ARTICLES

PRIVACY, THE HACKER WAY

ANDREA M. MATWYSHYN*

ABSTRACT

This Article seeks to clarify the relationship between contract law and promises of privacy and information security. It challenges three commonly held misconceptions in privacy literature regarding the relationship between contract and data protection—the propertization fatalism, the economic value fatalism, and the displacement fatalism—and argues in favor of embracing contract law as a way to enhance consumer privacy. Using analysis from Sorrell v. IMS Health Inc., *marketing theory, and the work of Pierre Bourdieu, it argues that the value in information contracts is inherently relational: consumers provide "things of value"—rights of access to valuable informational constructs of identity and context—in exchange for access to certain services provided by the data aggregator. This Article presents a contract-based consumer protection approach to privacy and information security. Modeled on trade secret law and landlord-tenant law, it advocates for courts and legislatures to adopt a "reasonable data stewardship" approach that relies on a set of implied promises—nonwaivable contract warranties and remedies—to maintain contextual integrity of information and improve consumer privacy.*

* Assistant Professor of Legal Studies and Business Ethics, The Wharton School, University of Pennsylvania; Affiliate, Center for Technology, Innovation, and Competition, University of Pennsylvania Law School; Affiliate Scholar, Center for Internet and Society, Stanford Law School. The author wishes to thank Gaia Bernstein, Ian Brown, Jum Carroll, Christina DeVries, Lilian Edwards, Gerald Faulhaber, Victor Fleischer, Craig Green, Andres Guadamuz, Stephen Hetcher, Jennifer E. Hill, Christopher Hoofnagle, Mathias Klang, Jacqui Lipton, Christopher Marsden, Brian Martin, Miranda Mowbray, Andrea Monroe, Deirdre Mulligan, Helen Nissenbaum, Paul Ohm, Deborah Pierce, Jon Pincus, Martin Redish, Elizabeth Rowe, Marcia Tiersky, Kevin Werbach, and Christopher Yoo for their insightful commentary and criticism. She also thanks the faculties of Notre Dame Law School and the Oxford Internet Institute, where she was a visitor during the writing of this Article. She can be reached at amatwysh@wharton.upenn.edu.

I. INTRODUCTION

The capacity of technology to find and publish personal information . . . presents serious and unresolved issues with respect to personal privacy . . . .

—Sorrell v. IMS Health Inc.[1]

In a tongue-in-cheek depiction of technology contracting, an episode of the iconic cartoon series *South Park* ridiculed the idea that consumers meaningfully consent to terms of use agreements and privacy policies.[2] One of the main characters, Kyle, is tracked through his gadgets by corporate "Business Casual G-Men," who seek to enforce several obligations to which he has ostensibly agreed under digital contracts—obligations which include being chained to a hospital bed and being used as a participant in machine-human convergence experimentation.[3] When Kyle's father asks the Business Casual G-Men where his son is being taken and what will happen to him, they reply that they cannot tell him because his son consented to the company's contracts and that the company's "inner workings are top secret to all users."[4] Kyle's father next suggests getting the police involved, to which Kyle's friends retort that there is no point in doing so because police rely on the company's tracking data to find people.[5] Finally, Kyle's father wins his son's freedom by sacrificing the privacy of his own information and agreeing to be digitally tracked.[6]

Though clearly exaggerated for comic effect, the plot of this *South Park* episode correctly captures the feelings of many users: they have lost control of their privacy. Like Kyle and his father, average consumers cannot successfully anticipate the privacy consequences of their contracts when they click "I Agree," and they are sometimes shocked by the resulting corporate conduct. According to at least one study, if Internet users read each of the privacy policies they encountered, they would each spend twenty-five days reading privacy policies every year, amounting to a nationalized number of 53.8 *billion* hours spent reading (unnegotiable) privacy policies.[7] As the *South Park* episode also demonstrates, contract

1. Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2672 (2011).

2. *South Park: Humancentipad* (Comedy Central television broadcast Apr. 27, 2011), *available at* http://www.southparkstudios.com/full-episodes/s15e01-humancentipad.

3. *Id.*

4. *Id.*

5. *Id.*

6. *Id.*

7. Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, ATLANTIC (Mar. 1, 2012), http://www.theatlantic.com/technology/archive/2012/03/

law is usually viewed as an obstacle to protecting privacy and is rarely viewed as part of the solution. Many consumers—despite acknowledging their consent to a user agreement—are deeply confused about what data is being collected about them, how it is used, and what recourse is available to them for commercial harms. Consumers frequently presume that a legal regime of consumer protection already governs all of their data exchanges.[8] However, such a legal regime currently does not exist in most cases.[9]

As technology services progressively move toward the "cloud" in both government and private sectors,[10] questions of consumer privacy become even more pressing. Yet, legal uncertainty pervades the developing field of consumer privacy law. As Congress considers new legislation in this area and the Supreme Court begins to turn its attention to consumer privacy in cases such as *Sorrell v. IMS Health Inc.*,[11] numerous open questions of law require resolution. One of the most important queries asks whether consumers possess any legally protectable interest in their data after it has been collected by a company. In other words, when social networking websites, search engines, online newspapers, pharmacies, mobile phone providers, or even grocery stores track information about consumers' communications or buying habits, do consumers have any legal basis to require that the companies handle their information with care? Do consumers possess any legally cognizable interest with respect to their information after sharing it pursuant to a contract? This Article asserts that consumers do indeed hold such a legal interest and that, in direct contradiction to the dominant view held in the privacy scholarship, contract law plays a key role in the future of consumer privacy.

First, in Part II, I debunk the idea that contract law is solely a problem for privacy and not a possible solution. In so doing, I address three

reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

8. *See, e.g.*, Kevin Sack, *Patient Data Posted Online in Major Breach of Privacy*, N.Y. TIMES, Sept. 9, 2011, at A1, *available at* http://www.nytimes.com/2011/09/09/us/09breach.html (noting one mother's frustration after a privacy breach on a hospital's website exposed her son's medical records online).

9. I am referring to affirmative data care rather than breach notification. The exceptions to this statement include data covered by the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 26, 29, and 42 U.S.C.), the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of 12 and 15 U.S.C.), and the Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2012).

10. The cloud is an ambiguous construct and generally means remote Internet data storage and services. *See* Kevin Werbach, *The Network Utility*, 60 DUKE L.J. 1761, 1811–14, 1821 (2011) (describing various cloud applications and detailing the general rise of cloud computing).

11. Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011).

common misconceptions, or "fatalisms," regarding the role of contract law in consumer privacy: the propertization fatalism, the value fatalism and the displacement fatalism. Using the language of the Supreme Court in *Sorrell*, I argue that data privacy should be analyzed in the context of an exchange of two services that are each a "thing of value": access to identity information in exchange for access to information services. Second, in Part III, I explain why contract law offers a viable vehicle for implementing a consumer protection regime in data privacy, and I present an approach derived from trade secret law. Finally, in Part IV, I introduce a "reasonable data stewardship" model of consumer privacy and information security, which aims to create a contract-based consumer protection regime for data sharing and information security through implied promises.

II. HACKING CONTRACT AND THE THREE FATALISMS

On February 1, 2012, Facebook filed an S-1, announcing its initial public offering ("IPO").[12] In its offering documentation, the company explained that its value was derived primarily from delivering collected consumer information to advertisers—an enterprise resulting in an IPO valued at $5 billion.[13] In particular, Mark Zuckerberg, Facebook's founder and CEO, included a noteworthy letter in the S-1 which described the company's corporate philosophy, called "The Hacker Way."[14] Zuckerberg explained "The Hacker Way" in the following manner:

> We have cultivated a unique culture and management approach that we call the Hacker Way.
>
> The word "hacker" has an unfairly negative connotation from being portrayed in the media as people who break into computers. In reality, hacking just means building something quickly or testing the boundaries of what can be done. Like most things, it can be used for good or bad . . . .
>
> . . . .
>
> Facebook exists to make the world more open and connected . . . .[15]

12. Facebook, Inc., Registration Statement (Form S-1) (Feb. 1, 2012), *available at* http://www.sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954ds1.htm.

13. *Id.* at 3.

14. *Id.* at 67–70.

15. *Id.* at 69–70. Zuckerberg's definition might be taking liberties with the traditional definition of hacking which is more in line with the notion of building something in a clever way that was not originally intended. *See, e.g.*, *FAQs*, CURIOSITY HACKED (Jan. 20, 2013), http://www.hacker-scouts.org/node/40 ("Unfortunately, there are some who associate [hacking] with illegal activity. Hacking is simply taking something—like an object or idea—and changing it to fit one's own need. Hacking is the improvement and modification of technology. Hacking is how we progress.").

Contract law, like novel data-intensive business models, can and should adopt a traditional "hacker" mentality in order to address emerging issues of consumer privacy. Scholars and lawyers must test the boundaries of what can be accomplished with contract law before declaring it an impotent method of privacy protection and, perhaps, recombine it in an unanticipated but useful way. Legal scholarship has not yet done so. To meet that need, in the following sections, I push the boundaries of contract law to their limits in addressing the increasingly important issue of consumer privacy.

