

March 2019

A Prospect Theory of Privacy

Bryan H. Choi

Follow this and additional works at: <https://digitalcommons.law.uidaho.edu/idaho-law-review>

Recommended Citation

Bryan H. Choi, *A Prospect Theory of Privacy*, 51 IDAHO L. REV. 623 (2019).

Available at: <https://digitalcommons.law.uidaho.edu/idaho-law-review/vol51/iss3/2>

This Article is brought to you for free and open access by Digital Commons @ UIIdaho Law. It has been accepted for inclusion in Idaho Law Review by an authorized editor of Digital Commons @ UIIdaho Law. For more information, please contact annablaine@uidaho.edu.

A PROSPECT THEORY OF PRIVACY

BRYAN H. CHOI*

ABSTRACT

Privacy law has languished for decades while the other information law doctrines have flourished. This paradox can be explained by the relative weight assigned respectively to moral argument versus economic argument.

Privacy law is unique in that it continues to be steered foremost by moral intuition. What qualifies as a “violation” of privacy is predicated largely on the moral reprehensibility of the act in question. By stark contrast, the intellectual property regimes have long since converted to being led primarily by economic considerations, and only secondarily by non-economic factors.

That distinction is counterproductive and nonsensical. Personal data is an informational good like any other. The same economic justifications for intellectual “property” can be extended to intellectual “privacy”—nonexclusivity harms the incentives to generate new information that can further the progress of social knowledge.

Where moral rhetoric has failed to advance robust recognition of privacy interests, economic reasoning may prove more effective. In particular, this Essay offers Edmund Kitch’s prospect theory as an important counterweight to prior economic critiques of privacy, which have frowned on restraints on alienation of information. Prospect theory shows that the social value of recognizing exclusive claims is not just to shield information that already exists, but also to shield deeper investigations of that information to unearth further information that would not be otherwise discoverable.

TABLE OF CONTENTS

I. INTRODUCTION	624
II. PYRRHIC PURITY.....	627
III. PROMOTING THE PROGRESS OF PRIVACY	630
IV. PANNING THE PANNERS	634
A. Wrong Incentives?	634
B. Wrong Mechanism?	636
IV. CONCLUSION	638

* Visiting Associate Professor of Law, New York Law School. I thank Helen Nissenbaum, Kathy Strandburg, Ira Rubenstein, Solon Barocas, and all participants of the NYU Privacy Research Group for extraordinarily helpful comments. I am also grateful to New York Law School, as well as the Kauffman Foundation and Thomson Reuters for financial support. All opinions, errors, and omissions are my own.

I. INTRODUCTION

Data libertarianism is driving us toward data poverty, not data wealth. The rise of Big Data has spawned exuberant optimism that personal data is a bountiful harvest that will never run dry. Private companies, researchers, and governments alike are eager to capitalize on a gold rush of information that purports to solve all problems except the problem of privacy.¹ Data mining is the new alchemy, and the fount of personal data is seemingly infinite.²

The anticipated response has been that the crowd would embrace data transparency and spurn those who clung to anachronistic expectations of privacy.³ But it has not turned out that way. The crowd has become skeptical of social-media platforms designed to harvest data, and is looking increasingly for tools that destroy data before it can be plundered.⁴ Privacy is not dead.

The mood has changed. We are beginning to see personal data as a liability, not an asset.⁵ If we cannot control it, then no one else should have it. Why participate in social networks, why leave comments on websites, why take any risks

1. See, e.g., Jonathan Shaw, *Why "Big Data" Is a Big Deal*, HARV. MAG., Mar. 2014, at 30, 34; Don Peck, *They're Watching You at Work*, THE ATLANTIC, Dec. 2013.

2. Cf. Mark A. Lemley, *IP in a World Without Scarcity*, SOC. SCI. RES. NETWORK (Mar. 24, 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2413974 (arguing that we need a "post-scarcity economics" in a world where the cost of production and distribution of information is effectively zero).

3. Michael Zimmer, *Mark Zuckerberg's Theory of Privacy*, WASH. POST (Feb. 3, 2014), ("in a 2008 interview at the Web 2.0 Summit . . . Zuckerberg predicted that the amount of information people will share online will double each year . . ."); Polly Sprenger, *Sun on Privacy: 'Get Over It'*, WIRED (Jan. 26, 1999).

4. See, e.g., Michelle Cottle, *The Adultery Arms Race*, THE ATLANTIC, Nov. 2014 (describing apps like Snapchat and TigerText that cause messages to "self-destruct"); *Help Center*, KIK, <https://kikinteractive.zendesk.com/entries/95570573-My-messages-are-all-gone-what-happened-> (last visited Apr. 22, 2015) ("Your chat history is cleared when . . . [y]ou login to your account on a different device . . ."); Farid Fadaie, *Building an Engine for Decentralized Communications*, BITTORRENT BLOG (July 30, 2014), <http://blog.bittorrent.com/2014/07/30/building-an-engine-for-decentralized-communications/> ("BitTorrent does not track or store information on who is communicating with whom, or when communications happen. We are not even storing data temporarily on servers and then deleting it. We never have the metadata in the first place."); Christopher "moot" Poole, *The Case for Anonymity Online*, TED (filmed Feb. 2010), http://www.ted.com/talks/christopher_m00t_poole_the_case_for_anonymity_online?language=en ("[W]hat's unique about [4Chan] is that it's anonymous, and it has no memory. There's no archive, there are no barriers, there's no registration."); Ladar Levison, *Secrets, Lies and Snowden's Email: Why I Was Forced to Shut Down Lavabit*, THE GUARDIAN (May 20, 2014, 7:30 AM), <http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email>; Joseph Pomianowski & Jane Chong, *In Order to Protect Users from Intrusive Governments, Apple Has Prevented Itself from Unlocking iOS 8 Devices*, FORBES.COM (Oct. 16, 2014, 2:56 PM), <http://www.forbes.com/sites/realspin/2014/10/16/in-order-to-protect-users-from-repressive-governments-apple-has-prevented-itself-from-unlocking-ios-8-devices/> ("Enter Apple. Its decision to lock itself out of its own devices—and by extension, lock out law enforcement—is an improvement on the oldest vanishing act in the book: going offshore."). But see Andy Greenberg, *Whistleblowers Beware: Apps Like Whisper and Secret Will Rat You Out*, WIRED.COM (May 14, 2014, 3:45 PM), <http://www.wired.com/2014/05/whistleblowers-beware/>; Mike Isaac, *A Look Behind the Snapchat Photo Leak Claims*, N.Y. TIMES BITS (Oct. 17, 2014, 7:30 AM), <http://bits.blogs.nytimes.com/2014/10/17/a-look-behind-the-snapchat-photo-leak-claims/> (describing flaws in Snapchat's privacy features).

5. Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, PEW RESEARCH CENTER (Mar. 16, 2015), <http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/>; Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CENTER (Nov. 12, 2014) <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>.

online, if it can result in loss of employment, public shaming, and death threats?⁶ Those who are most aware of the risks have been minimizing their digital exposure, leaving behind those who are least aware. This is a poor outcome. We are forfeiting stockpiles of future data because of poor resource management. The data we do obtain will be grossly skewed.

Personal data is like any other resource: incentives need to be aligned to promote investment.⁷ While the Big Data industry has grown fat on a wave of initial naiveté, we are coming into leaner years as savvier digital natives take over.⁸ Even as data accumulation has become ever more effortless,⁹ the current generation of data innovation has turned toward the pursuit of forgetting and impermanence.¹⁰ Increasingly, resources are being poured into technologies of privacy and anonymity.¹¹ Companies are being pressed to guard, disregard, or discard user data—a sen-

6. See Choire Sicha, *Going Down in Infamy*, N.Y. TIMES, Apr. 19, 2015, at BR13 (reviewing JON RONSON, *SO YOU'VE BEEN PUBLICLY SHAMED* (2015)); DANIELLE CITRON, *HATE CRIMES IN CYBERSPACE* (2014).

7. Harold Demsetz, *Toward a Theory of Property Rights*, 57 AM. ECON. REV. 347, 354, 356 (Pap. & Proc. 1967) (“[P]roperty rights arise when it becomes economic for those affected by externalities to internalize benefits and costs. . . . This concentration of benefits and costs on owners creates incentives to utilize resources more efficiently.”); Edmund W. Kitch, *The Nature and Function of the Patent System*, 20 J.L. & ECON. 265, 275 (1977).

8. See DANAH BOYD, *IT'S COMPLICATED: THE SOCIAL LIVES OF NETWORKED TEENS* 56, 70 (2014) (“The teens that I met genuinely care about their privacy Many of the privacy strategies that teens implement are intended to counter the power dynamic that emerges when parents and other adults feel as though they have the right to watch and listen. They shift tools and encode content, use privacy settings, and demand privacy.”); JOHN PALFREY & URS GASSER, *BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES* 53 (2008); Kate Murphy, *We Want Privacy, but Can't Stop Sharing*, N.Y. TIMES, Oct. 5, 2014, at SR4 (“[P]rivacy researchers said they are starting to see signs of a backlash. People are beginning to exercise a bit more reserve online or are otherwise engaging in subversive tactics to thwart data miners.”).

9. See FRANK PASQUALE, *THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION* (2015); CHRISTOPHER SLOBOGIN, *PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT* (2007); DANIEL J. SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* (2006); SIMSON GARFINKEL, *DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY* (2000); BOYD, *supra* note 8, at 11 (2014) (“Content shared through social media often sticks around because technologies are designed to enable *persistence*.”).

10. VIKTOR MAYER-SCHÖNBERGER, *DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE* (2009); Jonathan Zittrain, *Reputation Bankruptcy*, CONCURRING OPINIONS (Sept. 7, 2010), <http://www.concurringopinions.com/archives/2010/09/reputation-bankruptcy.html>; Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES MAG., July 19, 2010, at MM30; Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, (May 13, 2014), <http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=EN&cid=144621> (declaring a “right to be forgotten”).

11. See, e.g., David Gelles, *Betting on Security Start-Ups in an Age of Data Breaches*, N.Y. TIMES BITS (Dec. 2, 2014 9:17 PM) (“Last year, there were 240 investments worth a combined \$1.7 billion in [security start-ups], up from 83 investments worth just \$340 million in 2009, according to CB Insights, a research firm that follows venture money.”); Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, WALL ST. J., Feb. 28, 2011; Stephan Dörner, *For German, Swiss Privacy Start-Ups, a Post-Snowden Boom*, WALL ST. J. DIGITS (Aug. 20, 2014, 5:15 AM EST), <http://blogs.wsj.com/digits/2014/08/20/for-german-swiss-privacy-start-ups-a-post-snowden-boon/>; Jonathan Mahler, *Who Spewed That Abuse? Anonymous Yik Yak Isn't Telling*, N.Y. TIMES, Mar. 9, 2015, at A1; William D. Cohan, *In Rise of Yik Yak App, Profits and Ethics Collide*, N.Y. TIMES DEALBOOK (Apr. 7, 2015), <http://www.nytimes.com/2015/04/08/business/dealbook/profits-and-ethics-collide-in-nameless-turmoil.html> (valuing Yik Yak at \$200-300 million); Jenna Wortham, *Secret Reaches Beyond Tech Set, and Raises \$25 Million*, N.Y. TIMES BITS (July 14, 2014 1:00 PM EST), <http://bits.blogs.nytimes.com/2014/07/14/secret-moves-to-broaden-appeal-beyond-the-tech-set-and-raises->

timent that only a few years ago would have been likened to lighting money on fire.¹²

This Essay argues that personal information is a resource that must be husbanded and cultivated, not slashed and burned. The classic conception of privacy pits the individual's moral right to conceal information against society's collective loss in blocking access to that information.¹³ Framed that way, privacy has been the consistent loser in the court of legislative opinion.¹⁴ In response, privacy advocates have increasingly reframed privacy as a collective good, not just an individual one. While that broadening of privacy's appeal is a critical shift, more is needed.

An equally powerful source of inertia has been not just the tension between individual versus collective, but the dominant sway of economic reasoning over moral rights in contemporary politics.¹⁵ Traditionally, economists have attacked privacy as a barrier to free information flow, because they have assumed the flawed, individualist conception of privacy.¹⁶ Rarely is privacy defended on efficiency grounds.¹⁷ The gap that needs to be filled is a theory that marshals economic arguments to champion the collective societal benefits of restricting free information flow.

Intellectual property law is fertile ground for such theories. In particular, Edmund Kitch's prospect theory¹⁸—an influential theory in patent law—offers a useful framework for translating the social benefits of privacy into economic terms. A

20-million/; Joshua Kopstein, *Not All Encryption Apps Are Created Equal*, ALJAZEERA AMERICA (Apr. 3, 2015 2:00 AM EST) <http://america.aljazeera.com/opinions/2015/4/not-all-encryption-apps-are-created-equal.html>; Elizabeth Dwoskin, *Whisper and the Meaning of Anonymity*, WALL ST. J. DIGITS (Oct. 28, 2014, 12:39 PM EST), <http://blogs.wsj.com/digits/2014/10/28/whisper-and-the-meaning-of-anonymity/>.

