of self-interested choice is less deserving of protection.

Here, data privacy opponents object that limiting markets in personally-identified data will affect the range of other choices available to consumers within markets. The "attention economy," we are told, demands personal profiling as a survival tactic.[101] Vendors that are unable to exploit consumer profiles to target their products and services effectively will be forced, instead, to discontinue narrowly-targeted product offerings and/or charge higher prices for continued offerings. The effects, we are told, will be especially stark where targeted advertising has traditionally supported free or near-free content—e.g., in the news and broadcast industries.[102] Yet all other things being equal, a prohibition on individualized profiling (or on nonconsensual profiling) will not change the fact that businesses compete to provide products and services that consumers prefer, and that digital networks and search tools reduce the costs of niche competition.

The privacy-value tradeoff, moreover, rests on the same spurious technological determinism as the privacy-efficiency tradeoff discussed in Part II.C.[103] Currently, technologies designed to measure consumer preferences permit retrieval and matching of data with names and other identifying characteristics. Systems could be designed quite differently. They could, for example, allow aggregate profiling of groups of consumers without generating personally-identified or identifiable data.[104] For that matter, the problem

---

98. *See id*. at xvii-xviii.

99. *See* text accompanying notes 188-206 *infra*.

100. *See* ISAIAH BERLIN, TWO CONCEPTS OF LIBERTY (1958); David P. Currie, *Positive and Negative Constitutional Rights*, 53 U. CHI. L. REV. 864 (1986).

101. For a concise discussion of the "economics of attention," see CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 6-8 (1999); *see also id.* at 33-37, 166.

102. *See* Rohan Samarajiva, *Interactivity as Though Privacy Mattered*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE, *supra* note 51, at 277 (summarizing this argument and trends showing increasing frequency and granularity of profiling in media industries).

103. *See* text accompanying notes 51-61 *supra*.

104. *Cf.* Burkert, *supra* note 60, at 131-33 (discussing this option but noting the need for sensitivity to potential risks posed by group profiles).

of targeting information to consumers need not be solved by giving businesses more information about consumers; it could, instead, be solved by giving consumers more information about businesses. Rather than giving one entity rights to "shoes.com," for example, we might design the Internet domain name system to include directory pages for common words.[105]

To be sure, the argument that limiting personal profiling will force market tradeoffs is not frivolous. At the margin, some businesses will suffer, and some may go under (though others may thrive). The point is that the mere fact of a tradeoff with some (unquantifiable) impact on choice in markets dictates the outcome of the data privacy debate only if there is only one way to provide businesses with marketing information, and only if choice in markets is the touchstone. Neither assumption is warranted. Our options are more numerous, and more complicated, than market-tradeoffs reasoning suggests.

* * * *

Like "property," "freedom of choice" cannot function as a solving idea for the data privacy problem. The rhetoric of choice obscures the reality that we face not one decision (freedom or not), but a bewildering constellation of decisions about which choices to privilege, which to facilitate, and which to restrict. We confront, as well, a bewildering array of legal, informational, and technological tools that might be used to shape choices, or to set parameters for them.[106] A neutral conception of "freedom of choice" will not help us; there simply is no neutral way of deciding how to choose.

The easy response to this dilemma is no response. Yet as Larry Lessig so persuasively demonstrates, "doing nothing" and allowing market processes to dictate policy outcomes is itself a collective choice.[107] Taking freedom seriously requires more—or at least more honesty about why a particular context or field of choice is preferred over others. We may decide that market measures of choice are superior to other measures (for example, political ones).[108] Or we may decide that decentralized market processes are superior to conscious attempts at social engineering.[109] But we—as a soci-

---

105. Registration of generic domain names has become a multi-million-dollar business, and allows exclusive ownership of easily-remembered search terms. *See* Ira S. Nathenson, *Showdown at the Domain Name Corral: Property Rights and Personal Jurisdiction Over Squatters, Poachers, and Other Parasites*, 58 U. PITT. L. REV. 911, 956-57 (1997); *Net Names Glitter for Entrepreneurs*, CNET NEWS, Dec. 28, 1999 <http://www.news.cnet.com/news/0-1005-200-1507943.html>.

106. *See* LESSIG, *supra* note 36, at 85-99; *see also* Lessig, *supra* note 71.

107. *See* LESSIG, *supra* note 36, at 218-21.

108. This might, but need not, reflect a belief that distributing privacy based on income is fair. Instead, we might simply conclude that politically-determined criteria for privacy policy are likely to be worse.

109. *See* David G. Post & David R. Johnson, *"Chaos Prevailing on Every Continent": Towards a New Theory of Decentralized Decision-Making in Complex Systems*, 73 CHI.-KENT L.

ety—should decide, and we should acknowledge our reasons. And since choices about parameters are also, inevitably, choices about substance, we also should consider the substantive purposes and values that profiling is said to serve.

## IV. KNOWING

The data privacy debate is, third, a debate about the substantive value of personally-identified information. What do data processors in particular, and society in general, gain from the ready availability of this information? One view, broadly shared among participants on all sides of the debate and advanced with particular force by those concerned with access to data for research purposes, is that the collection and processing of personal data creates knowledge. In addition, because our society places important values on "sunlight," withholding or concealing personal data has moral overtones.[110] Finally, data privacy opponents argue that marketers armed with more information will serve consumer preferences more accurately, using means that are less intrusive than current marketing practices.

If any of these arguments is right, then strong data privacy protection seems singularly ill-advised—bad policy at best, and pernicious at worst. Yet the underlying questions that data processing seeks to answer—who people are, and what they want—are far more complicated than the knowledge justification makes them seem. This Part seeks to delineate the sorts of "knowledge" that ready access to personally-identified data furthers, and to understand the alternatives.

### A. *Theories of Knowledge*

The rush to capture ever-greater amounts of personally-identified information is premised on the assumption that this information will yield the ability to understand, and ultimately predict, individual behavior. Information, on this view, is simply the key to a preexisting reality that is determined and discoverable. For the most part, even advocates of strong data privacy have not questioned this central premise of the data processing industry.[111] Yet research in economics, psychology, and information theory suggests that

---

REV. 1055 (1998); David R. Johnson, *Let's Let the Net Self-Regulate: The Case for Allowing Decentralized, Emergent Self-Ordering to Solve the "Public Policy" Problems Created by the Internet* (Apr. 7, 2000) <http://www.cli.org/selford/essay.htm>; David R. Johnson & David G. Post, *And How Shall the Net Be Governed?: A Meditation on the Relative Virtues of Decentralized, Emergent Law* (Apr. 7, 2000) <http://www.cli.org/emdraft.html>.

110. *See* Kreimer, *supra* note 9, at 91-92, 99-102.

111. *See, e.g.*, Schwartz, *supra* note 84, at 25-31 (contesting the accuracy of conclusions drawn from genetic testing, but on the more limited grounds that current genetic knowledge is incomplete and that data processors will use data irrationally).

the relationship between data and behavior is much more complicated. Before making decisions about the contours of data privacy policy, it is worth probing more closely into what we think personal data tell us about human nature and predilection, and why we think this.

Within the legal academy, and within the larger data privacy debate, discussion of the value and social significance of personally-identified data is increasingly framed in economic terms. Neoclassical law and economics theory casts information asymmetry as inefficient because it precludes fully informed trades.[112] This view recognizes limited exceptions when secrecy is desirable to induce productive activity—for example, trade secrecy to induce research and development.[113] The individual desire to withhold personal data does not fall into this category, however. Individuals who withhold personal data are simply seeking to deceive their trading partners—or, more neutrally, to appropriate a greater share of the gains from trade than they otherwise would receive if their trading partners knew the "truth."[114] On this view, therefore, the default rule should be one of disclosure, and the burden falls on data privacy advocates to justify departures.

The standard legal-economic approach to personal information is firmly rooted in liberal political theory and in associated principles of Enlightenment philosophy. If individuals must be free to promote their own happiness by trading, and if individuals can best judge the happiness-enhancing effect of particular trades with full information, then it follows that a regime of disclosure is best. Fully informed, in turn, means "possessed of all the information that one would want." And (assuming one were rational) one would want nothing less than to be scientific about identifying, collecting, systematizing, and digesting the relevant facts.[115]

To be sure, this legal-economic justification for disclosure is neither monolithic nor universally accepted. First, some economically trained critics charge that it improperly discounts individual preferences for privacy.[116] Individuals who withhold personal data will not always be seeking to deceive trading partners, but rather (or at least sometimes) to promote their own happiness. To the extent that the knowledge justification discounts this sort of preference, it is both inaccurate and inappropriately paternalistic.

Second, the model does not seriously consider that the insights gained from data processing may be incomplete or otherwise inaccurate. As a re-

---

112. *See* Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978); George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623 (1980).

113. *See* Posner, *supra* note 112, at 404.

114. *See id*. at 399.

115. *See* BORGMANN, *supra* note 2, at 34-37.

116. *See* Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2416 (1996) (arguing that the utility derived from privacy is a substantial economic benefit).

sult, market participants may draw inaccurate conclusions about individual reliability or risk. For example, as Paul Schwartz shows, imperfect understanding of the correlation between genetic markers and disease may lead to poorly reasoned decisions about insurability, or even employability.[117] In addition, cognitive theory tells us that preexisting biases color interpretation of the insights gained from data processing.[118]

Inaccuracy and irrationality problems, however, do not seem to dictate an obvious policy response. In both cases, one might conclude that some degree of data privacy is the solution. But one might also conclude that the solution is more information, or better algorithms, or greater accountability. Indeed, this is precisely what the prevailing rationale for data collection would tend to suggest. On this view, the distortions caused by inaccuracy and irrationality are temporary and resolvable. The problem is not that we live in a world with an abundance of personal data, but that we have not yet learned how to understand what the data tell us. Much hinges on whether this is so, or whether these problems are more intractable than they appear.

The more profound objection to the prevailing legal-economic approach to information is that it conflates information with knowledge of (or truth about) reality. Information theory, in contrast, recognizes that "information" and "reality" are different (though related) things, and that "knowledge" forms an imperfect and culturally contingent bridge between them.[119] Knowledge in society is a function of "technique," defined broadly as the technical and cognitive tools used to process information.[120] For information to be translated into anything more meaningful than transient sensory input, some heuristic is necessary. Yet the choice of frame—the choice of how to think about how we know things—is a choice that has substantive consequences.

---

117. *See* Schwartz, *supra* note 84, at 25, 36.

118. *See, e.g.*, Amos Tversky & Daniel Kahneman, *Judgment Under Uncertainty: Heuristics and Biases*, 185 SCI. 1124, 1124 (1974) (showing that people rely on a limited number of heuristic principles to reduce the complex task of assessing probabilities and predicting values to simple judgmental operations, and that this sometimes leads to severe and systematic errors); *see also* Schwartz, *supra* note 84, at 25-31.

119. *See* ALBERT BORGMANN, HOLDING ONTO REALITY: THE NATURE OF INFORMATION AT THE TURN OF THE MILLENNIUM (1999); BRUNO LATOUR, WE HAVE NEVER BEEN MODERN (Catherine Porter trans., 1993); FRANK WEBSTER, THEORIES OF THE INFORMATION SOCIETY (1995); *cf.* THOMAS S. KUHN, THE STRUCTURE OF SCIENTIFIC REVOLUTIONS (2d ed. 1970) (arguing that our perceptions of scientific "facts" are shaped by the paradigms that we employ to make sense of them).

120. *See* BORGMANN, *supra* note 119; JACQUES ELLUL, THE TECHNOLOGICAL SOCIETY (John Wilkinson trans., 1964); KUHN, *supra* note 119; DONALD MACKENZIE, KNOWING MACHINES: ESSAYS ON TECHNOLOGICAL CHANGE (1997); LANGDON WINNER, AUTONOMOUS TECHNOLOGY: TECHNICS-OUT-OF-CONTROL AS A THEME IN POLITICAL THOUGHT (1977); *see also* LAKOFF & JOHNSON, *supra* note 16.

In our society, the prevailing approach to questions of technique is rationalizing. Knowledge of the world is attained by measuring, metering, and predicting. Information theorists recognize, however, that rationalizing techniques may incorporate and reproduce systematic *ir*rationalities. Information systems and technologies are designed, not given, and the design process for any technology or system for organizing information necessarily incorporates assumptions about the things or conditions that should be measured, and the relevant quanta of measurement.[121]

The data processing industry reflects and reproduces this rationalizing framework.[122] Data processing practices are predicated on a belief that individuals are reducible to the sum of their transactions, genetic markers, and other measurable attributes, and that these attributes are good predictors of risk and reward in future dealings. Plainly, this belief is not entirely wrong; there is much about individual behavior that is predictable on this basis. Yet there also is much about individual behavior that is not. Some relevant information is inherently incapable of measurement or prediction. Human motivation is internal, partly emotional, and often adventitious. The question is whether systematically ignoring this dimension of human behavior, and human potential, produces policy consequences that we would rather avoid.