Although contract law has played a critical role in the information privacy debate, privacy law scholars have generally discounted it as a viable route toward strengthening consumer privacy. This discounting is premature. As I have argued in other work,[16] contract law is the lynchpin bridging consumer privacy promises in privacy policies with information security promises that arise partially out of terms and conditions of use. These two promises are core to any interpretation of consumers' privacy rights.[17] Yet, many legal scholars believe that contract law should be circumvented in order to improve data privacy and information security for consumers. I argue to the contrary[18]: contract law should instead be *embraced* as a means of protecting consumer privacy more aggressively.

In particular, three "fatalisms" exist in privacy scholarship about the role of contract law in improving consumer privacy: the propertization fatalism, the value fatalism, and the displacement fatalism. As the following sections explain, none of these fatalisms actually cripples the potential of contract law to improve protection of consumer privacy.

A. THE PROPERTIZATION FATALISM

[P]ersonal information, thought of as the right of decision over one's private personality, should be defined as a property right . . . .

16. *See* Andrea M. Matwyshyn, *Mutually Assured Protection: Toward Development of Relational Internet Data Security and Privacy Contracting Norms*, *in* SECURING PRIVACY IN THE INTERNET AGE 73, 79–84 (Anupam Chander et al. eds., 2008) ("[T]erms of use and privacy policies significantly increased as data security contracting constructions online.").

17. *See id.* at 83–84 (evaluating Internet privacy in light of privacy policies and terms of conditions and use). As such, the totality of privacy and information security promises should be analyzed together as a single contractual construct: both privacy policies and terms of use together constitute bundles of promises made by a services provider to a consumer; they are executed simultaneously and frequently incorporate each other by reference. For an example of such an incorporation, see *Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/legal/terms (last updated Nov. 15, 2013) (explaining Facebook's privacy policies and informing users of their "commitments" when using the site).

18. *See infra* Part II.B.

—Alan Westin[19]

Do consumers possess any legal interest in their data? If so, does the interest change once the data has been embedded in a commercial database? As ample legal literature explains, an active debate exists on this point. This debate has traditionally turned on whether a property right of some sort, particularly an intellectual property right, can (or should) be constructed in consumer information. On one hand, one group of scholars argues in favor of creating property rights in consumer information.[20] For example, Henry Smith has argued that "exclusive rights in information are simple, indirect, and low-cost devices for solving the problem of appropriating the returns from . . . rival inputs."[21] On the other hand, companies that aggregate, use, and license consumer information onward would argue that although their corporate databases of aggregated information are protected by copyright, trade secret, and contract; individual consumers retain no legal interest in their information after it is collected.

The propertization fatalism, in turn, refers to the view held by many legal scholars that contract law approaches to consumer privacy require

19. ALAN F. WESTIN, PRIVACY AND FREEDOM 324 (1970).

20. Another group of scholars advocates a hybrid regime, blending elements of both a property and a human rights approach. Paul Schwartz, for example, argues that "while free alienability arguments are insufficient to justify unregulated trade in personal information, concerns about market failure and the public's interest in a protected 'privacy commons' are equally insufficient to justify a ban on the trade." Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2056 (2004).

21. Henry E. Smith, *Intellectual Property as Property: Delineating Entitlements in Information*, 116 YALE L.J. 1742, 1742 (2007). This approach contrasts with a second group of scholars who assert that a property rights approach is misguided and only a human rights focused approach correctly conceptualizes the consumer interest in aggregated data. Jessica Litman articulates this view in saying that a "property rights model would be ineffective in protecting data privacy." Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1295 (2000) (discussing the disadvantages of a privacy-as-property solution). *See also* Anupam Chander, *The New, New Property*, 81 TEX. L. REV. 715, 778–79 (2003) (discussing the limitations of a property model to intellectual property by distinguishing between the property concept itself and the abuse of that concept in the context of website domain names); Richard A. Epstein, *The Dubious Constitutionality of the Copyright Term Extension Act*, 36 LOY. L.A. L. REV. 123, 126 (2002) (noting the problems with merely characterizing copyright as property); Richard A. Epstein, *Intellectual Property: Old Boundaries and New Frontiers*, 76 IND. L.J. 803, 804 (2001) (noting the difficulty in analogizing real property law to intellectual property law); Jacqueline Lipton, *Information Property: Rights and Responsibilities*, 56 FLA. L. REV. 135, 140 (2004) (arguing that traditional property theories can help achieve appropriate checks and balances in the context of intellectual property); Jacqueline Lipton, *Mixed Metaphors in Cyberspace: Property in Information and Information Systems*, 35 LOY. U. CHI. L.J. 235, 239 (2003) ("I share the concerns of the commentators who have criticized the disturbing trend by governments to 'over-propertize' information in the digital age.").

first determining an alienable property right in consumer information.[22] In other words, this equation assumes that absent a finding of property rights in consumer information, contract law is an impotent route toward crafting consumer privacy law because allegedly nothing of economic value changes hands. But herein lies a misconception: finding property rights in consumer information is actually neither necessary nor sufficient in order to implement a contract law regime.[23] For the sake of argument, let us assume the weakest possible property position for the pro-privacy argument: that no underlying intellectual property or property interest exists for consumers in their data.[24] Even assuming that the individual pieces of consumer information likely have no protectable property interest, contract law can still offer a basis for consumer privacy protection. No propertization is required.

As the following sections illustrate, the propertization fatalism is subject to two major flaws. The first concerns a misunderstanding of consideration in contract: the propertization fatalism confuses the doctrine of contractual adequacy—whether the parties received a good deal—with contractual *sufficiency*—whether the parties exchanged things of value.[25] Second, the propertization fatalism erroneously treats information as a good, rather than construing access to information as a service.

1. Information Sharing as Consideration: A "Thing of Value"

A common refrain in the privacy debate asserts that when consumers sign up for a "free" service, such as a Facebook account, they get what they

22. In the words of Dan Solove,

> Theorists who view privacy as control over information frequently understand it within the framework of property and contract concepts. This is not the only way control can be understood, but the leading commentators often define it in terms of ownership—as a property right in information. Understood in such terms, control over something entails a bundle of legal rights of ownership, such as rights of possession, alienability, exclusion of others, commercial exploitation, and so on.

DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 76–77 (2004) (footnote omitted).

23. By way of explanation, let us take an example from another context: I offer to teach you a magic trick in exchange for your cleaning my neighbor's house. I hold no property rights in the magic trick, nor do I have property rights in my neighbor's house. Yet, if I teach you the magic trick, I have an enforceable contract against you. You are bound to perform the service or I have a right to pursue contract remedies available to me in law or in equity.

24. Let us also assume for purposes of this argument that a protectable compilation interest may exist for the data aggregator.

25. 3 SAMUEL WILLISTON, A TREATISE ON THE LAW OF CONTRACTS § 7:21 (Richard A. Lord ed., 4th ed. 2013). While courts analyze contractual sufficiency, adequacy is generally not analyzed in contract inquiries—it is a matter of private ordering left to the parties. *Id.*

pay for in terms of privacy—nothing.[26] In other words, this argument alleges that consumers can demand nothing in terms of privacy and security from companies because the companies essentially gift their services to consumers: the consumer conveys no "thing of value" to the company. This argument is inaccurate. In granting a license to access their data, consumers do indeed convey a "thing of value."[27] In other words, the act of sharing data is a form of legally sufficient consideration,[28] which therefore entitles consumers to demand enforcement of the promises that induced their data sharing in the first place. When consumers grant a company access to their personal data, they do so in exchange for—and are induced by—implicit and explicit promises of services and reasonable data stewardship. Access to one information stream created by consumers is exchanged for another information stream created by the company, both on limited terms of access.

The counterargument to this approach asks the following: "How can you assert that my generating a clickstream of data about video clips of piano-playing cats and my favorite beers constitutes something valuable? It's drivel, not consideration. In order for a contract to exist and be enforceable by both sides, consideration must be present." However, we

26. *See, e.g.*, Scott Goodson, *If You're Not Paying for It, You Become the Product*, FORBES (Mar. 5, 2012), http://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/ ("[T]he only real way to avoid Google tracking us is to stop using their services altogether. After all, the services are free so surely we should understand they come at a price?").

27. I have extensively examined elsewhere questions of acceptance and meaningful consumer consent. *See generally* Andrea M. Matwyshyn, *Technoconsen(t)sus*, 85 WASH. U. L. REV. 529 (2007) (analyzing limitations on meaningful consumer consent in consumer digital contracting).