12. See Erin E. Harrison, *The Privacy Puzzle*, INSIDECOUNSEL (Dec. 22, 2014), <http://www.insidecounsel.com/2014/12/22/the-privacy-puzzle> (noting that the FTC's recommendations on effective data security practices include "minimize personal information about consumers" and "de-identify as much as possible").

13. See *infra* Part II.

14. See Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1907 (2013) ("The positive liberty paradigm, moreover, has made little headway within U.S. privacy policy, which is dominated instead by a commitment to notice and choice that derives from the negative liberty paradigm."); PRISCILLA REGAN, *LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY* 5–7 (1995) ("The number of laws does not reflect enormous policy success by privacy advocates. . . . [T]he actual number of laws passed pales in comparison to the amount of congressional activity devoted to the subject and the number of laws not passed . . .").

15. See, e.g., WILLIAM M. LANDES & RICHARD A. POSNER, *THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW* (2003); NIVA ELKIN-KOREN & ELI M. SALZBERGER, *THE LAW AND ECONOMICS OF INTELLECTUAL PROPERTY IN THE DIGITAL AGE* (2013); William W. Fisher, *Theories of Intellectual Property*, in *NEW ESSAYS IN THE LEGAL AND POLITICAL THEORY OF PROPERTY* (2001); Mark A. Lemley, *Faith-Based Intellectual Property*, 62 UCLA L. REV. __ (forthcoming 2015); Cass R. Sunstein, *The Stunning Triumph of Cost-Benefit Analysis*, BLOOMBERG VIEW (Sept. 12, 2012), <http://www.bloombergview.com/articles/2012-09-12/the-stunning-triumph-of-cost-benefit-analysis>.

16. See, e.g., Richard A. Posner, *Privacy, Secrecy, and Reputation*, 28 BUFF. L. REV. 1 (1979); cf. *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 2663 (2011) ("Vermont's law thus has the effect of preventing detailers—and only detailers—from communicating with physicians in an effective and informative manner.").

17. See generally Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381 (1996).

18. Not to be confused with prospect theory in behavioral economics as coined by Daniel Kahneman and Amos Tversky—though the Kahneman/Tversky theory offers useful insights for privacy law as well. Cf. Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1886–88 (2013).

prospect theory of privacy offers at least two insights that alter the economic analysis. The first is the opportunity cost of secrecy. The absence of legal protection does not diminish demand for privacy; it merely drives up the price. Accordingly, recognizing legal claims saves the considerable expense of investing in non-legal means of maintaining secrecy, which can then be used more productively elsewhere. The second is the opportunity cost of future information relative to present information. When the production of future information depends on privacy, a loss in privacy means a loss in future information. Prospect theory helps illuminate that the information we have in hand may not be fully vested, and that an early period of exclusivity can be useful in allowing further discoveries beneath the surface. Too often—in privacy discussions as well as in intellectual property discussions—cost-benefit analyses are heavily biased toward the losses associated with information that is already known, and have much greater difficulty assessing the benefits of future information that is as yet unknown.

II. PYRRHIC PURITY

Privacy differs from other areas of information law in that it has remained strongly wedded to moral intuition.¹⁹ That commitment has come at a cost: privacy protections remain essentially toothless.²⁰ By stark contrast, other areas of information law have been wildly successful during that same period of time. Patents, copyrights, trademarks, trade secrets, and even publicity rights have shifted uniformly away from moral grounds to economic reasoning, and each has become dramatically more robust as a consequence.²¹ Nevertheless, it remains highly unusual to defend privacy rights on anything but moral grounds.²² Privacy rights are

19. See, e.g., Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 969–70 (1989); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1148 (2000) (“A moral rights-like approach might be worth considering as to personal data.”).

20. See *supra* note 14; Vera Bergelson, *It’s Personal But Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 391–94 (2003) (describing existing federal and state regulations as “piecemeal” and “[a]dopted in response to specific violations and concerns relating to a particular industry” rather than being “based on any uniform theory of rights”).

21. See generally Robert P. Merges, *One Hundred Years of Solicitude: Intellectual Property Law 1900–2000*, 88 CAL. L. REV. 2187 (2000); see also Mark A. Lemley, *The Economics of Improvement in Intellectual Property Law*, 75 TEX. L. REV. 989, 1034–35 (1997) (“As the term ‘intellectual property’ settles over the traditional legal disciplines of patents, copyrights, and trademarks and encroaches as well into such neighboring bodies of law as trade secrets, the right of publicity, misappropriation, unfair competition, and idea submissions, courts and scholars increasingly turn to the legal and economic literature of tangible property law to justify—or to modify—the rules of intellectual property.”); Amy Kapczynski, *The Cost of Price: Why and How to Get Beyond Intellectual Property Internalism*, 59 UCLA L. REV. 970, 981 (2012) (“IP scholarship today responds primarily to the value of efficiency, and it generally conceives of IP as a means to generate incentives for the production of information. Although copyright, patent, trade secret, and trademark were not always thought of as conjoined areas of law, the rubric of information has been used to unite them by relying on a common analysis of the peculiar economic qualities of information.”); cf. Madhavi Sunder, *IP*, 59 STAN. L. REV. 257, 261 (2006) (critiquing the fact that “legal scholars continue to understand intellectual property as solely a tool to solve an economic ‘public goods’ problem”).

22. See, e.g., *Riley v. California*, 134 S. Ct. 2473, 2495–2496, 573 U.S. ___ (2014) (“Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans ‘the privacies of life.’ The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the

the opposite of publicity rights; no economic market should exist for information that wants to be private. And if such a market does exist, then the information being traded must not be very private after all. Perhaps there is a lesson to be learned.

The canonical literature frames privacy as an individual right to control private information (or correspondingly as a negative duty upon others not to access such information).²³ Typically, those views have relied on natural law conceptions to determine how far the right/duty should reach.²⁴ We like to imagine that personal information about us belongs to us, and that we alone should choose how it may be shared. We “deserve” such power because the information at issue is intimately tied to our personality. Who else could stake a stronger claim than that?²⁵ We are offended when a nosy neighbor asks about our business; outraged when a lover snoops on our devices; and creeped out when confronted by advertisements that track our internet history a little too closely.