### B. *Knowledge, Persuasion, and Power*

There are two immediate arguments that the limitations inherent in the data processing paradigm do not matter much. First, some predictability is necessary for individuals, businesses, and governments to function. Second, and relatedly, it may simply be that the question whether personally-identified information is knowledge reduces to an argument about social attitudes toward predictability and its risks. There is a sense in which *un*predictability strains our tolerance; we need to see the "hard facts"—including, perhaps, the information gained from data processing—as certain, or at least certain enough.[123] And if that is all, then perhaps there is no problem here; reliance need not equal blind faith.

One might object, further, that problematizing the knowledge gained from data processing does not yield a particularly compelling argument for data privacy as opposed to any other regime. If there is no "truth," then why

---

121. *See* BORGMANN, *supra* note 119; ELLUL, *supra* note 120; GANDY, *supra* note 91, at 15-52; MACKENZIE, *supra* note 120; WINNER, *supra* note 120.

122. *See* GANDY, *supra* note 91, at 53-94. Paul Schwarz's discussion of "genetic determinism" in the use of personal health care information approaches this conclusion. *See* Schwartz, *supra* note 84, at 26-29.

123. This parallels the preference for the relatively bounded, deterministic language of property rights over the relatively fuzzy, open-ended language of "dignity rights." *See* notes 10-16 *supra* and accompanying text. *But see* BORGMANN, *supra* note 2, at 20-47 (arguing that the perceived need to control and predict is culturally determined).

does it matter what information others collect about us? Or, to be slightly less nihilistic, if there is no "truth," then why not let people choose for themselves whether to provide information to others?[124] On this view, the indeterminacy of knowledge is a ho-hum affair; it provides neither sufficient justification for nor sufficient objection to trade in personally-identified data.[125]

The indeterminate relation between information and "truth," however, is only half the story. The relationship between information and reality is dialectical: Reality eludes information and information-processing technique, but at the same time information and technique shape behavior.[126] Put differently, there is a real and substantial difference between denying there is a single, objectively knowable reality and denying that there is an experienced reality, or that the use of information to shape that reality matters. To reason from the constructedness of reality to its absence (or unimportance) is to negate human agency. The fact that identity (as a function of preferences) is malleable does not mean that identity is irrelevant.

Thus, the data privacy debate is not only about whether prediction is possible, or about how much predictability we require, but also (with apologies to Marx) about who controls the *modes of prediction*—in other words, about power over knowledge.[127] It follows that mechanisms for accountability (a watchword for data privacy advocates) should concern at least this much.[128] If categorization determines eligibility for rewards or opportunities, then we may have an interest in the algorithms used to categorize. More

---

124. This conclusion aligns with the observation that postmodern information theory is entirely compatible with the late-stage informational capitalism that it purports to criticize. *See* WEBSTER, *supra* note 119, at 190-91 (discussing theories by Fredric Jameson, David Harvey, and Daniel Bell that interpret post-modernism as a product of capitalism).

125. It is worth noting, too, that although the corpus of personally-identified information now residing in corporate and government databanks may mean less than we would like to believe, some information is still true, and the collection of some truthful information is still important. Individuals, both as consumers and citizens, have an interest in the accurate collection of some data about themselves and others. As Part VI.B discusses, a wise data privacy policy should attempt to identify the circumstances in which that interest should outweigh others. *See* notes 207-221 *infra* and accompanying text.

126. *See* BORGMANN, *supra* note 119; ELLUL, *supra* note 120; MACKENZIE, *supra* note 120.

127. *See, e.g.*, MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON (Alan Sheridan ed. & trans., 1977); MICHEL FOUCAULT, POWER/KNOWLEDGE (Colin Gordon ed. & trans., 1980). Historians of technology dispute whether Marx understood technology simply as an object of the struggle to control production, or as a critical constituent of production relations. *See* MACKENZIE, *supra* note 120, at 36-47 (describing the debate and taking the latter view). The postmodernists, in turn, have been criticized for devoting insufficient attention to the relationships between information, technology, and *economic* power. *See* WEBSTER, *supra* note 119, at 190-91.

128. *Cf.* Victoria Bellotti, *Design for Privacy in Multimedia Computing and Communications Environments*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE, *supra* note 51, at 63 (arguing that the design of information systems should take into account the values of those whose actions are to be recorded).

fundamentally, if preferences are subject to shaping and reshaping over time, then we may have an interest in the sorts of shaping that are permitted.

Data privacy opponents argue that more fine-grained profiling will eliminate the inaccuracies that lead to manipulation, by achieving a precise correspondence between product offerings and individual wants.[129] Yet surely that is far too simple. The goal of any advertising is to get people to buy—to create demand for what vendors want to sell. Targeted advertising may be more successful, but it doesn't necessarily follow that such advertising simply divines and reflects preexisting desires.[130] It is well-understood that the attractiveness of choices depends on how they are framed.[131] A more tailored frame is not necessarily less manipulative; it may be more so.

Again, though, the exclusive focus on purchaser choice is disingenuous. As noted above, many uses of personally-identified data occur outside the realm of direct-to-consumer marketing. And even the point of targeted advertising is not merely to enable choice by the target market, but also to effectuate choice by the advertiser. Better profiling enables discrimination in the broad sense, on any ground deemed reasonable, desirable, and not illegal.[132] And even "benign" discrimination—say, a decision to market only to those subsets of consumers who are statistically more likely to buy—operates to categorize at least some individuals on a basis other than the one they would wish.[133]

Here, as with transaction costs and choice, we confront an allocational inequality. The knowledge justification for personal profiling treats irrationality by information-seekers and information-withholders differently. Data processors are free to behave irrationally (though it is presumed that they ordinarily won't); data subjects may not. Or, more precisely, data subjects may behave as they please, but will be judged against standards of rationality not of their own choosing. The view of human nature reinforced by data-processing algorithms is both unforgiving and ungenerous. There is little room, or tolerance, for randomness, idiosyncrasy, or mistake, and little allowance for learning effects and second chances. The data processing para-

---

129. *See, e.g.*, The Direct Marketing Association, *DMA Interactive* <http://www.the-dma.org/>; Teleconnect, Inc., *Teleconnect* <http://www.teleconnect.com/>. For a more theoretical discussion of profiling, see Hal R. Varian, *Economic Aspects of Personal Privacy* (December 6, 1996) <http://www.sims.berkeley.edu/~hal/Papers/privacy/> (explaining economic rationale for profiling).

130. *See* Kirsten M. Lagatree, *Where You Live Gives Marketers Clues to Buying Habits*, L.A. TIMES, Dec. 15, 1996, at K3 (describing examples of targeted advertising); *cf.* Dinh, *supra* note 50, at 2130 (arguing that advertising seeks to create relative preferences, and that these preferences are socially inefficient).

131. *See generally* Tversky & Kahneman, *supra* note 118; Amos Tversky & Daniel Kahneman, *Rational Choice and the Framing of Decisions*, 59 J. BUS. S251 (1986) (describing common rules of framing and their effects on choice).

132. Prohibitions on racial profiling represent an implicit societal decision that not every use of "rational"/statistical knowledge should be permitted. *See* text accompanying note 178 *infra*.

133. *See* GANDY, *supra* note 91, at 80-87.

digm holds individuals rigidly accountable for their past experiences—even as it seeks to coopt agency prospectively.

Sometimes, categorization of individuals may be fair; sometimes, too, it will be inevitable, or we will conclude that the risks of attempting to prohibit it are too great. But the content of the categories, and the fairness of reliance on category-driven sorting as a means of allocating economic opportunity, are proper subjects for collective debate. It is at least worth discussing whether this approach is desirable, and considering the alternatives.

* * * *

The data processing paradigm conceals a power relationship, and that relationship, in turn, is a crucial determinant of the truth that data processing constructs. In evaluating knowledge claims about the processing of personally-identified data, we are not simply concerned with predictability and risk tolerance, but more fundamentally with questions of behavior modification and free will. Profiling represents not only a particular theory of knowing, but also a disturbing, deeply cynical opportunism about the use of persuasion to reshape individual and collective knowledge. If data reveals truth, it is possible to attain omniscience. If data constructs truth, it is possible to attain power. We have a vested interest in the content of the "truth" under construction. It follows that data privacy policy should be concerned with modes of knowing; a wise data privacy policy cannot do otherwise. Yet we also must consider, finally, whether constitutional protection for freedom of expression prevents this inquiry. To that question I now turn.

## V. SPEAKING

A final answer to the problem of knowledge, and a fourth perspective on the data privacy question, is that the difference between "knowledge" and "information" is irrelevant to resolving the data privacy debate. Instead, the data privacy debate is a debate about freedom of speech and its limits. On this view, the problem with strong data privacy protection is not that it would protect data subjects against erroneous judgments of their worth or limiting representations of reality. In our society, one may not spread deliberate falsehood (at least not without fear of a libel suit), but one is under no obligation to seek "truth" in some absolute sense. Instead, the problem with data privacy protection is that it would interfere with the speech rights of would-be data-collectors to spread any judgments, generalizations, and correlations that are salable and not demonstrably false.

Of all the categorical double-binds that the data privacy debate creates, the opposition of privacy and speech is by far the most difficult. Speech freedoms are central in our culture, and their vigilant protection has served us well. Yet of all the perceived privacy conflicts, this one most requires explo-

ration, and for precisely the same reason that it is hard: An expansive approach to the liberties of data processors threatens constitutional foreclosure of the data privacy debate. We must consider, then, whether the data privacy debate really forces us to choose between privacy and speech.

### A. *Theories of (Commercial?) Speech*

The First Amendment argument against data privacy protection begins by assuming that the collection, processing, and exchange of personally-identified data are "speech," and then asserts that regulation of these activities cannot survive the requisite scrutiny.[134] Both steps bear closer scrutiny. As applied to data privacy regulation, the standard balancing analysis has been categorical, driven by outcome-determining presuppositions about the expressive content and ownership status of personally-identified information. Closer attention to the competing interests that data privacy regulation seeks to balance might produce a different assessment of the constitutionality of generally-applicable protective measures. More fundamentally, though, there is reason to question whether the traditional modes of First Amendment review should apply in the same way, or at all, to regulation of commercial processing of personal information. Other approaches to theorizing about speech, and about information more generally, suggest different ways of thinking about the collection and exchange of personally-identified data and the role of these activities within the broader commercial fabric of society.

As an initial matter, a First Amendment analysis of data privacy protection must consider how to characterize the sort of speech involved. Traditionally, the threshold for regulation of speech classed as "commercial" has been lower than the threshold for regulation of other speech.[135] Both some advocates and some opponents of strong data privacy protection have assumed that the collection and exchange of personally-identified data by commercial entities is most appropriately classified as commercial speech, and the handful of courts that have addressed First Amendment challenges to data privacy regulations have followed suit.[136]

---

134. *See, e.g.*, SINGLETON, *supra* note 51; Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000).

135. First Amendment protection for commercial speech is a relatively recent development. *See* Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of N.Y., 447 U.S. 557, 561-63 (1980); Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 758-70 (1976). Previously, the Court had held that commercial advertising, at least, was not entitled to First Amendment protection at all. *See* Valentine v. Chrestensen, 316 U.S. 52, 54 (1942) ("[T]he Constitution imposes no . . . restraint on government as respects purely commercial advertising.").

136. *See* U.S. West, Inc. v. FCC, 182 F.3d 1224, 1232-33 (10th Cir. 1999); United Reporting Publ'g Corp. v. California Highway Patrol, 146 F.3d 1133, 1136-37 (9th Cir. 1998), *rev'd sub nom.* Los Angeles Police Dep't v. United Reporting Publ'g Corp., 120 S. Ct. 483 (1999).