28. When a consumer voluntarily reveals information to a data aggregator, the consumer grants the aggregator a nonexclusive license to access identity information. The consumer, in fact, clearly holds the appropriate rights in this "thing of value." There is no one with superior rights in knowing the consumer's favorite type of beer ahead of the consumer. Without the consumer's agreement and voluntary conduct, no data sharing can happen: only the consumer knows the brand of his or her favorite beer and can selectively embed that information into the possession of the aggregator. As a theoretical matter, therefore, a consumer information transfer is perhaps most appropriately viewed as a transfer similar to selling corporate "goodwill" or a relational opportunity through contract. What is transferred or created is the opportunity to better know consumers in order to do business with them, just as a goodwill transfer agreement in a corporate context would create an opportunity or access right to do business with a particular group of customers. The consumer provides access to this opportunity, but the consumer's relationship to information remains unsevered. Opportunities are regularly bought and sold through contract and have negotiated value—option rights, rights to stories or interviews, retainer agreements, settlement agreements, releases, noncompetition agreements, and nondisclosure agreements can each be conceptualized as contracts about opportunities. The relevant legal question is, therefore, what the terms are of this license. Are the dispositive terms the unnegotiated (and unnegotiable) terms stipulated by the data aggregator, or are the dispositive terms a set of terms that balance the consumer's selective embedding interest in the information with the aggregator's license interest?

will recall that contract law does not require us to provide objectively valuable items in order for an enforceable bargain to exist: contract law looks only for legal *sufficiency*, not adequacy, of consideration. Legal sufficiency inquiries for purposes of contract law merely look to whether the parties *subjectively value* the transferred things;[29] courts generally prefer not to second-guess the negotiated bargain and the adequacy of consideration, and do so only in the rarest of circumstances.[30] Thus, provided that the consideration is legally sufficient, courts will not economically re-evaluate the idiosyncratic terms of a deal with respect to consideration.[31] Specifically, in order for consideration to be legally sufficient, two "things of value" must be exchanged, and reciprocally conventionally induced[32] in a bargained-for exchange. Both of these elements are present when consumers grant access to their information.[33]

29. 3 WILLISTON, *supra* note 25, § 7:21. Adequacy of consideration refers to whether the parties received a "good deal" in the bargain. Legal sufficiency refers to whether a thing of value is exchanged to induce a promise from the other party. *Id.* § 7:3.

30. Even in such circumstances, the inquiry is framed more in terms of economic duress and unconscionability. *See, e.g.*, Williams v. Walker-Thomas Furniture Co., 350 F.2d 445, 449–50 (D.C. Cir. 1965) (discussing the unconscionability of a contract's terms and inequality of bargaining power rather than sufficiency of consideration when determining the enforceability of the contract).

31. Hence, courts conduct primarily only a minimal objective inquiry into consideration, giving deference to the parties' subjective assessment of value: Did the parties in fact exchange a thing of value, as defined by their *subjective* evaluation, and did the detriment (or benefit) on one side induce the performance of the other side? Provided there was no fraud or material misrepresentation in the exchange, courts essentially ask three questions: (1) Was a "thing of value" actually transferred in a bargained-for exchange? (2) Did the transfer reciprocally conventionally induce the promises in the agreement? (3) Did the transfer cause a detriment to the promisee or, in some jurisdictions, confer a benefit upon the promisor? Legal sufficiency does not require a good or fair transaction from the standpoint of value, but it requires an actual exchange. 3 WILLISTON, *supra* note 25, § 7:3.

32. *Id.* Reciprocal conventional inducement refers to the construct of the promise and performance of one party triggering the consideration from the other side of the transaction and vice versa. The promises and performance of each side triggers the promises and performance of the other side that are contingent upon each other in the bargained-for exchange, in a reciprocally conventionally induced manner. For example, you could pay me $50 to refrain from drinking coffee for one day. This forbearance would constitute a great detriment to me on most days, but perhaps not to someone who primarily drinks tea. Yet, I possess no underlying legal "right" in drinking coffee each day and may choose to refrain in some cases even without compensation. Regardless, this agreement between you and me that I refrain from coffee consumption is a properly formed and binding agreement on me, reciprocally conventionally induced.

33. A "thing of value" is anything that holds value in the eyes of one or all of the parties to the agreement, even if said "thing" holds value to no one else in the world. The transfer of the "thing of value" should trigger the promises of the other contracting party, who, in turn, begins performance of the negotiated obligations in the contract. Courts look not solely for a transfer of money or goods. A performance, a forbearance, or the creation, modification, or relinquishment of a legal right, each constitute a form of sufficient consideration when part of a bargained-for exchange. Each of them can constitute a sufficient detriment to one party or confer a sufficient benefit on the other party. One of the traditional contract law examples is the transfer of a peppercorn. A mere peppercorn, if conferred solely to provide an appearance of conveying a thing of value, constitutes insufficient consideration. If,

The transfer triggers and supports the exchange,[34] providing a basis for suit in case of a breach.[35]

The lack of a property right in a "thing of value" has never been an obstacle for contract. In fact, as a practical matter in many cases, even when it is clear that no underlying property right exists, contracts related to the subject matter are, nevertheless, prevalent and enforced. For example, though no copyright exists in a life story,[36] book authors and movie producers frequently secure rights in life stories from individuals, to prevent the disclosure of details to others for commercial purposes.[37] Similarly, although I have no protectable interest per se in my ability to purchase three cups of coffee today, you can pay me to refrain from doing so in an enforceable agreement. Or, perhaps most aptly for our discussion, attorneys possess no rights to the contract law knowledge in their heads, yet people pay them handsomely for access to it.

For an example of this dynamic from an information-aggregation context, let us momentarily turn to *Feist Publications, Inc. v. Rural Telephone Service Co*.[38]—the seminal case on copyrightability of databases.[39] In *Feist*, one white pages producer, Feist, tried to license consumer information from another white pages producer, Rural.[40] When

however, the peppercorn happens to be a very special, highly coveted peppercorn that holds intrinsic value for both the parties, its transfer is in fact a transfer of a "thing of value." *See* Chappell & Co. v. Nestlé Co., [1960] A.C. 87 (H.L.) at 114–15 (discussing the ability of a peppercorn to be adequate consideration).

34. As with all things of value, the appropriate inquiry from the standpoint of contract law goes purely to legal sufficiency for consideration purposes and whether sufficient rights exist—however they may be constructed—to enter into the contract. Other traditional contract formation and enforcement issues exist as well.

35. But how can the knowledge of my favorite beer, for example, offer any value? Are we sure that a detriment exists to me or a benefit exists to the data aggregator in access to seemingly frivolous information? As Part III explains, even seemingly mundane information such as my favorite type of beer has value precisely because it is not alienable: it remains embedded in a consumer and the consumer's network of friends potentially in perpetuity. Particularly when we consider certain types of mundane information—such as my favorite brand of beer—perhaps we may also decide that some types of information are "low value" goods and simply not important enough to warrant any kind of legal protection? Part III argues the answer is no—all information carries value because it gives access to the identity of the person to whom it pertains.

36. 1 JOHN W. HAZARD, JR., COPYRIGHT LAW IN BUSINESS AND PRACTICE § 7:24 (rev. ed. 2011).

37. Laura A. Heymann, *How to Write a Life: Some Thoughts on Fixation and the Copyright/Privacy Divide*, 51 WM. & MARY L. REV. 825, 829, 832, 863–69 (2009).

38. Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340 (1991).

39. For a discussion of *Feist*'s importance to the jurisprudence on the copyrightability of databases, see generally Jane C. Ginsburg, *No "Sweat"? Copyright and Other Protection of Works of Information After* Feist v. Rural Telephone, 92 COLUM. L. REV. 338 (1992).

40. *Feist Publ'ns*, 499 U.S. at 342–43.

Rural refused, the parties ended up in copyright litigation in which the Supreme Court ultimately held that Rural lacked any protectable interest in its database.[41] However, it is important to note that Feist's *first* course of action pursued was not to copy Rural's information but rather to attempt licensing the data through a contract.[42] Had Rural simply licensed the data to Feist, there likely would have been no suit. In that case, an enforceable contract would have been created, both parties would have generated a new revenue stream, and the time, expense, and bad precedent (from Rural's perspective) would have been avoided. Thus, even *Feist*'s facts remind us that holders of information do not need to understand the exact nature of their intellectual property right in information in order to be able to contractually leverage or restrict it.

Therefore, as long as contracts provide the primary source of ordering in data-privacy and information security contexts, the need to name and dissect the exact nature of legal interest consumers hold in their own information is functionally nonessential to the protection of that information. Regardless of how one categorizes the legal possessory interest of consumers in their own information, the information at issue is both embedded in consumers and within their sole control to selectively embed elsewhere.[43] Ergo, from a contract law viewpoint, the appropriate label for consumers granting access to their information is indeed a "thing of value," specifically an exchange of services for other services. Consequently, as the next section argues, the proper contract paradigm to apply is not a data-as-alienable-good paradigm but rather a data-services paradigm. According to a data-access conceptualization, access to knowledge of my favorite type of beer is less like buying a physical pint of beer, and more like buying the right to ask me questions about the beer knowledge I have accumulated in my head.

2. *Sorrell v. IMS Health Inc.*: Information as a "Service"

As the previous sections have explained, contract law approaches to consumer privacy have widely presumed that a property right needs to be created in consumer information in order to protect it through contract.[44] In other words, scholars advocating for that approach would argue that consumers "own" their information and can effectively alienate it. As such,

41. *Id.* at 342–43, 364.

42. *Id.* at 343.

43. As such, true alienation is functionally impossible, but simultaneously, the consumer clearly has the capacity, both contractually and practically, to grant a license to the information.