The individualist model is deeply appealing on a gut level, yet its flaws are amply documented.²⁶ The modern consensus is that enforcing privacy solely on the basis of “what the individual wants” is woefully inadequate. When privacy is defined strictly in terms of individual choice, the issue is reduced to notice and consent.²⁷ Because individuals differ in their judgments, it is easy to become agnostic

Founders fought.”); *Lawrence v. Texas*, 539 U.S. 558, 572 (2003) (“These references show an emerging awareness that liberty gives substantial protection to adult persons in deciding how to conduct their private lives in matters pertaining to sex.”); *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 357 (1995) (“[A]nonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority.”); *Griswold v. Connecticut*, 381 U.S. 479, 486 (1965) (“We deal with a right of privacy older than the Bill of Rights—older than our political parties, older than our school system. Marriage is a coming together for better or for worse, hopefully enduring, and intimate to the degree of being sacred. It is an association that promotes a way of life, not causes; a harmony in living, not political faiths; a bilateral loyalty, not commercial or social projects. Yet it is an association for as noble a purpose as any involved in our prior decisions.”); *Boyd v. United States*, 116 U.S. 616, 631–32 (1886) (“And any compulsory discovery . . . is contrary to the principles of a free government. It is abhorrent to the instincts of an Englishman; it is abhorrent to the instincts of an American. It may suit the purposes of despotic power, but it cannot abide the pure atmosphere of political liberty and personal freedom.”).

23. See, e.g., Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); ALAN WESTIN, *PRIVACY AND FREEDOM* (1967); Charles Fried, *Privacy: A Moral Analysis*, 77 YALE L.J. 475 (1968); see also HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* 70–71 (2010) (“most of what is written about privacy assumes it to be a form of control” over information about oneself); DANIEL J. SOLOVE, *UNDERSTANDING PRIVACY* 24 (2008) (“One of the most predominant theories of privacy is that of control over personal information.”); Cohen, *supra* note 14, at 1907 (“Most privacy theorists have tended to think that the key to defining privacy lies in locating privacy’s essence in one or another overarching principle (such as liberty, inaccessibility, or control) . . .”).

24. See SOLOVE, *supra* note 23, at 12–13 (classifying six general conceptions of privacy: (1) the right to be let alone, (2) limited access to self, (3) secrecy, (4) control over personal information, (5) protection of one’s personhood, and (6) intimacy).

25. Cf. Thomas W. Merrill & Henry E. Smith, *The Morality of Property*, 48 WM. & MARY L. REV. 1849, 1858–59 (2007) (“Rules making nearness and physical control the criteria for possession have a psychological basis, and the convention of respecting possession stems from people’s mutual expectations that they will respect the right to control these things.”).

26. See generally REGAN, *supra* note 14; Anita L. Allen, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861 (2000).

27. Cf. Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879 (2013); Lorrie Faith Cranor, *Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. TELECOMM. & HIGH TECH. L. 273 (2012); see also Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370 (2014).

as to whether any given data should be shared or not. As long as the individual has “consented,” other concerns are swept off the table. Thus, much of the discussion turns on whether individuals are being given an opportunity to consent, and whether that consent is meaningful.²⁸ Yet even assuming consent is voluntarily obtained, the behavioral literature shows that individuals do not always act in their own best interest.²⁹ Moreover, many individuals are in an unfair bargaining position relative to those with more sophistication, money, or influence.³⁰ Critics have pointed out that consent-based models lead to disproportionate exploitation of vulnerable populations—the same reason for banning voluntary contracts for activities such as child labor, prostitution, organ sales, and other forms of bodily subjugation.³¹

At the same time, the individualist model is not just underprotective but also overbroad. It idealizes the amount of control any given individual can exercise before colliding into the overlapping claims of others. Individual rights never exist in a vacuum; they necessarily touch on the concerns of other individuals.³² A right to speak freely conflicts with a right to keep things unspoken, for example.³³ Communitarian critiques have pointed out that individual preferences must be balanced against countervailing societal needs.³⁴ Insisting dogmatically that privacy rights must be respected at all costs is tone deaf, because it is both impracticable and dystopian.

Frustrated with the shortcomings of the individualist construct of privacy, a wave of post-liberal scholarship has sought to expand the conception of privacy’s value beyond just the individual. The “self” is an artificial construct; we do not

28. See Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 821–28 (2000) (describing key failings of notice-and-consent schemes); M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2013); Helen Nissenbaum, *A Contextual Approach to Privacy Online*, DAEDALUS, Fall 2011, at 32 (“I am not convinced that notice-and-consent, however refined, will result in better privacy online as long as it remains a procedural mechanism divorced from the particularities of relevant online activity.”).

29. See Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, in DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES 363 (Alessandro Acquisti et al. eds., 2008); Kirsten Martin, *Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online*, __ J. PUB. POL’Y & MKTG. __ (forthcoming). See generally DANIEL KAHNEMAN, THINKING FAST AND SLOW (2011); RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008); DAN ARIELY, PREDICTABLY IRRATIONAL (2008).

30. See generally JOSEPH TUROW, THE DAILY YOU (2012); PASQUALE, *supra* note 9; Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy*, 126 HARV. L. REV. 2010 (2013); Mary Anne Franks, *Unwilling Avatars: Idealism and Discrimination in Cyberspace*, 20 COLUM. J. GENDER & L. 224 (2011).

31. Margaret Jane Radin & Madhavi Sunder, *The Subject and Object of Commodification*, in RETHINKING COMMERCIALIZATION: CASES AND READINGS IN LAW AND CULTURE (Martha M. Ertman & Joan C. Williams eds. 2005); Margaret Jane Radin, *Market-Inalienability*, 100 HARV. L. REV. 1849 (1987).

32. See generally Joseph William Singer, *The Legal Rights Debate in Analytical Jurisprudence from Bentham to Hohfeld*, 1982 WIS. L. REV. 975 (1982).

33. See, e.g., SOLOVE, *supra* note 23, at 87 (“[P]rivacy conflicts with other fundamental values, such as free speech, security, curiosity, and transparency . . .”); 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); Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967 (2003); *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653 (2011).

34. See Posner, *supra* note 16. Compare SOLOVE, *supra* note 23, at 90–91 (“The problem with communitarianism is that it pits the individual against the common good.”).

exist in isolation from the community around us.³⁵ Our identities are defined by our relationships with others, just as others are defined by us.³⁶ Accordingly, many leading privacy scholars have embraced instead a theory of “constitutive” privacy, in which privacy’s value is expressed not just in terms of any single individual, but as the mutual shaping performed by society and its constituent members.³⁷ Privacy is not in tension with societal goals; it *further*s mutual goals such as civility, democratic self-governance, and innovation.³⁸ Similarly, Helen Nissenbaum describes privacy as the ongoing pursuit of contextual equilibrium: as new technologies and new developments disrupt preexisting norms, we call on privacy to “preserve the integrity of the social contexts in which we live our lives.”³⁹

In short, privacy is much more than an individual right to secrecy or control; it is a collective engine that fosters, mediates, and integrates social progress. While current approaches have undoubtedly pushed privacy theory in the right direction, they have yet to find meaningful purchase among policymakers. Privacy’s positive effects do not erase its negative specter, and moral rhetoric alone does not inform lawmakers how to draw difficult lines. Legal protections for privacy remain anemic. Moral rhetoric may help each of us articulate what we think privacy is for, but it has been remarkably unsuccessful at enlisting legislative consensus.⁴⁰ In the absence of overt legal protections, the natural fallbacks are various forms of secrecy—technological defenses, enforced vows of silence, or self-censorship. Privacy should not be synonymous with secrecy, but it has become so.