In fact, most regulation of commercial data-processing activities probably would not qualify as "commercial speech" regulation. The traditional justification for greater regulation of commercial speech turns on the listener's interest in receiving accurate information about market choices, and holds that the government may suppress misleading or deceptive commercial communications to protect this interest.[137] Although data privacy advocates object that current law does not hold data processors accountable for the accuracy of personally-identified data, their concerns extend far beyond factual accuracy. In addition, a focus on misleading or deceptive communications suggests that "commercial speech" encompasses only communications between buyer and seller about terms, or about the qualities of the seller's goods or services.[138] Arguably, this definition does not encompass the actual subject matter of the transaction—here, the data itself.[139]

That data privacy regulation burdens speech does not necessarily make it unconstitutional. Instead, courts undertake a balancing inquiry. Regulation of commercial speech must satisfy the four-part test articulated in *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*.[140] Under *Central Hudson*, if the regulation targets a communication that is not misleading or related to unlawful activity, it must be supported by a substantial government interest, must materially advance that interest, and must not be more restrictive than necessary to serve that interest.[141] A similar standard applies to content-neutral laws that burden speech only indirectly.[142] In

---

137. *See Central Hudson*, 447 U.S. at 563-64; *Virginia State Bd. of Pharmacy*, 425 U.S. at 771 & n.24. At least four current Justices would classify as "commercial speech" only speech that proposes a commercial transaction, and would apply intermediate scrutiny only where regulation of such speech is designed to prevent fraud or deception. *See* 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 509-14 (1996) (plurality); *id*. at 518 (Thomas, J., concurring); *see also* Alex Kozinski & Stuart Banner, *The Anti-History and Pre-History of Commercial Speech*, 71 TEX. L. REV. 747 (1993) (discussing the early history of advertising and arguing that the early cases do not support the notion of a general distinction between "commercial" and "noncommercial" speech); Alex Kozinski & Stuart Banner, *Who's Afraid of Commercial Speech?*, 76 VA. L. REV. 627 (1990) (arguing that a general distinction between commercial and noncommercial speech in untenable); ; Martin H. Redish, *First Amendment Theory and the Demise of the Commercial Speech Distinction: The Case of the Smoking Controversy*, 24 N. KY. L. REV. 553 (1997) (same); Martin H. Redish, *The First Amendment in the Marketplace: Commercial Speech and the Values of Free Expression*, 39 GEO. WASH. L. REV. 429 (1971) (same).

138. *See Central Hudson*, 447 U.S. at 562-63; *Virginia Bd. of Pharmacy*, 425 U.S. at 761-62, 771-72.

139. Data privacy opponents argue that transactions in personally-identified data are analogous to reporting by the press, and therefore should receive the highest First Amendment protection. *See* SINGLETON, *supra* note 51, at 7. I shall argue, however, that the fact that the data is the actual subject matter of the transaction argues for quite a different First Amendment standard of review. *See* text accompanying notes 161-164 *infra*; *see also* text accompanying notes 207-214 *infra* (discussing, and rejecting, the "journalism" objection to data privacy regulation).

140. 447 U.S. 557 (1980).

141. *See id.* at 564.

142. *See* United States v. O'Brien, 391 U.S. 367, 376-77 (1968) (noting that incidental limitations on First Amendment freedoms are permissible if they further a substantial government interest

other speech cases, the government interest must be compelling and the regulation narrowly tailored to advance the interest in the least restrictive way.[143]

A pair of recent cases, however, suggest that courts may interpret these tests in ways that pose insuperable difficulties for data privacy regulation. In both cases, the analysis was categorical; both courts paid lip service to the idea of balancing, but treated strong data privacy protection as definitionally incompatible with constitutional speech regulation. Together, the two decisions reveal an understanding of "speech"—derived from the germinal metaphor of a "marketplace of ideas,"[144] but conceptually quite distinct from it—as inextricably bound up with the exchange of informational property in markets.

In *U.S. West v. Federal Communications Commission*, a Tenth Circuit majority concluded that heightened informed consent requirements violated *Central Hudson*'s fourth prong.[145] The dispute concerned an FCC regulation requiring telephone companies to use opt-in rather than opt-out procedures before using their customers' personally-identified data to cross-sell other services. A majority of the panel agreed with U.S. West that, given the availability of less burdensome opt-out procedures, the opt-in regulation was more restrictive than necessary to serve the asserted purpose of protecting customer privacy. The court rejected the argument advanced by the FCC—and endorsed by the dissenting judge—that opt-in procedures were the least restrictive means likely to be effective in obtaining meaningful, informed consent.[146]

The *U.S. West* decision nicely illustrates Peter Edelman's observation that judges balancing speech and privacy claims reveal themselves to be "absolutists in balancers' clothing."[147] The ultimate question in *U.S. West*—the relative burden of opt-in and opt-out restrictions governing a consent-based regime for the reuse of personally-identified data—was narrow and factual. Given the extensive record developed by the FCC regarding the likely ineffectiveness of opt-out procedures, the majority's conclusion is difficult to

---

unrelated to the suppression of free expression and if the limitation is no greater "than is essential to the furtherance of that interest").

143. *See* Burson v. Freeman, 504 U.S. 191, 198 (1992) (plurality); Boos v. Barry, 485 U.S. 312, 321 (1988); Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 45 (1983).

144. *See* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting); Kathleen M. Sullivan, *Free Speech and Unfree Markets*, 42 UCLA L. REV. 949, 963-64 (1995); Kathleen M. Sullivan, *Discrimination, Distribution and Free Speech*, 37 ARIZ. L. REV. 439, 445-46 (1995).

145. 182 F.3d 1224, 1238 (10th Cir. 1999).

146. *See id*. at 1238-39; *id.* at 1246-47 (Briscoe, J., dissenting).

147. Peter B. Edelman, *Free Press v. Privacy: Haunted by the Ghost of Justice Black*, 68 TEX. L. REV. 1195, 1223 (1990).

justify.[148] *Central Hudson* itself is clear that burden cannot be assessed in a vacuum, but rather must be judged relative to likely efficacy. (By any standard, the dispute in *U.S. West* implicates core commercial speech concerns about deception of consumers; even if it didn't, though, the regulation seems designed to survive even stricter scrutiny than *Central Hudson* requires.) The *U.S. West* majority's lack of interest in the record bespeaks prejudgment—not only about speech, but also about ownership, choice, and the value of transactional information. The court presumed a world in which data processors own their customers' personally-identified information unless the customers say otherwise, and in which "choice" is assessed in the abstract, without considering whether there is enough information to make the choice a real one. And although it did not decide the question, it expressed skepticism that a broad, general interest in "privacy" could ever be weighty enough to support greater restrictions on the flow of "true information."[149]

Even an opposite resolution of the opt-in/opt-out problem, though, doesn't speak to the constitutionality of attempts to regulate secondary and tertiary uses of information already in a data processor's possession. Here, a recent Ninth Circuit decision (later reversed on other grounds) demonstrates that regulations restricting the use and exchange of personally-identified data may face an equally tough hurdle in the third prong of the *Central Hudson* test. *United Reporting Publishing Corp. v. California Highway Patrol*[150] involved a California statute authorizing release of arrestees' addresses for "scholarly, journalistic, political, or governmental" but not commercial purposes.[151] A unanimous court found that in light of these provisions, the restriction on commercial access would not materially advance the asserted interest of promoting the privacy of arrestees.[152] Therefore, the court concluded, the regulation was "directed at preventing solicitation practices"—in other words, at suppressing protected speech directed at the eventual targets of commercial profiling activities—and so invalid on its face.[153]

---

148. I have signed an amicus brief urging en banc reconsideration on this and other grounds.

149. *See U.S. West*, 182 F.3d at 1234-35 & n.7 (quoting FRED H. CATE, PRIVACY IN THE INFORMATION AGE 28 (1997)).

150. 146 F.3d 1133 (9th Cir. 1998), *rev'd sub nom.* Los Angeles Police Dep't v. United Reporting Publ'g Corp., 120 S. Ct. 483 (1999).

151. *Id*. at 1135 (quoting a 1996 amendment to CAL. GOV. CODE § 6254(f) (West 1995)).

152. *See id*. at 1138-40.

153. *Id*. at 1139 (citing Bolger v. Youngs Drug Products Corp., 463 U.S. 60, 73 (1983)). At oral argument in the Supreme Court, counsel for United Reporting characterized the statute's differential treatment of commercial and journalistic uses as content-based discrimination. *See* Appellee's Oral Argument at 32-34, Los Angeles Police Dept. v. United Reporting Publ'g Corp., 120 S. Ct. 483 (1999) (No. 98-678) (*available in* 1999 WL 970765) . Although he did not argue that this should trigger strict scrutiny, one presumes that the statute's express distinction between broadly "commercial" uses and other uses would be unacceptable to those Justices who urge a narrower definition of commercial speech. *See supra* note 137.

Again, though, the *United Reporting* court's conclusions seem driven by presuppositions about the nature and weight of data privacy claims rather than by a careful balancing of the interests involved. The court conflated information about individuals with communication to individuals, and thus refused, definitionally, to recognize profiling as a separate and distinct harm that the state might have an interest in seeking to prevent. As a result, it dismissed as "no more than speculation and conjecture" the state's argument that the statute would help prevent commercial profiling from reaching critical mass.[154] And the court's analysis of the statutory exceptions as directed at (a particular type of) direct-marketing communication rather than at protecting privacy erects a constitutional barrier to data privacy protection that is effectively insurmountable. The statutory language strongly suggests that the California Legislature attempted to strike a balance that would not threaten the important First Amendment interest in promoting reporting and comment on issues of public concern. For precisely that reason, one suspects that more comprehensive usage restrictions—restrictions designed to promote privacy even more "materially"—would have failed prong four of the *Central Hudson* analysis. In effect, then, the Ninth Circuit's decision says that government can't protect data privacy at all.[155]

In short, *U.S. West* and the circuit-level decision in *United Reporting* rest on the same implicit, and rather curious, syllogistic reasoning about the irreconcilability of legal protection for data privacy and legal protection for speech: Personally-identified data is (true) information; this information is owned, presumptively, by those who collect it; the solicitation of consumers is an expressive act; therefore, anything that burdens the collection, commercial use, and market exchange of personally-identified information impermissibly burdens speech. The effortless and wholly unremarked slippage between images of information as speech and as (owned and traded) commodity is all the more remarkable because neither court (and, for that matter, none of the parties) questioned the presence of "communication" at the collection, processing, and exchange stages—a threshold requirement either for *Central Hudson* scrutiny or for the stricter scrutiny that a narrowed conception of commercial speech might require. In the sense that counts for First Amendment purposes, personally-identified data is not collected, used or sold for its expressive content at all; it is a tool for processing people, not a

154. *United Reporting*, 146 F.3d at 1139.

155. The Supreme Court's reversal, on the ground that California was not required to give out arrestee information in the first place, does not disturb this reasoning with respect to information that government is required to disclose, nor with respect to regulation of purely private-sector information transactions. *See* Los Angeles Police Dep't v. United Reporting Publ'g Corporate,. 120 S. Ct. 483, 489 (1999). Moreover, the Court carefully reserved judgment on an as-applied challenge that the Ninth Circuit had not considered. *See id.* at 488; *id*. at 490 (Scalia, J., concurring); *see also id*. at 491-93 (Stevens, J., dissenting).

vehicle for injecting communication into the "marketplace of ideas."[156] Yet this objection is definitionally incompatible with the view that the highest and best First Amendment value of any information is realized through its free-subject-to-the-rules-of-property exchange in markets. And so, finally, our understanding of "speech" reinforces, and is reinforced by, the theory of market-based self-actualization that undergirds our models of knowledge, ownership, and choice.

Once again, though, other strands of theorizing about speech, and more broadly about law and information policy, point in other directions. First and most generally, some First Amendment scholars argue that speech markets require a certain amount of economic regulation—in other words, that a market-based understanding of speech justifies regulatory responses designed to correct market failures.[157] If we reconceptualized the government interest in protecting data privacy as an interest in correcting information asymmetries in the market for personally-identified data, the *Central Hudson* analysis (or a more stringent review) might proceed quite differently. In particular, an explicitly economic approach to regulation of speech markets would save regulations like the opt-in rule challenged in *U.S. West*, which focus on the quality as well as the fact of consent.

In addition, several scholars have advanced alternative approaches to the more broadly defined problem of government regulation of speech by commercial speakers. Here, the works of C. Edwin Baker and Daniel Halberstam are particularly important. Baker's theory of speech rights as intended to further individual liberty would accord minimal, if any, constitutional protection to commercial speakers that are not individuals.[158] Halberstam, in contrast, believes that commercial speech merits at least some First Amendment protection. He argues, however, that commercial speech, broadly defined, plays an important structural role in constituting commercial institutions within society, and thus merits regulation to the extent necessary to preserve institutional integrity.[159]

---

156. *Cf.* Dan L Burk, *Patenting Speech*, 79 TEX. L. REV. (forthcoming 2000) (discussing the dual nature of software as information and as an artifact embodying functionality). Robert Post argues that the "communication" trigger for First Amendment scrutiny is itself an empty formalism. *See* Robert Post, *Recuperating First Amendment Doctrine*, 47 STAN. L. REV. 1249, 1251-60 (1995).