44. *See supra* text accompanying note 22. *See also* SOLOVE, *supra* note 22, at 76–90 (discussing the property-based approach to privacy).

information is treated as an alienable good, akin to a pint of beer, a car, or a book.[45] If information is thus constructed as a sold good, then perhaps an information aggregator's intellectual property rights in a database of consumer information,[46] if any exist, should simply supersede any information privacy interest consumers have in their information. This data-as-alienable good approach has dominated the conversation about contract-based approaches to consumer privacy.[47] Even scholars who do not advocate a property right sometimes verge on equating contract approaches with property rights and treating information as a type of good.[48]

Therein lies the misconception. Consumer data is clearly not a good and the data-as-alienable paradigm is therefore a total logical mismatch: my name or my beer preferences are no more alienable than the knowledge of law in my head. They are each part of me. For illustration of this point, let us imagine that I am collecting information on beer preferences for a study on marketing practices. You agree to tell me the name of your favorite beer in exchange for my tutoring you in contract law. Specifically, you share with me that Samuel Smith Oatmeal Stout is your favorite beer. Have you "alienated" the information? No. You still know it is your favorite beer. Nor do I "alienate" my knowledge of contract law when I tutor you—it remains in my head.[49] In both cases, a service was simply

45. SOLOVE, *supra* note 22, at 77.

46. The aggregator's rights, apart from being unsettled, also fall within a broader debate over the nature of intellectual property itself and whether real property paradigms are appropriate to its regulation. *See, e.g.*, Anupam Chander & Madhavi Sunder, *The Romance of the Public Domain*, 92 CALIF. L. REV. 1331, 1354–55 (2004) (arguing that treating intellectual property as a form of property will increase the focus on the distributional effects of that property); Shubha Ghosh, *Deprivatizing Copyright*, 54 CASE W. RES. L. REV. 387, 389 (2003) (exploring the debate over "whether copyright law serves to protect certain essential private property interests, or whether copyright law is informed by public, regulatory values").

47. SOLOVE, *supra* note 22, at 76–77.

48. As Solove describes, "Giving people property rights or default contract rules is not sufficient to remedy the problem because it does not address the underlying power inequalities that govern information transactions." *Id*. at 85. Indeed, he later explains,

> It is not merely sufficient to allow people to sell their information, relinquish all title to it, and allow companies to use it as they see fit. . . . Nor is it enough to attach some default contractual rights to information transactions . . . . These solutions cannot work effectively in a situation where the power relationship between individuals and public and private bureaucracies is so greatly unbalanced.

Id. at 90. Elsewhere, however, Solove strikes a hopeful chord, saying that "contract law can protect privacy within relationships formed between parties." *Id.* at 81.

49. I could agree to never again use my name, drink my favorite coffee, or indulge in my favorite beer; however, this "alienation" would be completely illogical when considering the goals of a data aggregator. The whole point of the aggregation turns on my retaining these characteristics of myself—their continued embedding in me. *See infra* Part III.

exchanged for another service. We granted each other access to information. Whether it is the name of my favorite beer or my knowledge of contract law, I am being given something in return for providing the *service* of making certain information available and vice versa. As relevant in this Article, when we contract to share our data with an aggregator, we are engaging in the same sort of transaction as above: we are extending a contract right of access to our knowledge.[50]

Contract law is therefore not only about goods; it is equally about contracts for services, even if those services reflect no underlying property interests. In fact, returning to the Facebook S-1, we see Facebook speaking of user data sharing in similar terms: as an inherently relational construct in which data streams are exchanged for other data streams, services for services.[51] The quantifications of value Facebook presented in its S-1 are not about individual units of data: they are about *relationships* with individual users as the holders of data and access to their networks of friends.[52] Facebook then leverages these consumer relationships by crafting additional relationships with advertisers.[53] In other words, for Facebook, information streams are relational services.

This conceptualization of access to data as a service is also consistent with the First Amendment approach adopted by the Supreme Court in *Sorrell v. IMS Health Inc*.[54] In *Sorrell*, the Court struck down a Vermont pharmaceutical data privacy statute because it restricted access to information on a discriminatory basis that considered the identity of the party seeking the information and the content of its speech:

> On its face, Vermont's law enacts content- and speaker-based restrictions on the sale, disclosure, and use of prescriber-identifying information. . . . The measure then bars any disclosure when recipient speakers will use the information for marketing. . . . The statute thus

50. As any lawyer who relies on Westlaw or Lexis for research will attest, even in situations where the data at issue contains public records, access can be restricted with contracts and revenue can be generated for rights of access. *See Westlaw Next Plans*, THOMSON REUTERS, http://legalsolutions.thomsonreuters.com/law-products/westlawnext (last visited Sept. 28, 2013) (describing the various plans consumers can purchase to access documents on WestlawNext, including public records); *LexisNexis Store*, LEXISNEXIS, http://www.lexisnexis.com/store/us/?&WT.ad=Ver2_Store-JCM155387-Store-080112-Print-PT (last visited Sept. 28, 2013) (providing various links to pages through which users can purchase access to legal documents).

51. *See* Facebook, Inc., *supra* note 12, at 2–4 (describing the interaction among users, developers, marketers, and advertisers on Facebook).

52. *See id.* at 42 (explaining how advertising makes up almost all of Facebook's revenue and how Facebook "offer[s] advertisers a unique combination of reach, relevance, social context, and engagement to enhance the value of their ads").

53. *Id.*

54. Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011).

> disfavors marketing, that is, speech with a particular content. More than that, the statute disfavors specific speakers, namely pharmaceutical manufacturers.[55]

Stated another way, the statute was struck down because it gave access to information to some speakers but restricted access to others. In describing the transfers of data at issue, the Court explained that

> [p]harmaceutical manufacturers promote their drugs to doctors through a process called "detailing[,]" . . . [through which] [d]etailers bring drug samples as well as medical studies that explain the "details" and potential advantages of various prescription drugs. . . . Salespersons can be more effective when they know the background and purchasing preferences of their clientele, and pharmaceutical salespersons are no exception. Knowledge of a physician's prescription practices—called "prescriber-identifying information"—enables a detailer better to ascertain which doctors are likely to be interested in a particular drug and how best to present a particular sales message.[56]

Thus, the Supreme Court provides a description of an inherently relational process in which value is created by applying data to a particular social context. Although accessing data is the first step in providing this service, the data does not generate value simply by sitting in a database. Indeed, its value is instead derived when the data is embedded into a particular relational context, much like doctors' relationships with their patients and with pharmaceutical providers.

Perhaps some scholars would say that this analysis is untenable. Even if we assume that access to a data stream triggers the corresponding access rights granted by the other party, it is not clear that consumers' data stream about their favorite types of beer, ice cream, movies, and radio stations holds any real economic value to consumers. Consideration must reflect some value—a benefit to the recipient or, in some jurisdictions, a detriment to the transferring party. As the next section explains, this argument is inapposite. In particular, because courts do not examine the adequacy of consideration,[57] value in access to data can be created not merely in terms of its economic capital but also in terms of its social and cultural capital.

B. THE ECONOMIC VALUE FATALISM

The second commonly believed fatalism about contract-based privacy approaches relates to the economic valuation of information. This

55. *Id.* at 2663.
56. *Id.* at 2659–60.
57. 3 WILLISTON, *supra* note 25, § 7:21.

"economic value fatalism" argues that enforceable privacy obligations cannot exist between consumers and a data aggregator through contract because some consumer information is so seemingly frivolous—my favorite beer or ice cream flavor—that it is essentially worthless. Further, it asserts that mundane or ordinary consumer information has no independent value, and value does not arise until the information is embedded in a database. Therefore, because worthless data could never serve as consideration, consumers are unable to strike a meaningful deal. As such, contract offers no viable way to include terms to protect consumer privacy. This analysis is incorrect, however. As this section explains through the theory of Pierre Bourdieu, economic valuation is only one of three forms of value creation. A "thing of value" may provide value through access to economic, social, or cultural capital. Indeed, all three forms of value creation can be the subject of contract. To wit, I argue that value creation for contract purposes can arise from relational social context: the economic, social, or cultural value rests in finding a connection between a piece of information and a particular human and his social milieu, not the embedding of information in a database.

Further, some privacy scholars adopt a modified version of the economic value fatalism and argue that while some types of information are "sensitive" and high value to consumers—social security numbers, health history, and so forth—many other types of information, such as my favorite beer or flavor of ice cream, are of little value.[58] But, as the following discussion of marketing theory demonstrates, this thinking is also unduly negative. In fact, it may be the case that my favorite beer is actually my *most* valuable piece of information simply because it is shared with the fewest people. Value in information is driven by scarcity, not sensitivity.[59]

1. Bourdieu and the Value of Access

The prior sections explained that in the context of contract law, access to consumer information is a "thing of value" and is therefore sufficient consideration for contract purposes. This section unpacks this idea of "value." At the heart of the economic value fatalism are the incorrect

58. *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1848–52 (2011) (discussing the "surprising irrelevance" of many types of personally identifiable information gathered for marketing purposes).