III. PROMOTING THE PROGRESS OF PRIVACY

The relative paucity of economic literature on privacy is conspicuous. Much of what does exist grapples with the outdated individualist model of privacy. What is needed is an economic theory of privacy that incorporates the constitutive value of privacy beyond the individual cost-benefit. As a general rule, intellectual property theory is well-suited to that task. In particular, extending prospect theory from patent law to privacy law lends some useful insights.

35. See Cohen, *supra* note 14, at 1906 (“The self who benefits from privacy is not the autonomous, precultural island that the liberal individualist model presumes.”); SOLOVE, *supra* note 23, at 91 (“We do not live in isolation, but among others, and social engagement is a necessary part of life.”). See generally Bryan H. Choi, *For Whom the Data Tolls: A Reunited Theory of Fourth and Fifth Amendment Jurisprudence*, 37 CARDOZO L. REV. __ (forthcoming 2015).

36. Cohen, *supra* note 14, at 1910–11.

37. SOLOVE, *supra* note 23, at 91–93; Schwartz, *supra* note 28, at 834–35; JULIE COHEN, *CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE* (2012).

38. See, e.g., Cohen, *supra* note 14, at 1927 (“[P]rivacy does not only protect individuals. Privacy furthers fundamental public policy goals relating to liberal democratic citizenship, innovation, and human flourishing, and those purposes must be taken into account when making privacy policy.”); Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1613 (1999); Post, *supra* note 19, at 959.

39. NISSENBAUM, *supra* note 23, at 161–66, 186; see also Andrew Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643, 650–54 (2013).

40. Cf. Murphy, *supra* note 17, at 2389–90 (“Warren and Brandeis’s success in finding a natural right to privacy (or personality) separable from property rights was the cause of the [privacy] tort’s eventual failure. . . . Courts proved comfortable with rights characterized as property, but blanched at amorphous and ‘inalienable’ rights such as the right to control one’s personality.”).

In 1977, Edmund Kitch published a seminal paper offering an economic justification for allowing early patent claiming before the value of the information is fully realized.⁴¹ Kitch's key insight was that certain kinds of worthy investments in information cannot be achieved through secrecy alone.⁴² Secrecy is always an available option, of course. But a legal system that depends only on secrecy is less efficient at generating socially productive information than a system that supplements secrecy with early exclusivity.

Kitch contrasted two possible functions of a patent claim system.⁴³ Previous scholars had touted the reward function, i.e., that an inventor should be rewarded for the successful achievement of a worthy invention, so that he may capture his returns on investment.⁴⁴ In essence, the reward function is a backward-looking theory that seeks to protect the vested value of a completed invention. Kitch observed, however, that the reward theory failed to explain certain aspects of the patent system as it was actually practiced.⁴⁵

Instead, Kitch proposed an alternate, forward-looking theory: a prospect function that allows early claiming in order to draw future investment toward an area of interest.⁴⁶ The purpose of the patent system was not just to reimburse value achieved *before* the patent grant but also to push claimants to extract new value *after* the patent grant.⁴⁷ In particular, Kitch drew upon an analogy to mining claims in the American West during the late 1800s.⁴⁸ Because oil could not be easily detected from the surface, large investments in drilling needed to be made before any exclusive rights could be claimed.⁴⁹ To encourage such investments, miners were permitted to obtain mining claims prior to showing that the land had any commercial significance. Doing so afforded miners greater certainty over their ownership

41. Edmund W. Kitch, *The Nature and Function of the Patent System*, 20 J.L. & ECON. 265 (1977). *But see* John F. Duffy, *Rethinking the Prospect Theory of Patents*, 71 U. CHI. L. REV. 439, 441-43 (2004) (discussing several critiques that "have dogged the prospect theory," and concluding that "although the 'prospect features' of patent law . . . do serve a socially useful function, this function is not one identified by Kitch").

42. *Id.* at 275 ("The proposition advanced here is that a legal system which has trade secrecy and a patent system will better serve the public welfare than a legal system with only trade secrecy.").

43. *See id.*

44. *Id.* at 266.

45. *Id.* at 266-67 (arguing that "the reward theory offers an incomplete view of the functions of the patent system" and that "the prospect function is a significant, if not the predomina[nt], function of the American patent system as it has operated in fact").

46. *Id.* at 266.

47. *See* Mark A. Lemley, *Ex Ante versus Ex Post Justifications for Intellectual Property*, 71 U. CHI. L. REV. 129, 132 (2004) (describing Kitch's prospect theory as an "ex post" theory that "encourage[es] efficient use of existing works rather than the creation of new works") [hereinafter Lemley, *Ex Ante versus Ex Post*]; A. Samuel Oddi, *Un-Unified Economic Theories of Patents—The Not-Quite-Holy Grail*, 71 NOTRE DAME L. REV. 267, 281 (1995) (referring to prospect theory as a "post-classical theory"); J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data?*, 50 VAND. L. REV. 51, 163 (1997) ("The more that subpatentable innovation falls through the cracks of the classical intellectual property system, which rests on the mature patent and copyright paradigms, the more governments multiply hybrid *sui generis* regimes of exclusive property rights. The real purpose of these regimes is to protect investors against the risk of market failure that results from a chronic shortage of natural lead time.").

48. Kitch, *supra* note 41, at 271-75.

49. *Id.* at 273.

rights in the face of uncertain economic valuations.⁵⁰ Unpromising claims could be abandoned and returned to the public domain.⁵¹

Kitch listed several reasons a patent “prospect” is more advantageous than secrecy. Relevant to the present discussion were: first, that a patent system reduces the costs of maintaining secrecy; second, that a patent system encourages development of ideas that cannot be easily kept secret; and third, that legal recognition of claims facilitates sharing of information and reduces duplication of effort.⁵² Those who obtain a patent claim are spared the expense of having to guard their secrets with lockboxes and nondisclosure agreements.⁵³ That capital could be redirected elsewhere. More importantly, by reducing dependence on secrecy as the sole protective measure, a prospect system fosters sustained investment in projects even when they are impossible to keep secret until completion. A research effort that otherwise might be abandoned for futility becomes feasible again. That protection also encourages voluntary exchange of information and reduces wasteful duplication of efforts to generate knowledge that others have previously extracted. The purpose of furnishing legal protection was not to enhance secrecy, but to obviate it.