157. *See* C. EDWIN BAKER, ADVERTISING AND A DEMOCRATIC PRESS (1994); C. Edwin Baker, *Giving the Audience What It Wants*, 58 OHIO ST. L.J. 311 (1997); Ashutosh Bhagwat, *Of Markets and Media: The First Amendment, the New Mass Media, and the Political Components of Culture*, 74 N.C. L. REV. 141 (1995).

158. *See* C. EDWIN BAKER, HUMAN LIBERTY AND FREEDOM OF SPEECH 194-224 (1989); Randall P. Bezanson, *Institutional Speech*, 80 IOWA L. REV. 735, 735-36 (1995) (arguing that speech without an identifiable individual author is ineligible for First Amendment protection).

159. *See* Daniel Halberstam, *Commercial Speech, Professional Speech, and the Constitutional Status of Social Institutions*, 147 U. PA. L. REV. 771 (1999) (advocating a unified treatment of commercial and professional speech); *cf.* Post, *supra* note 156 (arguing that First Amendment doc-

Together, Baker's and Halberstam's analyses support an approach to (commercial) speech regulation that emphasizes the structural and production functions of speech markets within society.[160] One need not subscribe to Baker's conclusion that corporate commercial speech is wholly unprotected to endorse his more general point that promoting individual autonomy and self-determination are central First Amendment concerns.[161] On this view, Congress might regulate commercial data-processing practices that seek to reduce individuals to the objects of classification, sorting, and preference-manipulation. Halberstam's approach, meanwhile, suggests that Congress also may regulate the collection and exchange of personally-identified data to prevent the systemic, structural consequences of a growing imbalance of informational power between vendors and consumers.

Finally, a market-institutional approach to speech regulation also counsels greater sensitivity to the dual role of information as "speech" and as "product" or "property." Recent work in both First Amendment theory and intellectual property law raises provocative questions about how the law should reconcile the rigorous scrutiny due restrictions on speech with the much greater deference afforded regulation of property interests. For example, Spencer Overton suggests that because political contributions share important distributional characteristics with real property, courts should employ a hybrid standard for review of campaign finance legislation.[162] Foundational work in law and information policy by James Boyle, Yochai Benkler, Diane Zimmerman, and others explores the theoretical and logistical difficulties that the dual nature of information poses for rules concerning access to and use of information goods.[163] Much work remains to be done in exploring and describing the interfaces between property and speech, both gen-

---

trine should consider the functions of speech within social institutions); Frederick Schauer, *Principles, Institutions, and the First Amendment*, 112 HARV. L. REV. 84 (1998) (same).

160. The terminology is Neil Netanel's. *See* Neil Weinstock Netanel, *Copyright and a Democratic Civil Society*, 106 YALE L.J. 283, 288 (1997). Netanel argues that copyright law, properly understood, serves both to reinforce social institutions that prevent the entrenchment and abuse of power and to foster reasoned deliberation about public affairs. He concludes that limiting the scope of the rights accorded individual authors best promotes these goals. *See id*. at 364-85.

161. One need not even agree with Baker that the First Amendment exists primarily to promote *individual* self-determination. *See* OWEN M. FISS, LIBERALISM DIVIDED: FREEDOM OF SPEECH AND THE MANY USES OF STATE POWER 5 (1996) (arguing that "the role of the First Amendment is to preserve the fullness and openness of public debate"); CASS R. SUNSTEIN, DEMOCRACY AND THE PROBLEM OF FREE SPEECH (1993) (arguing that the First Amendment should be interpreted with the interest in democratic self-governance in mind). Informational privacy promotes collective self-determination as well. *See* text accompanying notes 188-206 *infra*.

162. *See* Spencer A. Overton, *Mistaken Identity: Unveiling the Property Characteristics of Political Money*, 53 VAND. L. REV. (forthcoming 2000).

163. *See* JAMES BOYLE, SHAMANS, SOFTWARE, AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INFORMATION SOCIETY (1996); Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354 (1999); Diane Leenheer Zimmerman, *Information as Speech, Information as Goods: Some Thoughts on Marketplaces and the Bill of Rights*, 33 WM. & MARY L. REV. 665 (1992).

erally and in the particular case of personally-identified data.[164] It is clear, however, that an approach to information policy that focuses only on information's expressive characteristics (or only on its proprietary aspects) is increasingly untenable.

In sum, as with theories of ownership, theories of speech preclude strong data privacy protection only to the extent that market exchange of informational property for value is considered the essence of the right that the First Amendment protects. Other understandings of the relationship between speech and speech markets, and more generally between information as speech and information as property or commodity, might produce different conclusions about the sorts of data privacy regulation that the First Amendment allows. I turn, therefore, to consideration of whether and how these understandings should matter.

### B. *Speech, Property, and Market Institutions*

As a society, we regulate the exchange of information as property all the time, and do so based on market-institutional considerations. In addition, the law routinely allows private parties to invoke property or contract rights to restrict others' speech. If collections of personally-identified data are like other sorts of regulated information, or if individuals have property or contractual interests that extend to (at least some) personally-identified information on an ongoing basis, the First Amendment landscape changes. The data privacy debate is not merely a debate about trading speech for privacy, although it is still that. Defining the contours of acceptable data privacy regulation becomes a problem of drawing boundaries between competing constitutional considerations—a problem, that is, of making wise constitutional policy.

The law affords numerous instances of regulation of the exchange of information as property or product. Securities markets, which operate entirely by means of information exchange, are subject to extensive regulation, and hardly anybody thinks that securities laws and regulations should be subjected to heightened or strict First Amendment scrutiny.[165] Laws prohibiting patent, copyright, and trademark infringement, and forbidding the misappropriation of trade secrets, have as their fundamental purpose (and their undis-

---

164. Much current scholarship focuses on the use of "property" formalism to override speech concerns. As I discuss, personally-identified data raises the opposite problem. *See* text accompanying notes 170-176 *infra*.

165. *See* Frederick Schauer, *The Aim and the Target in Free Speech Methodology*, 83 NW. U. L. REV. 562, 562-63 (1989); *see also* BOYLE, *supra* note 163, at 81-96. *But see* Burt Neuborne, *The First Amendment and Government Regulation of Capital Markets*, 55 BROOK. L. REV. 5 (1989); Nicholas Wolfson, *The First Amendment and the SEC*, 20 CONN. L. REV. 265 (1988); Aleta G. Estreicher, *Securities Regulation and the First Amendment*, 24 GA. L. REV. 223 (1990).

puted effect) the restriction of information flows.[166] The securities and intellectual property laws, moreover, are expressly content-based, and thus illustrate that (as several leading First Amendment scholars acknowledge) this characterization doesn't always matter.[167] Finally, federal computer crime laws punish certain uses of information for reasons entirely unrelated to their communicative aspects.[168]

In each of these examples, regulation of information markets is based on institutional concerns. The securities laws are designed to ensure that securities markets function as fair and efficient mechanisms for allocating capital and distributing investment risk. The intellectual property laws perform analogous functions for markets in creative capital. Patent and copyright law are expressly designed to foster innovation and to provide a framework for exploiting the economic value of inventive and creative products. Trademark and trade secret law, respectively, constrain unfair and deceptive misappropriation of reputational and innovative goodwill. Federal criminal prohibitions on the theft or misuse of information, meanwhile, protect the institution of private property, and sometimes other institutions as well.[169]

A similar analysis applies to laws regulating the collection, processing, and exchange of personally-identified data. As I have already noted, for each of these activities, the data itself is distinct from the speech that proposes and defines the transaction.[170] That doesn't necessarily mean, though, that the higher level of scrutiny reserved for noncommercial speech regulation should apply. It might mean, instead, that a lesser level of scrutiny is warranted, or that we need not apply First Amendment standards of review at all. The data is itself the subject matter of the transaction—the "goods" exchanged. And, as distinct from news or literature, or from reports of scientific research exchanged among colleagues, it isn't purchased to be "read." Rather, it is purchased to serve a fundamentally different sort of function—that of categorizing and segmenting a customer base.[171]

---

166. *See* 15 U.S.C. §§ 1114, 1125 (1994) (trademark); 17 U.S.C. § 106 (1994 & Supp. IV 1998) (copyright); 18 U.S.C. §§ 1831-1832 (Supp. IV 1998) (trade secret); 35 U.S.C. § 271 (1994 & Supp. IV 1997) (patent).

167. *See* Post, *supra* note 156, at 1265-70; Schauer, *supra* note 165, at 567 ("Thus, if we look beyond the class of cases that have '[F]irst [A]mendment' written all over them, we see everywhere both the inevitability and constitutionality of government regulation inspired precisely by the communicative impact of the regulated conduct."); *cf.* Clay Calvert, *Free Speech and Content-Neutrality: Inconsistent Applications of an Increasingly Malleable Doctrine*, 29 MCGEORGE L. REV. 69 (1997) (noting incoherence of the distinction even within "core" First Amendment cases).

168. *See, e.g.*, 18 U.S.C. §§ 1030, 2701 (1994).

169. *Cf.* Post, *supra* note 156, at 1252 (considering First Amendment implications of laws criminalizing conduct that communicates); Schauer, *supra* note 165, at 566-67 (same).

170. *See* text accompanying notes 138-139 *supra*.

171. *Cf.* Federal Election Comm'n v. Legi-Tech, Inc., 967 F. Supp. 523, 530-31 (D.D.C. 1997) (sustaining a Federal Election Commission order barring commercial resale of political con-

The accumulation, use, and market exchange of personally-identified data don't fit neatly into any recognized category of "commercial speech," in other words, because in the ways that matter, these activities aren't really "speech" at all. Although regulation directed at these acts may impose some indirect burden on direct-to-consumer communication, that isn't the primary objective of data privacy regulation. This suggests that, at most, data privacy regulation should be subject to the intermediate scrutiny applied to indirect speech regulation.[172] And the example of intellectual property, in particular, further suggests that if data privacy regulation incorporates sufficient structural protection for speech-related concerns (on which see Part VI.B., below), then—just as in garden-variety infringement cases—in many cases there will be no need for heightened scrutiny at all.[173]

From an institutional perspective, the unrestricted exchange of personally-identified data vitiates the expected boundaries of commercial interaction. Roughly speaking, we might define those boundaries to include each transaction or series of transactions with a particular type of merchant. As currently constructed, networked databases of personally-identified information do not recognize institutional boundaries or field-of-use restrictions. Data exchange within and across the many different markets experienced by

---

tribution information). *But see* Federal Election Comm'n v. Political Contributions Data, Inc., 943 F.2d 190, 196-98 (2d Cir. 1991) (construing "commercial use" prohibition narrowly).

172. *See* United States v. O'Brien, 391 U.S. 367 (1968) (articulating the intermediate scrutiny standard that applies to indirect burdens on speech).