59. For a discussion of information scarcity driving value, see 2 LOUIS ALTMAN & MALLA POLLACK, CALLMANN ON UNFAIR COMPETITION, TRADEMARKS AND MONOPOLIES § 14:26 (4th ed. 2009 & Supp. 2013) (defining a trade secret as "information which derives economic value from not being generally known and not being readily ascertainable by proper means").

assumptions that value creation is solely an economic process and that economic capital is the only kind of asset. In reality, value and capital arise in three different ways.

In *The Forms of Capital*, Bourdieu identifies three types of capital: economic, social, and cultural.[60] Economic capital refers to financial resources.[61] Social capital refers to "the aggregate of the actual or potential resources which are linked to possession of a durable network of more or less institutionalized relationships of mutual acquaintance and recognition."[62] For example, because I have friends who are doctors, when I have a medical question, they graciously answer it for me as a favor. Consequently, I have access to information that a person without my network of friends may not obtain as easily or reliably. Finally, cultural capital refers to forms of knowledge that are valued in society as indicators of skills, education, and advantages that a person possesses, which give that person a higher status in society.[63] Recognizing cultural capital means being able to read a "tell" about a person's wealth, status, upbringing, education, or social milieu. This knowledge allows you to connect with this person, passing as a member of the same "in" group through shared knowledge. For example, in some circles, it is socially valuable to be able to identify the difference between a California pinot noir and a New Zealand pinot noir, or to be able to identify the quality and cost of a stranger's Prada shoes. Although Bourdieu's approach has been both widely adopted and widely critiqued,[64] it highlights the important role that

60. Pierre Bourdieu, *The Forms of Capital*, *in* HANDBOOK OF THEORY AND RESEARCH FOR THE SOCIOLOGY OF EDUCATION 241, 243 (John G. Richardson ed., 1986). In later works, Bourdieu identified symbolic capital as a fourth type of capital. DAVID SWARTZ, CULTURE & POWER: THE SOCIOLOGY OF PIERRE BOURDIEU 88–93 (1997). Symbolic capital, according to Bourdieu, is "a form of power that is not perceived as power but as legitimate demands for recognition, deference, obedience, or the services of others." *Id.* at 90.

61. Bourdieu, *supra* note 60, at 243.

62. *Id.* at 248. *See also* PIERRE BOURDIEU & LOÏC J. D. WACQUANT, AN INVITATION TO REFLEXIVE SOCIOLOGY 119 (1992) ("Social capital is the sum of the resources, actual or virtual, that accrue to an individual or a group by virtue of possessing a durable network of more or less institutionalized relationships of mutual acquaintance and recognition.").

63. Bourdieu, *supra* note 60, at 243–48.

64. Hugo Verdaasdonk, for example, argues that because Bourdieu's approach asserts that "cultural tastes are group-specific in nature[,] . . . [it] leaves little room for the idea that in adjudicating value to cultural products social agents follow a specific procedure requiring some form of rational thought." Hugo Verdaasdonk, *Valuation as Rational Decision-Making: A Critique of Bourdieu's Analysis of Cultural Value*, 31 POETICS 357, 357 (2003). As such, Verdaasdonk further claims that "Bourdieu sometimes minimizes the role of conscious (rational) thought on inconclusive grounds." *Id.* In particular, Verdaasdonk, questions whether "the theory of the habitus embodies the risk of overestimating the similarities between tastes manifested by social agents," concluding that the "risk is reduced by admitting that factors other than the habitus shape cultural preferences." *Id.*

social context plays in giving value to seemingly mundane facts, particularly if these facts are combined with demographic information.[65]

Legal scholars have applied the work of Pierre Bourdieu to various legal contexts, including criminal law,[66] agency,[67] the new economy,[68] copyright,[69] adjudication,[70] social meaning,[71] and popular legal culture.[72] To date, few scholars have applied his insights to the context of digital content or privacy. However, Bourdieu's work lends itself to these applications nicely. Indeed, his analysis of law is always situated within the context of the broader social dynamics that interact with legal structures in an emergent manner.[73] In the copyright context, Julie Cohen examines

65. *See infra* Part II.B.3.

66. *See* Ron Levi, *Auditable Community: The Moral Order of Megan's Law*, 48 BRIT. J. CRIMINOLOGY 583, 586 (2008) (discussing Bourdieu's idea that government, as the locus of all forms of capital, defines the social institutions that govern our lives).

67. *See, e.g.*, Kerry Dunn & Paul J. Kaplan, *The Ironies of Helping: Social Interventions and Executable Subjects*, 43 LAW & SOC'Y REV. 337, 364 (2009) (relying in part on Bourdieu's theory to analyze the "hegemony of individualism in American society"); Jonathan Simon, Katz *at Forty: A Sociological Jurisprudence Whose Time Has Come*, 41 U.C. DAVIS. L. REV. 935, 951 (2008) ("Structures, for Bourdieu, literally structure the active agency of subjects because they embed ways of knowing and acting on the world that a subject who has grown up in those structures knows intuitively how to read and respond to.").

68. Catherine L. Fisk, *Knowledge Work: New Metaphors for the New Economy*, 80 CHI.-KENT L. REV. 839, 856, 865 (2005) (noting Bourdieu's relevance to intellectual property metaphors).

69. Michael J. Madison, *A Pattern-Oriented Approach to Fair Use*, 45 WM. & MARY L. REV. 1525, 1627, 1685 (2004) (advocating a pattern-oriented approach to fair use and noting that Bourdieu offers an "emergentist" approach).

70. *See, e.g.*, Brian Leiter, *Heidegger and the Theory of Adjudication*, 106 YALE L.J. 253 (1996) (applying Bourdieu to better understand theories of adjudication); Judith Resnik, *Trial as Error, Jurisdiction as Injury: Transforming the Meaning of Article III*, 113 HARV. L. REV. 924, 1008 n.332 (2000) (citing Bourdieu with respect to the symbolic and political meaning of federal courts in developing legal norms).

71. Lawrence Lessig, *The Regulation of Social Meaning*, 62 U. CHI. L. REV. 943, 1000 (1995) (using Bourdieu's theory to explain how meanings are contested in the law between laypersons and lawyers).

72. Stewart Macaulay, *Popular Legal Culture: An Introduction*, 98 YALE L.J. 1545, 1555 n.46 (1989) (interpreting Bourdieu as saying that "legal professionals have the power to *attempt* to construct the meaning of everyday events and influence cultural understandings of justice" (emphasis in original)).

73. Elizabeth Mertz explains Bourdieu's approach by contrasting it with those of Niklas Luhmann and Jürgen Habermas:

> Luhmann's perspective is thus much different from that of . . . Bourdieu . . . who does not agree that the legal system is fully self-referential, transforming itself according to its own laws. Unlike Luhmann, Bourdieu strongly separates the "symbolic order of norms and doctrines" from the "order of objective relations between actors and institutions in competition with each other for control of the right to determine the law." This leads Bourdieu to analyze legal developments not in terms of an autonomous symbolic interrelation of doctrines and norms alone, but as the result of the interaction of that symbolic dimension with struggles for power in a wider social world. Although Habermas shares this concern for the social concomitants of law-internal developments, Bourdieu also differs from Habermas

copyright theory and the meaning of creativity, pointing to Bourdieu's "explorations of the ways in which expertise and authority shape cultural production."[74] She advocates that

> in cases where interests in economic stability and cultural mobility must be balanced, an examination of creative practice informed by social and cultural theory can indicate the appropriate content of pragmatic compromises designed to foster cultural mobility. Such compromises will be more effective if they operate at copyright's baseline in the form of bright-line rules.[75]

Jonathan Simon, meanwhile, applies Bourdieu to the criminal privacy context,[76] arguing in favor of "[a] stronger embrace of the role of social knowledge" as part of the "reasonable expectations of privacy test" articulated in *Katz v. United States*.[77]

In the context of consumer privacy, Bourdieu's lessons are two-fold. First, Bourdieu highlights the importance of context in creating value from information. Second, his work points to both the benefits and limitations of "being known" in a particular context. As explained above, when a consumer engages in certain speech or behaviors, that conduct conveys cultural and social "tells" about that consumer. Commercial-data monitoring removes consumers' ability to control the leakage of these tells to their detriment. Using the language of psychology, technology-driven data mining diminishes the ability of consumers to "impression manage."[78]

> in his insistence on locating his analyses in particular social settings, achieving his theory *in* the telling of the story.

Elizabeth Mertz, Preface, *Alternative Paradigms for Legal Theory*, 83 NW. U. L. REV. 1, 6 n.15 (1989) (emphasis in original) (citations omitted).

74. Julie E. Cohen, *Creativity and Culture in Copyright Theory*, 40 U.C. DAVIS L. REV. 1151, 1169 (2007).

75. *Id.* at 1204. Following Professor Cohen's advice, the last section of this Article proposes a series of contract-implied terms and remedies, including some bright-line rules, to address contract-based privacy harms.