Those considerations are recognized even under trade secret doctrine, where courts have relaxed the requirement of absolute secrecy so long as reasonable efforts are made to guard the information.⁵⁴ The general consensus has been that requiring perfect secrecy is untenable because it encourages tactics that are costly and unreasonable to defend against.⁵⁵ To hold otherwise would force companies to assume unreasonable risks, to the point where many would refuse to enter entire lines of business because it has ceased to be economically rational to do so. When the expense of guarding information exceeds any potential revenue, no rational actor would invest in developing such information.

Those lessons are readily extended from trade secret and patent law to privacy law.⁵⁶ Secrecy has long been the main mechanism of privacy protection. As long as one holds one’s cards close to one’s chest, no one else is the wiser. But today’s data mining, behavioral tracking, and surveillance technologies have made secrecy more difficult and costly to maintain.

50. *Id.* at 274–75.

51. *Id.* at 274.

52. *Id.* at 279.

53. See Posner, *supra* note 16, at 9–10 (“[E]ven where secrecy would afford some protection . . . it might be an extremely costly method of protection . . .”).

54. See Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L. REV. 1, 42–43 (2007) (“Without a rule protecting trade secret holders even when their precautions against improper acquisition or accidental loss are only ‘reasonable,’ the amount spent by owners and takers would escalate without any corresponding social benefit. This is why absolute secrecy is not required . . .”); Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets As IP Rights*, 61 STAN. L. REV. 311, 348–50 (2008) (“The benefit of trade secret law is that it reduces investment in secrecy compared to what would happen absent that law. So there is no reason we should want to establish a minimum investment level as an end in itself.”); see also Sharon K. Sandeen, *Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection*, 19 VA. J.L. & TECH. 1 (2014).

55. See, e.g., *E.I. duPont deNemours & Co. v. Christopher*, 431 F.2d 1012, 1016 (5th Cir. 1970) (“To require DuPont to put a roof over the unfinished plant to guard its secret would impose an enormous expense to prevent nothing more than a school boy’s trick.”).

56. Cf. Samuelson, *supra* note 19, at 1152 (analogizing information privacy law to trade secrecy law).

Raising the cost of data secrecy leads to two outcomes—both suboptimal. The first is an arms race: as surveillance technologies encroach on private interests, those who wish to resist can choose to expend increasing amounts of labor and capital to counter those effects. In the physical context, inventive minds have devised entire cottage industries of masks, walls, locks, and alarms. In the virtual context, the equivalents have been proxies, firewalls, encryptions, and alerts. Those with technical skill and financial resources have doubled down.⁵⁷ As more attention and effort is poured into the collection and analysis of data, the software community has responded in kind with countermeasures that are increasingly sophisticated and expensive. On the one hand, the technologies of obfuscation are better than they have ever been. On the other hand, those efforts and resources could be spared and redirected elsewhere.

The second outcome is surrender: those without technical or financial means will accept that they are unable to protect their private information, and they will stop resisting. A world without privacy leads to blandification of the mainstream and marginalization of the alternatives.⁵⁸ It reinforces conformity and chills ideas that deviate from the norm.⁵⁹ There is little incentive to develop one's own personality—unless one is already outcast. The result is an overall loss in individual agency, diversity of ideas, and progress of knowledge.

Legal recognition of privacy “prospects” could help stabilize those problems by offering a supplemental form of information protection, just as the patent system complements the trade secrecy regime. One should not have to prove secrecy—or even reasonable efforts at secrecy—in order to stake a privacy claim. Nor should one have to prove personal, subjective desire for privacy in the claimed information. Instead, such value should be presumptive unless the claim is “abandoned” due to factors such as waiver, commercial use, death, or sufficient expiry of time.

To be sure, such protection would shrink the public domain by some quantifiable measure. Private information would no longer become subject to public use simply by virtue of having been leaked. Then again, *all* informational rights shrink the public domain, and that short-term loss is compensated by a longer-term societal gain.⁶⁰ A traditional reward theory analysis undervalues that quid pro quo, by accounting for only the known universe of information. By contrast, a prospect

57. A noteworthy example of using resources to purchase privacy was the personal e-mail server maintained by Hillary Clinton during her tenure as Secretary of State. See Michael S. Schmidt, *No Emails from Clinton's Time at State Dept. Are on Her Server, Lawyer Says*, N.Y. TIMES, Mar. 28, 2015, at A14.

58. See generally DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011); Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 12–15 (2008); Posner, *supra* note 16, at 30 (“Rational behavior respecting privacy is also suggested by the way in which people will substitute reticence for physical privacy when the latter is in short supply . . .”).

59. See Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 483 (2015); Sarah K. Cowan, *Secrets and Misperceptions: The Creation of Self-Fulfilling Illusions*, 1 SOC. SCI. 466, 468 (2014); First Amended Complaint, *First Unitarian Church of L. A. v. NSA*, No. 3:13-cv-03287 (N.D. Cal. Sept. 10, 2013).

60. See Jessica Litman, *The Public Domain*, 39 EMORY L.J. 965 (1990); Lemley, *supra* note 21, at 993–99; William M. Landes & Richard A. Posner, *An Economic Analysis of Copyright Law*, 18 J. LEGAL STUD. 325, 326, 343 (1989); see also R. Polk Wagner, *Information Wants to be Free: Intellectual Property and the Mythologies of Control*, 103 COLUM. L. REV. 995 (2003).

theory analysis is more complete because it accounts for the potential of exclusivity to spawn future information that otherwise would go undiscovered. A person who suffers a bout of depression or illness,⁶¹ or engages in sexually transgressive acts, or reads a subversive pamphlet,⁶² or breaks with the accepted norm in any manner has generated some private data. But the societal value of that data is not necessarily ripest at the instant moment it comes into being. Allowing some period of maturation can pay future dividends that are more meaningful than a superficial mosaic cobbled together from haphazard parts.⁶³

IV. PANNING THE PANNERS

In extending a utilitarian approach to privacy theory, several objections can be anticipated. One set of questions is whether an incentives-based model is appropriate for personal data: many forms of personal data are created automatically without any incentive at all, and those that do depend on incentive may be socially undesirable. Another longstanding debate concerns whether propertization is a prudent model to extend to personal data, especially in light of the problems that have developed in intellectual property law. A final reservation raised is whether championing a utilitarian approach is incompatible with the moral rights traditions. This Part takes each of those objections in turn.