173. *Cf.* Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 555-60 (1985) (holding that copyright doctrines such as the fair use doctrine and the idea-expression distinction accommodate First Amendment concerns); New Kids on the Block v. News Am. Publ'g, Inc., 971 F.2d 302, 307 (9th Cir. 1992) (defining class of "non-trademark use[s] of a mark" that safeguards First Amendment concerns). There is currently considerable dispute as to the precise location of structural First Amendment safeguards within existing copyright and trademark doctrine. *See, e.g.*, Memorandum in Support of Plaintiff's Motion for Judgment on the Pleadings at 31-52, *Eldred v. Reno*, No. CA99-0065JLG, 31-52 (D.D.C. Oct. 28, 1999) <http://cyber.law.harvard.edu/eldredvreno/sj_memo.pdf>; Benkler, *supra* note 163; Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089, 1133-34 (1998) [hereinafter Cohen, *Self-Help*]; Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996) [hereinafter Cohen, *Right to Read Anonymously*]; Rochelle Cooper Dreyfuss, *Expressive Genericity: Trademarks as Language in the Pepsi Generation*, 65 NOTRE DAME L. REV. 397 (1990); Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147 (1998); Netanel, *supra* note 160; Malla Pollack, *The Right to Know?: Delimiting Database Protection at the Juncture of the Commerce Clause, the Intellectual Property Clause, and the First Amendment*, 17 CARDOZO ARTS & ENT. L.J. 47 (1999); Zimmerman, *supra* note 163; *see also* Burk, *supra* note 156 (predicting similar dispute within patent law as a consequence of Ninth Circuit decision that computer software in object code form qualifies as protected speech). Almost nobody, however, argues that First Amendment principles require heightened scrutiny as to every aspect of every copyright or trademark dispute. *But see* Lemley & Volokh, *supra*, at 183-86 (arguing that because copyright protection is content-based, First Amendment doctrine about prior restraints should govern in disputes about injunctive relief); Eugene Volokh & Brett McDonnell, *Freedom of Speech and Independent Judgment Review in Copyright Cases*, 107 YALE L.J. 2431 (1998) (arguing that the First Amendment requires de novo review of infringement judgments).

individuals is relatively seamless and will become more so. The bounded speech institutions of commerce described by Halberstam are becoming, instead, the total institution—a commercial panopticon whose goal is the precisely calibrated extraction of consumer surplus.[174]

It may be objected that an institutional theory of commercial speech regulation would not tell us what should happen when pressures for change come from within the institution of commercial interaction itself. Halberstam's preliminary and general statement that regulation should seek to preserve expectation, or "social practice" with respect to a "predefined communicative project" might counsel restraint in times of institutional change.[175] The conclusion that the government may never regulate changing institutions, though, leads swiftly (and unsurprisingly) to the conclusion that the government may not seek to regulate social institutions at all. It also begs the question whether particular institutional changes reflect the consensus of all involved parties, or only some.[176] If the latter, then a decision that the First Amendment prohibits the regulation is, inevitably, also a decision about whose interests to privilege—exactly the sort of entrenchment that the First Amendment is supposed to prevent.[177]

The point here is not that the First Amendment imposes no constraints whatsoever on regulation of the collection, use, and exchange of personally-identified data, or that regulation of information exchange does not raise serious, legitimate concerns about the exercise of government power to shape social practice. The point is that these are difficult questions that can't be answered by rote incantation of the proposition that information exchange is speech. It just isn't that simple. Sometimes, speech concerns cannot so easily be disentangled from concerns about commercial practices in markets, and sometimes regulation of information practices within markets really is about commercial fair play.

Let me be quite clear, too, that I do not mean to suggest more generally that the market-exchange value of information is undeserving of constitutional protection. Markets for speech are a vital and indispensable alternative to government production of speech, and an equally indispensable corrective to government abuse and excess. Moreover, a degree of agnosticism about the sorts of speech that facilitate self-determination is essential in

---

174. *See generally* GANDY, *supra* note 91, at 53-94 (characterizing the goal of the data processing industry as seamless panoptic categorization and sorting of individuals); Froomkin, *supra* note 3, at 482-91 (describing the practice of "data mining" based on interlinked digital databases).

175. Halberstam, *supra* note 159, at 831-33.

176. *Cf.* Cohen, *Right to Read Anonymously*, *supra* note 173, at 994-1003 (taking a skeptical view of the argument that disputes about Internet governance can be resolved using the same informal, norm-based mechanisms that are so effective in small, homogeneous communities); Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257 (1998) (same).

177. *Cf.* Overton, *supra* note 162 (arguing that a campaign finance jurisprudence that equates money with speech disserves First Amendment values).

a diverse and pluralistic society. There is a vast difference, though, between saying that markets in information play an important role in creating and sustaining a thriving marketplace of ideas and saying that the two sorts of markets are one and the same, or that every information market plays this role to the same extent. Markets, including information markets, are in and of society, and also serve other important social purposes. The argument that government cannot regulate to promote these other purposes—when plainly it can and does—is absurd.

Entirely apart from considerations of market structure, moreover, we routinely prohibit certain uses of gathered information that we deem inconsistent with shared notions of human dignity and equality. For example, we prohibit race-based classification by private parties in virtually every aspect of commercial life without regard to whether statistical correlations exist between, say, race and loan default rates.[178] No one seriously argues that this practice infringes on protected speech. As discussed in Part IV, moreover, the conclusion that the data captured by transactional profiling yield an accurate portrait *of the individual*, and that more of it will yield a better portrait, is open to serious criticism. We might reasonably conclude that the First Amendment does not forbid giving dignity principles broader scope.

Balancing speech claims against data privacy claims also requires consideration of "information as property" in a wholly different sense. Arguments from speech assume a resolution of the property question favorable to data processors, and thus no conflict between property rights and speech rights. If personally-identified data is no one's property, or property of the person who collects it, then of course this is correct. No conflict exists; to the contrary, any property interests that do exist are added to the scales on the side of (data processors') speech. But if, instead, personally-identified data is the property or quasi-property of the individual to whom it refers, then data processors' asserted speech rights cannot be absolute, and may not prevail at all.[179]

By the same token, data privacy opponents ignore the implications of their own freedom-of-contract paradigm for arguments from freedom of

178. *See, e.g.*, 42 U.S.C. § 2000e-2 (1994) (employment); *id.* §§ 3601-3604 (1994) (housing).

179. *Compare* Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569 (1994) (holding copyright claims limited in some circumstances by First Amendment concerns), Marsh v. Alabama, 326 U.S. 501 (1946) (same for real property rights), *and* New Kids on the Block v. News Am. Publ'g, Inc., 971 F.2d 302 (9th Cir. 1992) (same for trademark rights), *with* Frisby v. Schultz, 487 U.S. 474 (1988) (holding First Amendment claims limited by residential real property rights), San Francisco Arts & Athletics, Inc. v. United States Olympic Comm., 483 U.S. 522 (1987) (same for sui generis statutory right to control uses of "Olympic"), Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539 (1985) (same for copyright), and Hudgens v. NLRB, 424 U.S. 507 (1976) (same for commercial real property rights). *Frisby* is particularly suggestive, for there the Court invoked personhood-related interests in the privacy of the home to support speech restrictions. *See* Frisby, 487 U.S. at 484.

speech. Courts routinely enforce private, contractual restrictions on expression.[180] It is hard to see why contractual restrictions on the use and exchange of personally-identified data should be presumptively *un*enforceable.[181]

The proper relation between competing property rights and speech rights, and between freedom of contract and freedom of speech, is bitterly contested.[182] Moreover, I would argue that speech concerns were given insufficient weight in most (but not all) of the cases just cited. My purpose here is not to locate either boundary at a particular point, but simply to point out the illogic of concluding that a First Amendment right to exchange personally-identified data trumps any and all rights that individuals might assert to prevent such exchange. Here again, recourse to neutral, categorical arguments about the paramount importance of speech rights masks a basic inequality in our understanding of who may enjoy these rights. If the powerful may exert property rights or invoke contractual obligations to prevent or limit speech, so too may others.[183] Juxtaposing data privacy opponents' "speech" arguments with their arguments from "property" compounds the inequality. Taken together, these arguments assert that personally-identified data may be their property or their speech, as it suits them.[184]

For information that has characteristics of both property and speech, the questions whether speech rights should limit property or contract rights, and if so how, can't be resolved by formalistic resort to either category. (And so—again, let me be quite clear—the assertion of countervailing property or contract rights shouldn't end the inquiry, either.) Instead, these are questions that require context-sensitive balancing to answer. Again, copyright offers a useful way to think about the interaction between competing property/contract and speech rights in personally-identified data. It is well-recognized that the First Amendment protects some unauthorized uses of

---

180. *See, e.g.*, Cohen v. Cowles Media Co., 501 U.S. 663 (1991) (media source confidentiality agreement); Snepp v. United States, 444 U.S. 507 (1980) (nondisclosure agreement imposed pursuant to contract and fiduciary duty); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 41 cmt. d (1995) (discussing trade secrecy confidentiality agreements); *see also* Kang, *supra* note 13, at 1267-84 (proposing contract-based data privacy statute).

181. *See* Volokh, *supra* note 134 (acknowledging this point).

182. On the tension between speech rights and property rights, see Mark Cordes, *Property and the First Amendment*, 31 U. RICH. L. REV. 1 (1997); and the sources cited in note 173 *supra*. On the tension between speech rights and contract rights, see Alan E. Garfield, *Promises of Silence: Contract Law and Freedom of Speech*, 83 CORNELL L. REV. 261 (1998); see also Cohen, *Self-Help*, *supra* note 173; Niva Elkin-Koren, *Copyrights in Cyberspace—Rights Without Laws?*, 73 CHI.-KENT L. REV. 1155 (1998); William W. Fisher III, *Property and Contract on the Internet*, 73 CHI.-KENT L. REV. 1203 (1998).

183. For the converse argument (and thus a more consistent speech absolutism), see Lemley & Volokh, *supra* note 173, at 197-98 & n.230.

184. *Cf.* John O. McGinnis, *The Once and Future Property-Based Vision of the First Amendment*, 63 U. CHI. L. REV. 49, 70 (1996) (arguing that the First Amendment was intended to protect "natural property rights" in speech).

others' copyrightable expression.[185] It does not, however, shield any and all unauthorized uses, and the point at which its protection ends is the point at which authors' property rights begin.[186] The one is a correlative of the other, and the precise location of the boundary between the two is a function of public policy concerns. The same is true of the boundary between speech and contract; the argument now in vogue that "contract" is different than "property" and so trumps public policy limits on copyright commits exactly the error I seek to avoid.[187]

It bears repeating, once again, that data privacy protection would rest on very different policy concerns than copyright; thus, we might not choose to strike the balance between speech and property, or between speech and contract, in the same way. What copyright reminds us is that we may choose the boundary between data privacy rights and speech rights with both ownership and expressive freedoms in mind. Identifying property/contract claims in tension with speech claims doesn't end the analysis; it begins it.

* * * *

The speech objection to data privacy regulation is important, but not absolute. Calling data exchange "speech" doesn't mean it can't be regulated, and doesn't (without more) tell us much about the sorts of regulation to allow. Balancing data privacy concerns against the speech rights of third parties requires closer consideration of both the nature of ownership and contractual interests in personally-identified information and the extent to which data privacy regulation is really directed at the exchange of information as property rather than as speech. Whether speech trumps privacy, in other words, depends to a considerable extent on our understandings of property, choice, and information—and thus illustrates, again, both the ways in which the conventional understandings of these categories reinforce each other and the ways in which different understandings might yield different answers. Part VI explores a theory of data privacy that these different understandings might support—one that begins with consideration of the developmental conditions that are necessary for individuals to become autonomous decisionmakers and speakers in their own right.

---

185. *See Harper & Row*, 471 U.S. at 555-60.

186. *See id.*

187. *See, e.g.*, Bell, *supra* note 41; Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. CHI. LEGAL F. 217; Merges, *supra* note 54; Nimmer, supra note 40; Maureen A. O'Rourke, *Copyright Preemption After the* ProCD *Case: A Market-Based Approach*, 12 BERKELEY TECH. L.J. 53 (1997). *See generally* Cohen, *supra* note 44, at 481-90, 517-38 (analyzing this argument and rejecting it as a matter of economic theory); Cohen, *Self-Help*, *supra* note 173, at 1128-37 (analyzing this argument and rejecting it as a matter of copyright law and policy).

## VI. BECOMING: TOWARD A DYNAMIC THEORY OF INFORMATIONAL PRIVACY

It is conventional to justify trade in personally-identified data with reference to individual liberty. Yet, as this discussion has shown, on sustained examination the concern with the individuals who are data subjects proves relatively superficial. The rhetorics of liberty mask the fact that, at a more fundamental level, data privacy discourse has been driven by concerns for the autonomy of those who would objectify individuals—with the rights of the data processor as owner, trader, vendor, speaker, chooser. If we are serious about fostering individual freedom in reality as well as in rhetoric, this is an odd result.

What is needed, instead, is a dynamic theory of informational privacy—one that focuses on the conditions for meaningful autonomy in fact. The theory must be grounded in a considered appreciation of the benefits of shadow as well as those of sunlight. This Part lays the theoretical and practical foundations for an autonomy-based approach to data privacy protection, and argues that such protection need not threaten the important social and political benefits that access to information provides.

### A. *The Values of Informational Privacy*

Prevailing market-based approaches to data privacy policy—including "solutions" in the form of tradable privacy rights or heightened disclosure requirements before consent—treat preferences for informational privacy as a matter of individual taste, entitled to no more (and often much less) weight than preferences for black shoes over brown or red wine over white. But the values of informational privacy are far more fundamental. A degree of freedom from scrutiny and categorization by others promotes important noninstrumental values, and serves vital individual and collective ends.