76. Simon, *supra* note 67, at 951. Regarding Bourdieu's theory on "habitus," Simon argues:

> This kind of analysis of behavior in socially structured spaces was carried to a high level of scientific objectivity by . . . Pierre Bourdieu[,] [who] looked at a built environment as a "habitus" or "a structuring structure, which organizes practices and the perception of practices, [and] also a structured structure . . ." Structures, for Bourdieu, literally structure the active agency of subjects because they embed ways of knowing and acting on the world that a subject who has grown up in those structures knows intuitively how to read and respond to. Such structures are also "durable," resisting momentary fluctuations in public passions, as suggested by Bourdieu's description of the habitus as a "durable, transposable disposition."

Id. (second ellipses and third alteration in original) (footnotes omitted).

77. *Id.* at 943. *See also* Katz v. United States, 389 U.S. 347 (1967) (extending the Fourth Amendment protection from unreasonable search and seizure to protect individuals with a "reasonable expectation of privacy").

78. For a discussion on how social actors attempt to influence the impressions others form of them, see BARRY R. SCHLENKER, IMPRESSION MANAGEMENT: THE SELF-CONCEPT, SOCIAL IDENTITY,

In other words, when consumers cannot understand how information about them is being collected and transferred, they cannot control the impression they give to others. As a result, consumers lose the ability to exert meaningful control over the context of their conduct. Therefore, when an aggregator is permitted to monitor these tells, it potentially obtains access to a treasure trove of information that allows it to generate associations among consumers and products. In other words, privacy violations harm consumers' control over their cultural capital. Also, because this loss of control is coupled with the "pushed" nature of marketing communications,[79] privacy issues also impact social capital by affecting access to knowledge about consumers' friends. For example, social network websites frequently use friend endorsements,[80] a strategy that amounts to a sharing of the consumer's social capital.

In other words, Bourdieu's work helps articulate a legal detriment and benefit for contract law purposes in the consumer privacy context. Through Bourdieu's lens, it becomes clear that consumers do, in fact, incur a detriment in granting data access to a commercial aggregator and that the aggregator receives a benefit from such an exchange. It also becomes clear that obtaining access to such data should indeed be legally sufficient to contractually bind an aggregator to perform the promises of privacy and security that induced the consumer's exchange of information access.

2. Marketing Theory and the Value of Context

Data aggregators would argue, however, that many consumers enjoy sharing copious amounts of information with marketers—not only because consumer data sharing triggers pecuniary rewards such as coupons, but also because sharing leads to a nonpecuniary value of being recognized and known. This effect of "being known" might be termed the "Norm Effect,"[81]

AND INTERPERSONAL RELATIONS, at v (1980) ("Consciously or unconsciously, people attempt to control images in real or imagined social interactions. By doing so, they define the nature of the interaction, the identities they and others possess, and the meanings of their interpersonal actions.").

79. For a discussion of "pushed" communication technology, see KANAKA JUVVA & RAJ RAJKUMAR, A REAL-TIME PUSH-PULL COMMUNICATIONS MODEL FOR DISTRIBUTED REAL-TIME AND MULTIMEDIA SYSTEMS 4–6 (1999), http://reports-archive.adm.cs.cmu.edu/anon/1999/CMU-CS-99-107.pdf.

80. It is common practice for social networking websites to announce to a member's friend network that the member has "liked" a certain product or joined a certain group. *See*, *e.g.*, LINKEDIN, http://www.linkedin.com (last visited Sept. 29, 2013).

81. Norm was a character on the television series *Cheers* who, upon entry to the establishment, was loudly greeted by the staff bellowing his name in a sign of recognition and welcoming. *Cheers* (Charles/Burrows/Charles Productions, in association with Paramount Network Television). This type of greeting confers nonpecuniary value upon its targets, including a sense of group identity and belonging. It simultaneously partially identifies the individual to others, however, resulting in loss of

after one of the characters on the classic television show *Cheers*, who received a boisterous greeting from bar staff whenever he entered. Just as many of us enjoy the experience of the barista in our favorite café or bar greeting us by name, some consumers enjoy their beloved online stores "knowing" them. However, this Norm Effect has logical limitations. While I may enjoy my barista knowing my four shot skim latte drink order, I certainly would not want her to install surveillance equipment in my kitchen in order to be able to "know me better" when I am away from her café. Yet, this intuitive boundary is missing in digital spaces, as aggressive behavioral surveillance is precisely the turn that advertising in virtual spaces has taken. What is the critical difference between these two scenarios? It is the consumer's loss of control over context coupled with marketers' increasing technological ability to ascertain a consumer's identifying quirks and unique preferences.

Targeted or behavioral advertising,[82] in particular, embodies these questions of control over context.[83] Indeed, with increasing frequency, website advertisements are intentionally tailored to advertisers' perception of particular consumers and their interests,[84] which are deduced from mined data about their past online behavior, their "friends'" behaviors, and

anonymity.

82. The advertiser may have collected data about the consumer, licensed data about the consumer and his web surfing from a data aggregator, and potentially supplemented this data with generalizations about people who are similar to the consumer. It is this loss of contextual control over information that many consumers find troubling. According to some studies, over two-thirds of consumers view information aggregation even for personalization purposes as an invasion of privacy. Robert Hof, *People Don't Want Personalized Ads. What Should Marketers Do?*, FORBES (Mar. 9, 2012, 2:06 PM), http://www.forbes.com/sites/roberthof/2012/03/09/people-dont-want-personalized-ads-what-should-marketers-do/.

83. Behavioral advertising is the practice of tracking consumers' behavior online in order to repackage and resell this information to advertisers. For an in-depth analysis on the practice, see generally *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles*, FED. TRADE COMMISSION, http://www.ftc.gov/os/2007/12/P859900stmt.pdf (last visited Nov. 22, 2013).

84. This happens either directly or through an intermediary such as Google's advertising programs. Google describes how it targets advertisements to Gmail users in the following manner:

> [W]e work hard to help you sort through the unimportant messages that get in your way. We use a similar approach with ads. For example, if you've recently received a lot of messages about photography or cameras, a deal from a local camera store might be interesting. On the other hand, if you've reported these messages as spam, you probably don't want to see that deal. This type of automated processing is how many email services provide features like spam filtering and spell checking.

Ads in Gmail, GOOGLE, https://support.google.com/mail/answer/6603 (last visited Sept. 29, 2013).

In an effort to reassure its customers, Google also states that "[a]d targeting in Gmail is fully automated, and no humans read your email or Google Account information in order to show you advertisements or related information." *Id.*

other demographic information.[85] Behavioral advertising is particularly analogous to a nosy barista installing a camera in my kitchen to better "know" my coffee habits. But behavioral advertising perhaps goes even further: it equates to my barista not only monitoring my coffee habits at home, but also monitoring how often I vacuum—and then repurposing this information by telling maid services that I am cleaning-challenged.[86] Advertising technologies today, such as Facebook's "Like" button, now follow consumers across the web, aggregating information about them across numerous different websites for conceptually unrelated goods and services.[87]

In more practical terms, marketing literature provides a powerful explanation in the concept of a "preference minority"—a group of consumers with highly specialized tastes, interests, and purchasing preferences.[88] One of the key consequences of my data sharing is that it gives marketers the potential ability to place me in the context of a "preference minority." In particular, if my preferences reveal that I am likely to be underserved in real space, either because of geographic isolation or preference isolation of demand,[89] I may be an untapped source

85. AOL, for example, describes its data aggregation and advertising policies in the following terms:

> In the same way that we use information about you . . . to customize or personalize the content or services we provide, we may also use information to make the ads you see more relevant for you, and more effective for advertisers. We may also use information from other companies or sites to assist in determining the effectiveness of advertising. This helps advertisers spend their money wisely and helps the providers of content (publishers) increase revenues and stay online.

Advertising, Analytics, and Policy¸ AOL, http://privacy.aol.com/advertising-and-privacy (last visited Oct. 1, 2013). AOL collects this information from a variety of sources, including publicly available demographic information, website traffic patterns, and registration data or other household data that users have provided or was otherwise acquired from other companies. *Id.* Although the intended purpose of data collection is to better tailor advertisements, they are often ineffective. As one commentator complained, "[J]ust because I looked at a sweater for my wife on your site doesn't mean I want to be followed around the Web by your ads for the next week." Hof, *supra* note 82.

86. Alternatively, my coffee habits might be shared with the vacuum cleaner company in order to induce a purchase, despite an unrelated context. As one marketing consultant explained the dynamic, because she browsed but rejected a pair of clogs on a shoe website, she triggered a set of widgets that made the clogs follow her across various unrelated websites for the next several weeks. Everywhere she went online, there they were—the clogs that she had deemed too unattractive for purchase were "stalking" her.

87. For a discussion of the Facebook "Like" button and privacy, see Haley Tsukayama, *Facebook "Like" Button Violates Privacy Laws, German Official Rules*, WASH. POST (Aug. 19, 2011, 3:44 PM), http://www.washingtonpost.com/blogs/faster-forward/post/facebook-like-button-violates-privacy-laws-german-official-rules/2011/08/19/gIQADCCMQJ_blog.html.