A. Wrong Incentives?

As a threshold matter, one might ask whether personal data differs from patentable inventions and copyrightable works, in that the former is generated as a natural byproduct of living—our facial features, our DNA and fingerprints, our blood, our biometric data—whereas the latter are not. No amount of incentive can alter the presence or absence of data “constants” that either exist or not. Courts have repeatedly relied on this type of reasoning to hold that such fixed information is a “foregone conclusion” and thus cannot be shielded as private.⁶⁴

A first-order response is to point out that other kinds of personal data do respond to incentives—our actions, our habits, our preferences, our thoughts. Moreover, even if biometric data is fixed, the collection and use of biometric data has second-order effects that influence our behavior. The fallacy here is to view data as inert in relation to the past without considering its potential to have future effects. Prospect theory helps correct for hindsight bias by championing a forward-looking perspective on information production.

The main line of attack, however, has come from older economic treatments of privacy, which have been highly skeptical of privacy as an inefficient restraint

61. Frank Pasquale & Tara Adams Ragone, *Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing*, 17 STAN. TECH. L. REV. 595, 630 (2014).

62. Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at “Copyright Management” in Cyberspace*, 28 CONN. L. REV. 981, 1008 (1996).

63. See Murphy, *supra* note 17, at 2387 (“When disclosure will diminish the quantity or quality of information generated, prohibiting disclosure may have a positive net effect.”).

64. *Hiibel v. Sixth Jud. Dist. Ct. of Nev., Humboldt Cnty.*, 542 U.S. 177, 191 (2004) (names); *Maryland v. King*, 133 S. Ct. 1958, 1962 (2013) (DNA samples); *Schmerber v. California*, 384 U.S. 757, 772 (1966) (blood samples); see also *Fisher v. United States*, 425 U.S. 391, 411 (1976).

against free information flow.⁶⁵ Not all private information is the *kind* of information we want to promote as a society.⁶⁶ Information is often concealed in furtherance of criminal acts, or because of shame and other reputational fears. Richard Posner has argued that a person should not be entitled to conceal discreditable facts (such as a criminal past or a history of bankruptcies) that lower the person's valuation to others.⁶⁷ Justice Scalia has complained that anonymity "facilitates wrong by eliminating accountability, which is ordinarily the very purpose of the anonymity."⁶⁸ We give exclusive rights to inventors and authors because we believe their ideas are socially useful; perhaps that reasoning does not extend to information that is actively harmful to others.⁶⁹ Perhaps it is wiser to discourage socially disruptive ideas. For example, if a lawyer knows a client has murderous intent, or a doctor knows an airline pilot is suffering depression, why should such information be protected a la works of fine art?

The difficulty lies in measurement of value. Most economic analyses weigh only the cost of disclosure upon the individual (an abstract dignitary harm) against the cost of nondisclosure upon society (a concrete, measurable harm such as number of lives lost).⁷⁰ Those analyses commit the same errors that early privacy theorists made of characterizing privacy as a zero-sum game. A more nuanced analysis is needed.

Again, prospect theory offers a helpful lens by bridging constitutive theory and economic theory. Shielding private information—even "disreputable" information—is the equivalent of investing in an idea that has zero or negative value at present, but which may yield net positive value in the future. Premature disclosure is undesirable because it cuts short productive explorations before they can prove their worth. On the other hand, when the net present value is clearly negative—as in the example of the murderous client—prospect theory would support immediate forfeiture of the privacy claim. Conversely, when the net present value is overwhelmingly positive, as in the case of newsworthy items or other matters of great public interest, then the privacy interest in nurturing future dividends must yield to the present need.

Furthermore, typical economic analysis does not account for the macro costs associated with *not* protecting privacy. If we can assume demand for privacy is highly inelastic, then consumers are willing to pay substantial amounts to obtain privacy. As Kitch noted, "it is difficult to imagine any system—absent the most

65. See, e.g., Posner, *supra* note 16; George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUDIES 623 (1980); Hal R. Varian, *Economic Aspects of Personal Privacy*, in PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (1996); PAUL H. RUBIN & THOMAS M. LENARD, PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION (2002); see also Alessandro Acquisti et al., The Economics of Privacy, <http://ssrn.com/abstract=2580411> (describing three waves of research in the economics of privacy).

66. See Murphy, *supra* note 17, at 2384–85 ("Thus, many claims for privacy are really claims to protect a *reputation*. When the only interest is in reputation, it is usually inefficient to limit disclosure of *true* information.").

67. See Posner, *supra* note 16, at 11–14.

68. *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 385 (1995) (Scalia, J., dissenting).

69. Cf. Tun-Jen Chiang, *Competing Visions of Patentable Subject Matter*, 82 GEO. WASH. L. REV. 1858, 1888 (2014); Eldar Haber, *Copyrighted Crimes: The Copyrightability of Illegal Works*, 16 YALE J. L. & TECH. 454 (2014).

70. See *supra* note 16.

draconian and costly measures—that would reduce the phenomenon of secrecy to an insignificant level.”⁷¹ The more sensitive the information, the more people will pay to guard it. The greater the consequences of inadvertent disclosure, the more people will pay to limit their exposure to risk. And on the other side, those interested in thwarting those defenses must increase their spending as well. Total economic waste in expenditures can quickly spiral out of proportion.⁷² An economic analysis of privacy requires appraising not only the social cost of protecting data, but also the social cost of withholding legal protection. In the end, legal recognition of privacy claims may prove the more prudent fiscal choice.

B. Wrong Mechanism?

Setting aside whether the production of private information is worth incentivizing, a separate challenge is whether propertization is the appropriate mechanism for doing so. The dominant objection against propertization of privacy has been that it would promote too much sharing of information.⁷³ As Jessica Litman has written, “We deem something property in order to facilitate its transfer. If we don’t intend the item to be transferred, then we needn’t treat it as property at all.”⁷⁴ By assigning information a property value, it becomes a commodity for sale—and once it can be sold, it will be sold.⁷⁵ Thus, privacy absolutists argue that private information should never be commodified in the first place.⁷⁶ The point of protecting private information is that it is private; allowing it to be freely traded seems contrary to the spirit.

On a pragmatic level, that ship has sailed. Data is already commodified; robust markets exist for the purchase and exchange of personal data.⁷⁷ It is unrealistic

71. Kitch, *supra* note 41, at 275.

72. See Liana B. Baker et al., *Exclusive: Cyber IPO Pipeline Grows as Data Breaches Boost Security Spending*, REUTERS, Mar. 20, 2015 (“With global spending on IT security set to increase 8.2 percent in 2015 to \$77 billion, according to market research firm Gartner, the shares of publicly traded cybersecurity firms have done well.”); Ponemon Institute, 2015 Cost of Data Breach Study, *available at* <http://www-03.ibm.com/security/data-breach/> (last visited June 16, 2015) (finding the average consolidated total cost of a data breach to be \$3.8 million).

73. Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1295–96 (2000); Samuelson, *supra* note 14, at 1138 (“Consider also that the most common justification for granting property rights—to enable market allocations of scarce resources—does not seem to apply to personal data. What is scarce is information privacy, not personal data. If anything, personal data are being too plentifully distributed in the marketplace right now.”); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1533–35 (2000); *cf.* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1378–84 (2000) (“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.”).

74. Litman, *supra* note 73, at 1296.

75. See Samuelson, *supra* note 19; *see also* Acquisiti & Grossklags, *supra* note 29; *see generally* Christine Jolls, *Rationality and Consent in Privacy Law* (Yale Law School, Working Paper Dec. 10, 2010), *available at* http://www.law.yale.edu/documents/pdf/Faculty/Jolls_RationalityandConsentinPrivacyLaw.pdf.

76. See Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2057 n.4, 2090–94 (2004) (collecting critical commentary of legal scholars who have “advocated imposing a ban on data trade”).

77. See PASQUALE, *supra* note 9; Natasha Singer, *You for Sale*, N.Y. TIMES, June 17, 2012, at BU1.

to imagine returning to a bygone era in which personal data is inalienable. If data can be traded freely by third parties, it seems perverse to disallow trading by first persons. Any such disparity rests on the false conception of privacy-as-secrecy. Information that is *actually* kept secret does not require legal protection; privacy is concerned with an independent subset of data that is only *reasonably* kept secret.

That said, to the extent there are special concerns regarding the initial transfer of information, those concerns could be mitigated by limiting the privacy claim to exclude any information sold or bartered for value (such as for discount coupons or free content). Propertization would extend only up to the point of sale, at which point it would expire. In this way, the privacy claim could accommodate both the ideal of discouraging alienation by first persons and the reality of commodification by third parties.

Interestingly, in intellectual property scholarship, the most pointed attacks have been that property rights *block* too much sharing of information.⁷⁸ Once a property claim is assigned, it divides the world into those who are valid claimants and those who are not. The claimants receive a right to exclude others from using the claimed information.⁷⁹ Accordingly, many prominent patent and copyright scholars have worried that too much information has come under exclusive proprietorship.⁸⁰ They have pointed to problems of thickets and cross-licensing, as well as uncertainties surrounding fair use, which diminish opportunities for communal re-use and remixing of information.⁸¹

The challenges of negotiating overlapping privacy claims are undeniable. Anyone who wishes to pass along gossip, publish a memoir, conduct research using personal data, manage user-generated content, or share any information at all would have to sort through conflicting privacy claims. Therefore one might well ask: Why extend the woes of intellectual property law to privacy law? Yet this would be a strange critique for privacy advocates to raise, because it would mean their efforts have been *too* successful—hardly the challenge today.

Nevertheless, a distinction could be drawn between commercial and non-commercial uses, as it has been to a limited extent in intellectual property law.⁸² Noncommercial uses cover most of the ordinary interactions we have historically carried on. And although noncommercial disclosures can be devastating on an indi-

78. See Lemley, *Ex Ante versus Ex Post*, *supra* note 47, at 142–43 (“The idea that granting exclusive rights over information will reduce the use and distribution of that information compared with an open market makes perfect sense. It is consistent with everything we know about basic economics.”).

79. Demsetz, *supra* note 7, at 354 (“Private ownership implies that the community recognizes the right of the owner to exclude others from exercising the owner’s private rights.”); Thomas W. Merrill, Property and the Right to Exclude, 77 NEB. L. REV. 730 (1998); Henry E. Smith, Property and Property Rules, 79 N.Y.U. L. REV. 1719 (2004).

80. See generally LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY (2004); Litman, *supra* note 74, at 1294–95.

81. See Mark A. Lemley & Carl Shapiro, *Patent Holdup and Royalty Stacking*, 85 TEX. L. REV. 1991, 2010–15 (2007); Jacqueline Lipton, *Information Property: Rights and Responsibilities*, 56 FLA. L. REV. 135 (2004).

82. See Jessica Litman, *Lawful Personal Use*, 85 TEX. L. REV. 1871, 1874 (2007); see generally Ronald D. Hantman, *Experimental Use as an Exception to Patent Infringement*, 67 J. PAT. & TRADEMARK OFF. SOC’Y 617 (1985); *Madey v. Duke University*, 307 F.3d 1351, 1362 (Fed. Cir. 2002) (discussing experimental use defense to patent infringement).

vidual level, the commercial profit motive is more systematically problematic because it drives up repetition and scale.

More generally, however, these conflict considerations are precisely the questions that must be confronted under any data privacy regime. There is no easy avoidance. The best we can do is to set good defaults that minimize the need to overturn initial allocations of rights. If intellectual property serves as a historical lesson, a robust privacy right would most likely reduce nonconsensual disclosures, while encouraging more voluntary disclosures. This is the outcome privacy law should want.

C. Wrong Justification?

But the most formidable objection to overcome may be that cost-benefit analysis is insensitive or repugnant to the moral attributes of privacy. Many in the privacy community are deeply skeptical of reducing privacy to numerical terms, because they worry it flattens and distorts the robust nature of privacy. Some things cannot be quantified, and those ineffable qualities cannot be factored into any cost-benefit equation.

This is a fair criticism. The best—and perhaps only—response is to point out that cost-benefit analysis can be in alliance with other moral approaches. They need not be in tension. The purpose of this Essay has been to point out that moral indignity has been remarkably ineffective at promoting actual privacy protections, and that economic reasoning may be better equipped to achieve the *same*, desired results. While there may be differences further down the road, why not hitch the wagons together as far as they will go?

IV. CONCLUSION

Private information is valuable precisely because it is information the public cannot produce. Stories of shame, of stigma, of failure—these are stories that are tremendously helpful when shared with others who are undergoing the same trauma. Under premature scrutiny, these stories wither and cannot be cultivated or later shared. Without privacy, knowledge is lost. We are afraid to admit our own internal struggles; we marginalize those who can offer insight; and we are slow to learn from the mistakes of others. Whether it is treatment options for stigmatized illnesses, existential doubts, advice for difficult relationships, or coping mechanisms for bereavement, we fall into familiar patterns instead of standing on the shoulders of confidants.

How can we transcend those samsaric cycles of human ignorance? The same way we have achieved all other kinds of progress: by compiling libraries of information. Big Data is not the enemy. It is a tool; a technology. But all technologies must be used with care. The world's most advanced tractor is of little use in a field of weeds. Privacy is a mechanism for allowing some fields to lie fallow, for a limited time, so that they can turn more fruitful in future years. As we evolve from data gatherers into data farmers, we must become more mindful of data sustainability.