First, informational autonomy comports with important values concerning the fair and just treatment of individuals within society. From Kant to Rawls, a central strand of Western philosophical tradition emphasizes respect for the fundamental dignity of persons, and a concomitant commitment to egalitarianism in both principle and practice.[188] Advocates of strong data privacy protection argue that these principles have clear and very specific implications for the treatment of personally-identified data: They require that we forbid data-processing practices that treat individuals as mere conglomerations of transactional data, or that rank people as prospective customers, tenants, neighbors, employees, or insureds based on their financial or

188. *See* IMMANUEL KANT, THE METAPHYSICS OF MORALS 73-74, 231-32 (Mary Gregor ed. & trans., Cambridge Univ. Press 1996) (1797); JOHN RAWLS, A THEORY OF JUSTICE (rev. ed. 1999).

genetic desirability. The drafters of the European Data Protection Directive agreed with this characterization; the Directive is explicitly grounded in "the fundamental rights and freedoms of natural persons."[189]

Arguably, however, the leap from normative first principles to the European model of fair information practice requires further explanation. In theory, at least, a market model of tradable privacy rights is fully consistent with first-order normative commitments to dignity and equality, in that it treats each individual as an autonomous, rational actor and presumes that all individuals are equally capable of ascertaining and pursuing the goals that will maximize their own happiness. As discussed in Parts III and IV, though, individuals experience substantially less choice about data-processing practice, and enjoy substantially less agency, than the rational-actor model predicts. The disjunction arises because the rational-actor model (even modified to acknowledge preferences for privacy as legitimate) devotes no attention to how individuals attain autonomy in fact—that is, to how we develop the capacity and facility for choice.

Autonomous individuals do not spring full-blown from the womb. We must learn to process information and to draw our own conclusions about the world around us. We must learn to choose, and must learn something before we can choose anything. Here, though, information theory suggests a paradox: "Autonomy" connotes an essential independence of critical faculty and an imperviousness to influence. But to the extent that information shapes behavior, autonomy is radically contingent upon environment and circumstance. The only tenable resolution—if "autonomy" is not to degenerate into the simple, stimulus-response behavior sought by direct marketers—is to underdetermine environment. Autonomy in a contingent world requires a zone of relative insulation from outside scrutiny and interference—a field of operation within which to engage in the conscious construction of self. The solution to the paradox of contingent autonomy, in other words, lies in a second paradox: To exist in fact as well as in theory, autonomy must be nurtured.[190]

A realm of autonomous, unmonitored choice, in turn, promotes a vital diversity of speech and behavior. The recognition that anonymity shelters constitutionally-protected decisions about speech, belief, and political and intellectual association—decisions that otherwise might be chilled by un-

189. *See* European Data Protection Directive, *supra* note 4, at art. 1(1).

190. This insight appears, in more limited form, in the literature on organizational theory and psychology. This literature recognizes that autonomy is an important factor in workplace productivity, and requires investment and forethought to develop. *See, e.g.*, Steve Williams, *An Organizational Model of Choice: A Theoretical Analysis Differentiating Choice, Personal Control, and Self-Determination*, 124 GENETIC SOC. & GEN. PSYCH. MONOGRAPHS 465 (1998) (summarizing research).

popularity or simple difference—is part of our constitutional tradition.[191] But the benefits of informational autonomy (defined to include the condition in which no information is recorded about nonanonymous choices) extend to a much wider range of human activity and choice. We do not experiment only with beliefs and associations, but also with every other conceivable type of taste and behavior that expresses and defines self. The opportunity to experiment with preferences is a vital part of the process of learning, and learning to choose, that every individual must undergo.[192]

The benefits of informational privacy are related to, but distinct from, those afforded by seclusion from visual monitoring. It is well-recognized that respite from visual scrutiny affords individuals an important measure of psychological repose. Within our society, at least, we are accustomed to physical spaces within which we can be unobserved, and intrusion into those spaces is experienced as violating the boundaries of self.[193] But the scrutiny, and the repose, can be informational as well as visual, and this does not depend entirely on whether the behavior takes place "in private." The injury, here, does not lie in the exposure of formerly private behaviors to public view, but in the dissolution of the boundaries that insulate different spheres of behavior from one another.[194] The universe of all information about all record-generating behaviors generates a "picture" that, in some respects, is more detailed and intimate than that produced by visual observation, and that picture is accessible, in theory and often in reality, to just about anyone who wants to see it. In such a world, we all may be more cautious.

The point is not that people will not learn under conditions of no-privacy, but that they will learn differently, and that the experience of being

---

191. *See* Cohen, *Right to Read Anonymously*, *supra* note 173, at 1006-14; Kreimer, *supra* note 9, at 59-71. *See generally* Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect,"* 58 B.U. L. REV. 685 (1978) (defining and discussing this "chilling" effect); Lee Tien, *Who's Afraid of Anonymous Speech?* McIntyre *and the Internet*, 75 OR. L. REV. 117 (1996) (defending online anonymity).

192. *See* Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 754-55 (1999) ("Privacy is a matter of escaping as well as embracing encumbrances of identity. Without adequate privacy, there can be no meaningful identities to embrace or escape, and no opportunities to engage in meaningful reflection, conversation, and debate about the grounds for embracing, escaping, and modifying particular identities."); Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL L. REV. 451, 514 (1995) (discussing and developing a conceptual framework for health information privacy); Kreimer, *supra* note 9, at 69-70 ("[E]xposure as the author of an action or statement links that action to our identity; the broader the exposure, the more indissoluble the link and the harder it is to disavow it.").

193. *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 32-42, 57-60 (1967); Thomas Scanlon, *Thomson on Privacy*, 4 PHIL. & PUB. AFF. 315, 317 (1975); Barry Schwartz, *The Social Psychology of Privacy*, 73 AM. J. SOCIOL. 741, 745-51 (1968).

194. *See* Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 L. & PHIL. 559 (1998); Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 984-85 (1989); Jonathan Schonsheck, *Privacy and Discrete "Social Spheres,"* 7 ETHICS & BEHAV. 221 (1997).

watched will constrain, ex ante, the acceptable spectrum of belief and behavior.[195] Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream. The result will be a subtle yet fundamental shift in the content of our character, a blunting and blurring of rough edges and sharp lines. But rough edges and sharp lines have intrinsic, archetypal value within our culture. Their philosophical differences aside, the coolly rational Enlightenment thinker, the unconventional Romantic dissenter, the skeptical pragmatist, and the iconoclastic postmodernist all share a deep-rooted antipathy toward unreflective conformism.[196] The condition of no-privacy threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it.[197]

The autonomy fostered by informational privacy also generates more concrete collective benefits. Development of the capacity for autonomous choice is an indispensable condition for reasoned participation in the governance of the community and its constituent institutions—political, economic, and social.

The cornerstone of a democratic society is informed and deliberate self-governance. The formation and reformation of political preferences—essential both for reasoned public debate and informed exercise of the franchise—follows the pattern already discussed: Examination chills experimentation with the unorthodox, the unpopular, and the merely unfinished. A robust and varied debate on matters of public concern requires the opportunity to experiment with self-definition in private, and (if one desires) to keep distinct social, commercial, and political associations separate from one another.[198] Here again the point is relative. People will still make choices under conditions of no-privacy, and targeted commercial advertising can be used to

---

195. Research in cognitive psychology indicates that lack of privacy makes people both less inclined to experiment and less inclined to seek help. *See* Stuart A. Karabenick & John R. Knapp, *Effects of Computer Privacy on Help-Seeking*, 18 J. APPLIED SOC. PSYCH. 461 (1988); NEW DIRECTIONS IN HELPING: HELP-SEEKING (Jeffrey D. Fisher, Arie Nadler & Bella M. DePaulo eds., 1983); *see also* Kreimer, *supra* note 9, at 52-53 n.145. Individuals who experiment with unpopular views or behavior also must consider the possibility of physical, economic, or social sanctions. *See* Kreimer, *supra* note 9, at 39-54; Gostin, *supra* note 192, at 490-91.

196. *See, e.g.*, RICHARD A. POSNER, OVERCOMING LAW (1995); STEVEN H. SHIFFRIN, THE FIRST AMENDMENT, DEMOCRACY, AND ROMANCE (1990); DUNCAN KENNEDY, A CRITIQUE OF ADJUDICATION (FIN DE SIECLE) (1997).

197. *See* Schwartz, *supra* note 93, at 1654-57. Postmodern literary theory holds that to name a thing or person is prima facie to limit its potentiality. *See* JUDITH BUTLER, EXCITABLE SPEECH: A POLITICS OF THE PERFORMATIVE 2-7 (1997). This reasoning has been invoked to support limits on hate speech, on the ground that such speech has "performative" significance. *See id.* at 2-7. This is not to say that direct marketing and hate speech are the same or even comparable—plainly, they are not—but rather that there are categories of speech that have concrete impact on an individual's development as an autonomous speaker, and thus exist uneasily at the boundary between expression and action.

198. *See* Kreimer, *supra* note 9, at 59-71; Schwartz, *supra* note 93, at 1650-54.

manufacture political preferences (or political apathy) as well. But if we do not wish to live in communities governed by apathy, impulse, or precautionary conformism, we must produce individuals capable of governing themselves.[199]

The same qualities that produce the capacity for political self-government also produce innovation in markets and in the governance of market institutions. I have argued that the welfare of markets is properly viewed as subordinate to the welfare of society as a whole, but it does not follow that markets are unimportant. The health of markets as institutions within a democratic society is vitally important to overall social welfare. And dynamic, competitive markets require inventors as well as consumers and entrepreneurs as well as audiences.[200] Inventiveness and entrepreneurship, in turn, require the ability to think outside or around existing, predictable technological and social patterns. A regime built on pervasive practices of monitoring, prediction, and preference-shaping is far more likely to stifle these habits of independent thought than to stimulate them.

At the same time, though, the insulation provided by informational privacy also plays a subtler, more conservative role in reinforcing the existing social fabric. Sociologist Erving Goffman demonstrated that the construction of social facades to mediate between self and community is both instinctive and expected.[201] Alan Westin describes this social dimension of privacy as "reserve."[202] This characterization, though, seems incomplete. On Goffman's account, the construction of social personae isn't just about withholding information that we don't want others to have. It is about defining the parameters of social interaction in ways that maximize social ease, and thus is about collective as well as individual comfort.[203] We do not need, or even want, to know each other that well. Less information makes routine interactions easier; we are then free to choose, consensually and without embarrassment, the interactions that we wish to treat as less routine. Informational privacy, in short, is a constitutive element of a civil society in the broadest sense of that term.

Last, but hardly least, a societal commitment to informational privacy has an important role to play in defining our collective vision of the role of

---

199. *Cf.* Netanel, *supra* note 160, at 343 ("A state whose citizenry has not internalized these skills and values will rule through fiat and obedience, without any sense, so vital to our understanding of democracy, that its laws and social norms originate in the commitments of a self-governing polity."). Netanel notes, as well, that self-governance also occurs outside the formal bounds of "government." *See id*.

200. *See, e.g.*, SAMUEL BOWLES & RICHARD EDWARDS, UNDERSTANDING CAPITALISM: COMPETITION, COMMAND, AND CHANGE IN THE U.S. ECONOMY (1985); JOSEPH A. SCHUMPETER, CAPITALISM, SOCIALISM AND DEMOCRACY (1942).

201. *See* ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959).

202. *See* WESTIN, *supra* note 193, at 32.

203. *See* GOFFMAN, *supra* note 201, at 8-10, 113-40, 229-33; Post, *supra* note 194, at 984-86.

information technologies, and technique more broadly, within society.[204] Technological progress affords a yardstick for measuring human achievement, but not the only or most important one.[205] To appreciate other measures of progress, we must be sensitive to the limits of technique, and recognize the hubris inherent in pretensions to total prediction and control.[206] A protected zone of informational autonomy is valuable, in short, precisely because it reminds us what we cannot measure.

### B. *Informational Privacy in Practice*

As the foregoing discussion shows, there are compelling theoretical and practical justifications for legislating strong data privacy protection that creates and preserves a zone of informational autonomy for individuals. To be both effective and constitutional, data privacy legislation must solve three difficult problems. First, it must strike the right balance between ownership and speech concerns, by defining the scope of protection in a manner that excludes constitutionally-privileged uses of personally-identified data. Second, it must define the appropriate parameters of choice about privacy practices, to ensure that consent to the collection, use, and exchange of personally-identified data is informed and meaningful. Finally, it must incorporate additional protections that hold the data processing industry accountable, both to individuals and to the larger society within which it operates, for its practices regarding information use.