88. Jeonghye Choi & David R. Bell, *Preference Minorities and the Internet*, 48 J. MARKETING RES. 670, 670 (2011).

89. *Id.*

of revenue. Therefore, my revelations potentially embed me in a monetizable, cultural context. In the words of leading marketing theorists, "Selling niche brands in high-[preference minority] markets is especially attractive because these customers face high offline shopping costs and are therefore less price sensitive."[90] In this manner, I confer a benefit upon marketers in granting access to seemingly mundane information: I give them the ability to attempt to generate new contexts in which to place me. By successfully placing me within a particular preference minority group, the marketer receives an information benefit.[91] Moreover, by using consumer self-reported information and matching it with demographic information about me, a marketer may be able to ascertain the extent of my social and cultural capital in order to better interact with me commercially. Stated another way, when I reveal details that are a scarce information resource, such as my favorite beer, I confer a benefit upon a marketer. Through my information transfer, I convey an insider's view of myself and my group, as well as my group's preferences, and some of its "secret handshakes." I allow the marketer to ostensibly possess more of a phatic[92] connection with my group of friends and to better identify and capitalize on unmet commercial needs. This access also allows for more resonant communication with me, which, in turn, allows marketers to better categorize me with other people who are "like" me. In this way, I confer capital to the aggregator on the one hand while simultaneously devaluing the access to my information.[93] Stated differently, my knowledge becomes less exclusive and therefore less valuable because scarcity drives the value.

Returning to the Facebook IPO, the S-1 discussion of the company's valuation faced exactly this sort of issue—how to articulate the value proposition of information whose value is inherently relational and derived

90. *Id.* at 680. Further, different behavioral dynamics for preference minorities exist in internet contexts as opposed to real space: in other words, marketing in technology-mediated spaces is context-specific. *Id.* at 681.

91. *Id.*

92. Phatic communication is a linguistics term of art referring to communication for the sake of relationship building. *See, e.g.*, *Phatic Communication*, FREE DICTIONARY, http://www.thefreedictionary.com/phatic+communication (last visited Sept. 29, 2013) (defining phatic communication as "conversational speech used to communicate sociability more than information").

93. A particular fact or preference may seem unimportant to one person, but it may be dispositive to conceptually grouping that person with people who appear similar to a marketer. Even seemingly mundane facts are useful in mapping a person's preferences and social relations for marketers; they help a data aggregator to better approach consumers and their social networks with business opportunities. This is partially the magic (and the concern) behind behavioral advertising. *See* Emily Steel & Julia Angwin, *On the Web's Cutting Edge, Anonymity in Name Only*, WALL ST. J. (Aug. 4, 2010), http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html.

entirely from context.[94] The company resorted to self-crafted, data-driven measurements in an attempt to quantify the economic value of the consumer data it collects.[95] Although commentators pointed out the slipperiness of these data valuation constructs, the market clearly recognizes the relational value of the data held by Facebook.[96] In Zuckerberg's words, "Personal relationships are the fundamental unit of our society . . . [and the means by which] we discover new ideas, understand our world and ultimately derive long-term happiness."[97] His commentary reflects an understanding of the dynamics of all three types of Bourdieu's capital—economic, social, and cultural.

3. The Case of Beer

To elaborate on the relational dynamics described above, the case of beer provides an illustrative example. As the following exercise demonstrates, access to knowledge of my favorite beer could, perhaps counterintuitively, be a high-value bit of information. It reflects a transfer of a thing of value that is relationally connected to indicators of my identity.

Let us imagine that a website has presented me with a user agreement and asks me to disclose my favorite beer brand in exchange for a five-dollar coupon. This seemingly innocuous data point initially appears to reveal little about me. But, in fact, knowledge of my favorite beer reveals much about me, particularly when aggregated with other information about me and my network of friends.[98]

Let us assume that I assert that my favorite beer is Milwaukee's Best, an inexpensive alcoholic beverage affectionately known to its aficionados as "The Beast."[99] From this assertion, a marketer is likely to assume that I am a price-conscious consumer whose primary interest in beer focuses on quantity over quality.[100] My price-consciousness may arise from a deficit

94. Facebook, Inc., *supra* note 12, at 75–80.

95. *Id.* at 44–47.

96. *See* Randall Smith & Shayndi Raice, *Facebook Beefs up Its IPO Roster*, WALL ST. J. (Mar. 14, 2012, 3:34 PM), http://online.wsj.com/article/SB10001424052970204603004577267882864878176.html (mentioning that some private markets valued Facebook's total shares at $100 billion).

97. Facebook, Inc., *supra* note 12, at 67.

98. As described elsewhere, cultural capital is composed of different "tells" regarding income, social class, group affiliations, tastes, and likely behaviors. *See supra* text accompanying notes 63–65.

99. *12 Beers You Should Only Drink in College*, CAMPUS SQUEEZE (June 13, 2011), http://www.campussqueeze.com/post/Only-College-Beers.aspx ("The Beast is probably America's worst tasting item. It honestly tastes like someone put a slice of bread in a can and poured old Miller light over it.").

100. Milwaukee's Best is a low price-point beer and one of the Miller Brewing Company's

of economic capital, but it may also arise from a deficit of cultural capital. Perhaps I think Milwaukee's Best is actually a good beer—something beer cognoscenti, if not everyone,[101] would violently oppose.[102] If the second is true but not the first, then my "mistaken"[103] opinion potentially arises from a lack of education about "correct" beer. Or perhaps The Beast is the "correct" beer in my social circle, and I pretend to like it in order to maximize my social capital. If so, how do we determine which form of capital I lack?

Marketers answer this question by constructing additional context. They pair up my beer responses with demographic information about me—whether accurate or not—and match me with potential products and services. If I am a twenty-one-year-old renting an apartment in a low-income neighborhood of a struggling city, I am employed at a fast-food chain, and my favorite beer is Milwaukee's Best, Bourdieu would say that I may have a deficit of all three forms of capital. A marketer would then deduce that I would be a bad candidate for a Roche Bobois[104] furniture marketing campaign, for example. However, if I am fifty-five, own a three-bedroom condo in SoHo, and my favorite beer is Milwaukee's Best, Bourdieu would say I may have a deficit of cultural capital but not economic capital. I simply have "bad" taste in beer. Conversely, if I am that fifty-five-year-old living in SoHo, but I assert that my favorite beer is Delirium Tremens,[105] I have just made a statement that, in beer circles, acts as a marker of high cultural capital. Beer cognoscenti would likely presume certain associations of education and resources to accompany that beer

"economy" brands. Douglas A. McIntyre, *The Eight Beers Americans No Longer Drink*, 24/7 WALL ST. (Sept. 9, 2011, 2:55 PM), http://247wallst.com/retail/2011/09/09/the-eight-beers-americans-no-longer-drink/.

101. *See infra* text accompanying notes 103–07.

102. *See, e.g.*, *Milwaukee's Best Premium—Miller Brewing Co.*, BEER ADVOCATE, http://beeradvocate.com/beer/profile/105/1286 (last visited Sept. 30, 2013) (awarding the beer a grade of 47/100, or "poor," and including reviews that liken it to "urine," which "taste[s] like afterbirth").

103. The word "mistaken" appears in quotes because a third option exists with a small number of consumers. These consumers may know that Milwaukee's Best is an objectively inferior beer by conventional beer standards and may be able to afford the most expensive beer available, yet for other reasons—such as sentimental value, they prefer to consume The Beast.

104. Roche Bobois is a furniture manufacturer that would likely be considered very expensive by an average consumer. ROCHE BOBOIS, http://www.roche-bobois.com (last visited Sept. 30, 2011).

105. Delirium Tremens is a somewhat obscure Belgian lambic beer with a higher than average beer price point and a logo of a pink elephant. *See, e.g.*, Delirium Tremens—Brouwerij Huyge, BEER ADVOCATE, http://beeradvocate.com/beer/profile/180/1385 (last visited Sept. 30, 2013). Another possible social "tell" with respect to beer consumption may be a preference for a somewhat obscure, regional microbrew. This preference may be indicative of either physical residence within the market of the brewery, frequent travel to that market, or relationships with individuals who reside in that market and have introduced the consumer to the microbrew.

preference. My love of Delirium Tremens may also place me within a beer preference minority. It may signal to marketers that I am also more likely than the other two consumers to seek out higher price point, "quality" products in other realms, such as high-end furniture. I appear to possess substantial financial resources, as I can afford to spend money on expensive beer. This may mean that I can purchase my desired products with less price sensitivity,[106] and a marketer may view me as the ideal candidate for a Roche Bobois online-marketing campaign. Meanwhile, by matching my beer preference with the preferences of my friends, my position within my social circle may be deduced, as well as the extent to which my preferences correlate with those of my friends.[107]

Knowing my favorite type of beer means that marketers are better able to form a relationship with me. They can make a better sales pitch to me because they know how to relationally embed me in a particular social context. Further, by knowing my context, marketers may be able to better sell to my entire social network; it is also likely that my beer preferences are at least partially shared within my networks of friends. In this way, marketers obtain not only economic capital but also social and cultural capital. Bourdieu's analysis of social relations highlights exactly these dynamics about the way social context is used to generate value. In fact, Bourdieu's logic is, at least in part, the asserted logic behind data hoarding of information aggregators and behavioral advertising—those who control context control value.