Although neither speech nor "truth" concerns preclude strong data privacy protection, legislation designed to protect informational privacy nonetheless must provide for both constitutionally-required and socially-valued uses of personally-identified information. Data privacy opponents of widely varying persuasions argue that this simply cannot be done. Libertarian data privacy opponents contend that a right to prevent use and disclosure of personally-identified data necessarily threatens valuable and constitutionally-protected journalistic and research activities.[207] From the communitarian movement, meanwhile, comes the argument that data privacy rights would foreclose uses of personally-identified data that protect the public health and safety.[208] Both libertarian and communitarian objections, however, assume that any entitlement in personally-identified data must take the form of a tra-

---

204. *See* text accompanying notes 119-121 *supra* (discussing relationship between information technology and the construction of knowledge).

205. *Cf.* Margaret Chon, *Postmodern "Progress": Reconsidering the Copyright and Patent Power*, 43 DEPAUL L. REV. 97 (1993) (arguing that the definition of "progress" is socially constructed and should be shaped by social values and human priorities).

206. *See generally* BORGMANN, *supra* note 2 (identifying prediction and control as central, and deeply flawed, organizing principles of modern (Western) society).

207. *See* SINGLETON, *supra* note 51, at 7; Volokh, *supra* note 134.

208. *See* AMITAI ETZIONI, THE LIMITS OF PRIVACY (1999).

ditional "property" right—a right against all comers and all uses. Again, the example of intellectual property, and in particular copyright, shows that this need not be so. Copyright confers a set of enumerated rights against particular types of conduct, but does not forbid other, unenumerated uses of protected works.[209] In addition, the Copyright Act specifies a number of important exceptions to owners' rights; these limitations are expressly designed to balance competing public policy goals.[210] Similarly, a theory of informational privacy may, and should, be crafted to preserve the benefits of sunlight.

The objection that broad data privacy protection will threaten press freedoms is worth taking seriously. The threat is, however, avoidable if the right is defined narrowly. The First Amendment right to publish personally-identified facts is not absolute. It is constrained, first, by a newsworthiness (or "public concern") limitation.[211] Most facts about individual transactions will not be "newsworthy" in the constitutional sense; larger trends in purchasing habits may well be, but (as discussed below) data privacy protection won't prevent the study of these. More important, the First Amendment protects the right to publish information lawfully obtained through one's own efforts.[212] It neither presumes nor guarantees a preexisting social practice consisting of the pervasive collection and aggregation of personally-identified data by third-party "infomediaries." A reporter may follow a public figure into the store, and we also may decide that First Amendment values require statutory leeway to obtain transactional data about named individuals

---

209. *See* 17 U.S.C. §§ 106, 106A (1994 & Supp. IV 1998).

210. *See, e.g.*, 17 U.S.C. §§ 102(b) (1994) (excluding from copyright protection ideas, methods of operation, and the like); *id.* § 107 (fair use doctrine); *id.* § 108 (copying privileges for libraries); *id.* § 109(a) (first sale doctrine) ; *id.* § 110 (Supp. IV 1998) (public performance and display exemptions for nonprofit activities and organizations); Feist Publications, Inc. v. Rural Tel. Serv., Inc., 499 U.S. 340, 349-50 (1991) (holding that denial of copyright protection for facts is constitutionally compelled); Cohen, *supra* note 44, at 543-51, 555-59 (discussing shared public benefits produced by copyright limitations); Lemley, *supra* note 38, at 993-99 (same); Jessica Litman, *The Public Domain*, 39 EMORY L.J. 965 (1990) (explaining the ways in which a rich public domain bolstered by copyright limitations promotes ongoing creative progress).

211. *See, e.g.*, Florida Star v. B.J.F., 491 U.S. 524 (1989); Edelman, *supra* note 147, at 1228-35; Kang, *supra* note 13, at 1280 n.348. In theory, at least, this limitation allows tort liability for invasion of privacy based on publication of private facts, or of a private person's name or likeness. As Edelman and Kang note, courts take an extremely broad view of what constitutes a matter of public concern. Yet even so, the mundane transactional details that fill commercial databanks are unlikely to qualify. Although a tort action may not currently lie for publication of such details, *see* William J. Fenrich, *Common Law Protection of Individuals' Rights in Personal Information*, 65 FORDHAM L. REV. 951, 989-94 (1996), data privacy legislation may constitutionally bar publication. *Cf.* Joseph Elford, *Trafficking in Stolen Information: A "Hierarchy of Rights" Approach to the Private Facts Tort*, 105 YALE L.J. 727 (1995) (offering a reconceptualization designed to preserve the private facts tort and extend it to profiling activities).

212. *See Florida Star*, 491 U.S. at 533. For this reason, the libertarian argument that data privacy protection will chill casual conversation about others, *see* Volokh, *supra* note 134, is simply silly.

directly from (certain types of) vendors, if the vendors are willing.[213] But a right against the accumulation, reuse, and sale of *collections* of personally-identified information threatens nothing to which the press, or anyone else, is entitled.[214]

The argument that data privacy protection will threaten valuable research, on the other hand, mistakenly conflates the two very different activities of data analysis and direct-to-consumer communication. Certainly, much valuable research proceeds by collecting and processing data from and about individuals.[215] But in most cases, the data need not remain personally-identified or -identifiable for the research to proceed and to generate its intended results. Empirical studies of population samples seek knowledge about groups, not about individuals.[216] A statutory requirement that research data be stripped of personal identifiers will hinder subsequent efforts to market new, improved products directly to targeted individuals, but it won't hinder efforts to study demographics, tastes, and trends.

Certain industries do require the exchange of personally-identified data in order to function. Prominent examples include the credit reporting, health care and biomedical research, insurance and financial services, and higher education industries. All serve important social needs, and none would survive an outright ban on the accumulation and exchange of personally-identified data. It doesn't follow, though, that members of these industries should enjoy blanket immunity from data privacy protection.[217] Allowing

---

213. Sector-specific laws guaranteeing informational privacy for video and cable patrons don't even provide this much, and (as far as I can tell) no one thinks these laws violate the First Amendment. *See* 18 U.S.C. § 2710; 47 U.S.C. § 551; Kang, *supra* note 12, at 1282.

214. As Part V.B noted, such a right arguably places an indirect burden on direct marketers' communications to consumers. *See* text accompanying notes 172-173 *supra*. Even so, however, Part VI.A. delineates very substantial government interests, and the restriction is appropriately tailored. *See* text accompanying notes 188-206 *supra*; *see generally* United States v. O'Brien, 391 U.S. 367 (1968) (articulating standard for First Amendment review of laws that indirectly burden speech). Strong data privacy protection would not prevent direct marketers from communicating with consumers via direct solicitation, or from tailoring their messages to the demographic characteristics of different customer pools; it simply would limit their ability to categorize individual consumers. *See* text accompanying notes 101-105 *supra*. More fundamentally, the examples discussed in Part V.B illustrate that resort to *O'Brien* analysis may not be necessary. We don't, for example, require all securities regulations to pass *O'Brien* scrutiny simply because there might (and undoubtedly will) be indirect effects on someone's speech.

215. One notable example is the census, which is also constitutionally-mandated. *See* U.S. CONST. art I, § 2, cl. 3.

216. *But cf.* Burkert, *supra* note 60, at 131-33 (noting that in some circumstances group profiles may be used unfairly).

Situations in which data must remain personally-identifiable can be handled with appropriate sector-specific regulation. *See, e.g.*, Gostin, *supra* note 192 (discussing the problem of protecting privacy in personal health care information).

217. All of these industries are already subject to a degree of privacy-related regulation. *See, e.g.*, Graham-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, Title V, §§ 501-527, 113 Stat. 1338 (1999) (financial services); Consumer Credit Protection Act, 15 U.S.C. §§ 1681-1681t (1994 & Supp. IV 1998) (consumer credit reporting); 20 U.S.C. §1232(g) (1994 & Supp. IV

privileged industries carte blanche to determine which items of data to collect and share would endorse the categorical error discussed in Part III: It would inscribe the technocratic paradigm of knowledge, and of power over knowledge, that data privacy protection seeks to avoid. Instead (and the only alternative), data privacy legislation must include special provisions covering these industries, and specifying the types of information to which the privilege extends and the standards of fair information practice governing their use.

The communitarian social-benefit objection raises a slightly different, and more difficult, problem. The uses of personally-identified data claimed as beneficial—sexual offender tracking, HIV notification programs, and the like—all involve government.[218] This article has focused largely on the privacy problems created by large commercial databases. I don't intend to suggest, though, that government collection and cross-referencing of personal data poses a lesser privacy threat. We should be concerned, moreover, about spillover effects—about private-sector access to data compiled by the government, and vice versa. A broadly-drafted prohibition on the transfer and aggregation of personally-identified data, applicable to private and public sectors alike, is the best way to minimize all of these threats.[219] We may conclude that collection and use of particular items of data by particular governmental units is justifiable (or unavoidable).[220] And in some cases, we may conclude that the First Amendment or related concerns require government to disclose the data it has collected.[221] But these facts don't justify per-

---

1998) (higher education); Protection of Human Subjects, 45 C.F.R. § 46.101 *et seq.* (1993) (biomedical research); *se also* U.S. Dept. of Health & Human Servs., Standards for Privacy of Individually Identifiable Health Information, Proposed Rule, 64 FED. REG. 59,918 (Nov. 3, 1999) (health care information).

218. Etzioni advocates strong protection against private-sector data processing activities. *See* ETZIONI, *supra* note 208, at 141-82.

219. For a thorough summary of the data privacy rules that currently govern private and public sectors within the U.S., see SCHWARTZ & REIDENBERG, *supra* note 10.

220. I take no position on the specific uses that Etzioni advocates. *See id.*

221. *See, e.g.*, United Reporting Publ'g Corp. v. California Highway Patrol, 146 F.3d 1133 (9th Cir. 1998), *rev'd sub nom.* Los Angeles Police Dep't v. United Reporting Publ'g Corp., 120 S. Ct. 483 (1999) (names of arrestees) (holding that the state was not constitutionally required to disclose this information); Federal Election Commission v. Political Contributions Data, Inc., 943 F.2d 190 (2d Cir. 1991) (names of contributors to political campaigns) (holding that a statute requiring disclosures but restricting commercial use of information struck a constitutionally permissible balance). I cite these cases solely to illustrate the sorts of data that are likely to raise issues of legitimate public concern; I take no position on the breadth of the disclosures authorized by the actual statutes at issue, or on whether the First Amendment should be interpreted to require that these items be disclosed at all. My analysis suggests, moreover, that stricter "commercial use" restrictions for government-disclosed information would be entirely permissible, and good policy. And in some cases, we should conclude that the First Amendment or other constitutional provisions *bar* disclosure. *See* Cohen, *Right to Read Anonymously*, *supra* note 173, at 1003-19 (arguing that First Amendment protects against disclosure of reading habits and other speech-related preferences); Kreimer, *supra* note 9, at 62-71.

vasive government accumulation, aggregation, and cross-referencing of personally-identified data any more than the public benefits of credit reporting justify allowing credit bureaus unlimited freedom to design their own data processing mandates. The baseline presumption should be one of strong data privacy protection; exceptions should be carefully considered and narrowly circumscribed.

The next set of questions that data privacy legislation must address concerns the conditions for consent to the release and reuse of personally-identified data. The first question, of course, is why this information needs to be market-alienable at all. As discussed in Part II, exchange value is a customary attribute of property rights, but not a necessary one. Yet people may have legitimate reasons for trading privacy for value in particular cases, when the benefits and costs are reasonably capable of estimation and reasonably immediate. Presumably for this reason, even the European Data Protection Directive does not require Member States to prohibit trade in most types of personally-identified data; instead, it authorizes a market-inalienability approach only for particularly sensitive categories of data, such as those relating to race, religion, and sexual preference.[222] Because these latter sorts of information are especially closely related to dignity concerns, and especially likely to be used in dignity-destroying ways, we may wish to do likewise. Then, though, we must consider the vast majority of data that this rule will not cover.

As Part III.B explains, current data-processing practices provide individuals with so little information about the uses of personally-identified data, and their associated costs and benefits, that consent to these practices cannot plausibly be called "informed."[223] In particular, the farther removed a particular use of personally-identified data is from its initial collection—whether in terms of subject matter, time, or the nature of the entity making the use—the more difficult it will be for individuals to foresee the use, estimate its likelihood, and arrive at an ex ante valuation. Failure to correct for these information problems could negate every protection the statute seeks to provide. It is far from clear that the adoption of P3P technology alone will do the job; P3P will allow individuals to indicate at least some of their preferences (once, up front) at a higher level of granularity, but won't necessarily require vendors to provide the kind of detail about contemplated uses that individuals need to make these choices in the first place.[224] To be effective, data privacy protection must define the conditions for effective consent.

First and most obviously, consent cannot be meaningful as to unknown uses or unspecified recipients. In theory, effective data privacy legislation

---

222. *See* European Data Protection Directive, *supra* note 4, at art. 8.

223. *See* text accompanying notes 82-88 *supra*.

224. *See* text accompanying notes 64-65 *supra*.

should require that individuals be given specific information, and the opportunity to consent or refuse, as to each contemplated reuse or transfer. The European Data Protection Directive adopts this fully-specified model.[225] As a practical matter, it may be sufficient to aggregate certain categories of use or transfer, and require express consent as to each category. Some uses and/or recipients, however, may be so significant that most people would prefer to require particularized consent—for example, the sale of information about grocery or alcohol purchases to employers or health insurers.

Relatedly, provisions defining the scope of consent must specify what constitutes a business enterprise for purposes of privileges to use personally-identified data. Given trends toward horizontal and vertical integration, a broad view of who may exercise the privileges granted by individuals could surrender substantially more control than intended. To avoid this result, both use privileges and any accompanying "legitimate business purpose" or "functionally necessary" exceptions should extend only to the specific business unit or subunit that collected the data initially.[226] The same proviso, moreover, applies to government reuse of personally-identified data. Assuming that the government may compel the provision of at least some types of personal information, it does not follow that the information should be shared across governmental units as a matter of routine practice.

Second, the quality of consent attenuates over time. As Part III.B. discusses, it is very difficult to predict the kinds of uses likely to be made of personally-identified data ten years hence, much less to estimate their significance.[227] Logically, then, consent to the reuse or transfer of personally-identified data should expire after a fixed time period; uses extending past the specified time period should require a new agreement. Like the enumerated-rights model, the notion of time-limited consent has precedent in the Copyright Act, which gives authors who transfer their copyrights a power of termination after thirty-five years.[228] This "termination of transfers" provision is intended to protect authors in the event of dramatic and unforeseeable increases in the value of a work, or unforeseeable improvements in distribution technology.[229] A similar provision in data privacy legislation could protect individuals against new and unforeseeable uses of their information.

---

225. *See* European Data Protection Directive, *supra* note 4, at arts. 6, 7, 11, 14.

226. Many commentators have noted that "legitimate business purpose" exceptions introduce vague and potentially ruinous loopholes into data privacy law. *See* SWIRE & LITAN, *supra* note 13, at 34-35; Kang, *supra* note 13, at 1271; Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 519 (1996). Jerry Kang's proposal to allow routine use only to the extent "functionally necessary" to the operation of the data processor's business is a significant improvement. *See* Kang, *supra* note 13, at 1271-72.

227. *See* text accompanying notes 87-88 *supra*.

228. *See* 17 U.S.C. § 203 (1994 & Supp. IV 1998)

229. *See* H.R. REP. NO. 94-1476, at 124 (1976); 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 9.02 (1999).

The duration of consent to reuse of personally-identified data should be substantially shorter, however. In the case of copyright, both author and publisher have an interest in allowing the publisher enough time to recoup the value of its investment in the work. Where personally-identified data are concerned, there is no such commonality of interest.

Third, consent to limited reuse and exchange of personally-identified data is meaningless if recipients may transfer the data to third parties without the restrictions that accompanied the initial transfer. Instead, as the European Data Protection Directive provides, each use or transfer by a third-party recipient should require a separate act of consent.[230] This recommendation diverges markedly from copyright policy. Under the Copyright Act, an author may control only the first sale of her work.[231] This, though, is a good example of an area where the different policies underlying copyright protection and data privacy protection should matter. The first sale doctrine represents a considered judgment that society's interest in the broad dissemination of creative works, and in the free alienability of tangible goods, outweighs the author's interest in seeking additional remuneration.[232] Durable restrictions on the uses of personally-identified data, in contrast, promote the individual's interest in dignity and autonomy, and there is no comparable societal interest in unfettered dissemination. Instead, as Part VI.A explains, society's interests align substantially with the individual's.[233]

It may be objected that these provisions would define consent so narrowly as to leave no meaningful scope for individual choices to surrender informational privacy. This, though, repeats the categorical error discussed in Part III by ignoring the institutional parameters of choice. Society has always defined the conditions of effective consent; that's what contract law is all about.[234] Without question, data privacy regulation would impose a collective decision that where personally-identified information is concerned, the definition of consent should be narrower. If informational privacy is a foundational requirement for individual self-determination and collective self-government, this sort of "coercion" is essential, and is no coercion at all.[235]

Finally, effective data privacy legislation also must incorporate other, non-consent-based requirements for fair information practice. The notion

---

230. *See* European Data Protection Directive, *supra* note 4, at arts. 6, 7.

231. 17 U.S.C. § 109(a) (1994). *But see* 17 U.S.C. § 1201 (1994 & Supp. 1998) (prohibiting tampering with technological measures designed to limit access to a copyrighted work).

232. *See* H.R. REP. NO. 94-1476, 124 (1976); Bobbs-Merrill Co. v. Straus, 210 U.S. 339 (1908); 2 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 8.12 (1999).

233. *See* text accompanying notes 188-206 *supra*.

234. *See* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 529-31 (1999).

235. *See* Allen, *supra* note 192, at 739-40.

that informed consent alone is sufficient to protect individual interests in the uses of personally-identified data is a peculiarly American one.[236] Internationally-agreed principles of fair information practice require a variety of other substantive and procedural protections. In particular, fair information practice requires attention to the transparency of data-processing practices, the security of collected data, access to one's own personally-identified data and the opportunity to correct inaccuracies, and the accountability of data processors.[237] These principles are designed to ensure that data processors are held accountable to individuals in fact as well as in theory, by affording individuals simple, effective procedures for holding data processors both to the terms to which they have agreed and to basic standards of fair play.

Accountability has collective as well as individual dimensions, moreover. As Part IV.B discussed, profiling practices implicate not only individualized notions of consent and fair process, but also collective values about the respect due individuals.[238] For this reason, the European Data Protection Directive grants each individual the right "not to be subject to a decision which produces legal effects concerning him *or significantly affects him* and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him."[239] Similarly, data privacy legislation should incorporate safeguards to ensure that data processors are held accountable to society for at least some types of choices. The exact form and content of these safeguards are subjects for collective discussion.

* * * *

Informational privacy is an essential building block for the kind of individuality, and the kind of society, that we say we value. Legislating for informational privacy, in turn, requires a different kind of attention to the categories that have dominated the discussion about data privacy protection. Effective data privacy protection must delineate the appropriate boundary between ownership and speech, specify the parameters for effective consent, and impose meaningful procedural and substantive protections on information practices.

The detailed implementation of provisions to ensure fair information practices is a subject for another article. It's worth noting, here, that although the basic outlines of data privacy protection can be legislated along the lines described here, the model I've proposed probably can't be sustained by legislation alone. Some fair information practices are likely to require

---

236. I am indebted to Joel Reidenberg for reminding me of this point.

237. *See* European Data Protection Directive, *supra* note 4, at Arts. 10-21; *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD Doc. C(80)58 (Final) (1980).

238. *See* text accompanying notes 126-133 *supra*.

239. European Data Protection Directive, *supra* note 4, at art. 15(1) (emphasis added).

ongoing regulatory oversight. Others are likely to require rulemaking at regular intervals; for example, it's hard to see how legislation alone could define categories of uses and recipients for disclosure purposes against a background of constantly changing commercial practice. These and other details of a comprehensive data privacy regime will demand careful consideration. This article has simply sought to clear away the theoretical obstacles to the discussion, so that the project of designing concrete legal protections for informational privacy can proceed.

## VII. CONCLUSION: INFORMATIONAL PRIVACY BY DESIGN

It is easy, and therefore tempting, to say that strong data privacy protection raises insurmountable jurisprudential dilemmas. But it is also wrong. Personally-identified data is neither unambiguously data processors' property nor simply their speech—it cannot, in any case, be first one and then the other, depending on which categorical argument works best—and the surrender of autonomy in exchange for the satisfaction of prefabricated preferences is not the only kind of choice. Invoking platonic ideals of ownership, speech, truth, and choice just avoids the hard policy questions, and inscribes in the guise of liberty a politics and practice of objectification. Wise information policy can, and should, do better.

There remains, however, one final objection: A charming academic hobby-horse, but what of it? It has become commonplace (and, oxymoronically, a sign of great sophistication) to assert that legal guarantees of privacy will be rendered empty by rapid technological change. On this view, strong data privacy protection is a sentimental pipe dream—as grandiose as Canute's, and with about as much chance of success.[240] It doesn't matter whether informational privacy is good or bad, principled or not. We have simply gone too far, too fast, to turn back.

I have tried to show, though, that the characterization of the data privacy problem as driven by technological tradeoffs grossly oversimplifies the choices that we face. The architectures of data collection are chosen. Thus far, privacy considerations have not been uppermost in the design process, but what is chosen can be changed.

In fact, technologists have made substantial headway toward the design of technical parameters for the exercise of autonomous, anonymous choice. Object-oriented programming techniques make it possible to endow individual items of data with broad ranges of attributes that specify the sorts of processing permitted. Personally-identified data can be encoded with de-

240. *See, e.g.*, DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998); Polly Sprenger, *Sun on Privacy: "Get Over It,"* WIRED NEWS, Jan. 26, 1999 <http://www.wired.com/news/politics/0,1283,17538,00.html> (quoting Scott McNealy, the CEO of Sun Microsystems).

tailed information about restrictions on use and exchange, or encased within digital firewalls that prevent its aggregate extraction in personally-identified form.[241] In addition, as Phil Agre describes, digital technologies enable the construction of "technologies of identity"—transactional systems that operate anonymously or pseudonymously, and so prevent personally-identified data from being collected at all.[242] The growing array of options for the design of transactional systems reminds us (again) that "progress" is not unidirectional. We can choose the system or systems that best comports with other social values and priorities.

It is also clear that, from a technological standpoint, strong data privacy protection need not preclude a serious commitment to solving the very real information problems that confront providers of goods and services in an information society. What is necessary is to look beyond purported efficiency tradeoffs, and envision other possibilities. We can design information systems that help vendors find and target customers. But we also can design information systems that decouple information from intrusion, by helping vendors learn about customer tastes and desires in aggregate. And we can design information systems that help customers find vendors—in other words, systems that reserve agency, and meaningful choice, to individuals.

Ultimately, we must use both technology and law to create and sustain the conditions for meaningful, autonomous choice.[243] At minimum, however, law can and should establish a new set of institutional parameters that supply incentives for the design of privacy-enhancing technologies to flourish. Legal protection alone cannot create or guarantee informational privacy. But it is a place to begin.

---

241. *See, e.g.*, Bellotti, *supra* note 128; Burkert, *supra* note 60; Tessa Lau, Oren Etzioni & Daniel S. Welch, *Privacy Interfaces for Information Management*, COMM. ACM, Oct. 1999, at 89.

242. *See, e.g.*, Agre, *supra* note 60; Burkert, *supra* note 60; Michael K. Reiter & Aviel D. Rubin, *Anonymous Web Transactions with Crowds*, COMM. ACM, Feb. 1999, at 32; David Goldschlag, Michael Reed & Paul Syverson, *Onion Routing for Anonymous and Private Internet Connections*, COMM. ACM, Feb. 1999, at 39; Eran Gabber, Phillip B. Gibbons, David M. Kristol, Yossi Matias & Alain Mayor, *Consistent, Yet Anonymous, Web Access with LPWA*, COMM. ACM, Feb. 1999, at 42 (1999); Robin Lloyd, *Total Digital Privacy May Be on the Horizon*, CNN INTERACTIVE, Aug. 18, 1999 <http://www.cnn.com/TECH/computing/1998/18/freedom/>. *See generally* Philip E. Agre, *The Architecture of Identity: Embedding Privacy in Market Institutions*, 2 INFO. COMM. & SOC'Y 1 (1999) (arguing that privacy practices and market institutions are mutually constituting).

243. Whether law should play a more direct role in fostering the design of privacy-enhancing technologies, and if so how, are questions beyond the scope of this article. For a discussion of such questions, see generally LESSIG, *supra* note 36 (discussing how technology, law, and policy shape each other); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998) (same).