Perhaps the most essential part of finding value in access to information about my favorite beer and my network of friends, however, rests in its scarcity. The fewer the number of people who know the name of my favorite beer and the identities of my friends, the fewer the number of companies that can market to us with an informational edge. In other words, access to the knowledge of my favorite beer involves information that is subject entirely to my control and derives independent value from not being widely known.[108]

106. Choi & Bell, *supra* note 88, at 672.

107. Thus, my beer preferences may provide the key to marketing to my entire social circle, and to understanding how many of my friends may be similarly interested in an advertisement for expensive furniture.

108. This is also the language and logic of trade secret law. In Part III, these principles of information scarcity will be merged with ideas from trade secret law to buttress consumer privacy protection through contract. *See infra* Part III.

C. THE DISPLACEMENT FATALISM

"The single greatest obstacle to effective legal protection of privacy," according to Cohen, "is not imperfect fit with the available legal theories, but the fact that each available theory gives way to contract in many, if not all, circumstances."[109] Despite its recognition of this relationship, "[T]he law has failed to translate these challenges into a workable legal theory capable of displacing contract when threats to privacy reach unacceptable levels."[110]

Many consumers strongly believe that companies with whom they share information owe them a duty of reasonable consumer privacy and information security. These consumers' gut intuitions about their entitlements remain, despite their willingness to share information with data aggregators pursuant to terms of use and privacy policies.[111] When consumers contractually agree to give access to their data, have they also automatically and irretrievably agreed to accept the consequences of corporate mismanagement of their information? As Cohen eloquently articulates in the quote above, the default position of many noted legal scholars assumes the answer is "yes," and asserts that contract law is the enemy of consumer privacy. This third fatalism—the displacement fatalism—thus asserts that contract law must be displaced in order to protect consumer privacy. I respectfully disagree.

In Parts III and IV, I introduce a contract paradigm of implied privacy promises modeled on trade secret law and landlord-tenant law. In this section, however, I briefly investigate the conceptual privacy question that the displacement fatalism raises: the fit of contract theory as a method of reframing the consumer privacy discourse. Perhaps unexpectedly, because both contract law and consumer privacy law blend autonomy, freedom, and consumer protection concerns, they are a good conceptual match.

According to Cohen, the traditional privacy discourse has generally been divided into two strands of thought.[112] The first involves interests in intellectual privacy deriving from an interest in personal autonomy, and the second concerns physical freedom from intrusion.[113] Personal autonomy privacy interests include "rights of bodily integrity and other corporeal

109. Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 605 (2003).

110. *Id.*

111. Facebook is certainly not alone in this consumer privacy situation. Any data-intensive enterprise—be it a search engine or a hotel with a customer preference database—will regularly face this tension with respect to customers' information.

112. Cohen, *supra* note 109, at 577.

113. *Id.* at 576–79.

rights," as well as "rights over one's own thoughts and personality."[114] Surveillance and compelled disclosure result in a loss of control over uses of the gathered information. This loss "violates rights of self-determination" and "devalue[s] the fundamental dignity of persons by reducing [them] to the sum of their 'profiles.'"[115] Creating privacy rights in information about intellectual activities and preferences creates a "breathing space" for developmental and intellectual growth.[116] The second strand of privacy theory pertains to privacy within physical spaces, and "reserv[ing] certain types of 'private space' to the individual or the family."[117] In essence, privacy in physical spaces gives people room to be free from intrusion.[118]

The questions that are raised by consumer privacy create a complicated inquiry because they blend both of these strands to some extent. The "surveillance" in the consumer privacy context happens with at least some degree of contractual consent of the surveilled consumer—the consumer can, at least in theory, discontinue use of the surveilling product to terminate the surveillance. While we think of data aggregation and use as being in line with the surveillance concerns from an autonomy-based, "breathing space" perspective, this framing does not fully capture the element of economic private ordering that is central to information contracting. A contractual relationship is, in some ways, also a private space with uniquely negotiated rules between the parties. With limited exceptions, the goal is to maintain a private arrangement, free from intrusion by third parties and the state. In other words, consumer privacy issues pick up some of the "breathing space" rationale, but surround it with an economic overlay that is more in line with a "private space" and freedom-from-intrusion rationale.

Similarly, privacy has traditionally been framed with a more defensive posture, asserting an informational or physical space that cannot be invaded. However, the autonomy concerns in consumer privacy are more agentic and *offensive* in their posture. Indeed, they are driven by consumers' desire to control and selectively embed information in commercial contexts. Thus, both consumer privacy inquiries and contract law present a situation in which a consumer's autonomy to engage in a

114. *Id.* at 577.
115. *Id.* at 577–78.
116. *Id.* at 578.
117. *Id.*
118. *See, e.g.*, Anita L. Allen, *Privacy Torts: Unreliable Remedies for LGBT Plaintiffs*, 98 CALIF. L. REV. 1711, 1721 (2010) (explaining that common private places are not reliably private from intrusion for members of the LGBT community).

commercial exchange needs to coexist with a safety net against unscrupulous actors who seek to take commercial advantage of information imbalances and unequal bargaining power. In this way, a consumer privacy inquiry differs in its framing from a traditional privacy inquiry. Consumers want to be able to share information at their discretion while, at the same time, seeking to maintain a safety net of fair treatment of that information.

Turning to traditional contract doctrine and theory, we see structures reflecting this balance of economic autonomy within a broader system of economic trust and commercial safety nets.[119] As Part III explains, this flexibility of a contract approach is precisely what permits trade secret law to rely upon it.

III. CRAFTING A NEW CONTRACT THEORY OF CONSUMER PRIVACY: SELECTIVE EMBEDDING

The Dead Collector: Bring out yer dead.

[A man puts a body on the cart]

Large Man with Dead Body: Here's one.

The Dead Collector: That'll be ninepence.

The Dead Body That Claims It Isn't: I'm not dead.

. . . .

The Dead Collector: 'Ere, he says he's not dead.

. . . .

Large Man with Dead Body: Well, he will be soon, he's very ill.

The Dead Body That Claims It Isn't: I'm getting better.

Large Man with Dead Body: No you're not, you'll be stone dead in a moment.

—Monty Python and the Holy Grail[120]

119. This dynamic is particularly visible in, for example, Article 2 of the Uniform Commercial Code. For a discussion of consumer protection and Article 2, see generally James J. White, *Form Contracts Under Revised Article 2*, 75 WASH. U. L. Q 315 (1997) (discussing consumer protection and Article 2). We also see it in landlord-tenant law. *See, e.g.*, Melissa T. Lonegrass, *Convergence in Contort: Landlord Liability for Defective Premises in Comparative Perspective*, 85 TUL. L. REV. 413, 417 (2010) (discussing consumer protection under landlord-tenant law).

120. *Monty Python and the Holy Grail: Quotes*, IMDB, http://www.imdb.com/title/tt0071853/quotes (last visited Oct. 1, 2013). *See also* MONTY PYTHON AND THE HOLY GRAIL (Python (Monty) Pictures Ltd. 1975).

Contract law is not quite yet dead in consumer privacy. As Zuckerberg explained in the Facebook S-1, Facebook and companies like it will continue to knowingly push the boundaries of technology, law, and consumers' privacy comfort zones. Their legal tool of choice is contract law—the modification of terms of use and privacy policies.[121] For example, around the time of its IPO, Facebook found itself facing a Federal Trade Commission inquiry in response to a complaint filed by four consumer privacy groups,[122] as well as extensive negative press coverage with respect to its evolving data disclosure policies.[123] Perhaps most damaging to the goodwill of the company, however, was the disclosure of a series of cavalier instant messages that Zuckerberg sent during the early days of the company. In these messages, he allegedly used colorful language to question the intelligence of four thousand Harvard students who "trusted" him to act as a steward of their personal information.[124] The perceived tone of this exchange when coupled with Facebook's contractual modifications struck a cacophonous chord both with the press and Facebook users.[125] However, contract law is not merely a tool for diminishing consumer privacy. Through constructing a contract law approach of implied privacy promises modeled on trade secret law, legislatures and courts can craft a legal regime in which consumers maintain the ability to selectively embed data, cushioned by a net of consumer protection.

121. Craig Timberg, *Instagram, Facebook Stir Online Protests with Privacy Policy Change*, WASH. POST (Dec. 18, 2012), http://articles.washingtonpost.com/2012-12-18/business/35908189_1_ kevin-systrom-instagram-consumer-privacy (detailing user backlash against changes to Facebook's and Instagram's terms of use). Thus, even as regulators and legislators craft new approaches to consumer privacy, business reality reminds us of contract law's importance in the consumer privacy conversation.

122. Complaint, Request for Investigation, Injunction, and Other Relief, *In re* Facebook, Inc. and the Facial Identification of Users (F.T.C. June 10, 2011), *available at* http://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf.

123. *E.g.*, Maria Aspan, *How Sticky Is Membership on Facebook? Just Try Breaking Free*, N.Y. TIMES (Feb. 11, 2008), http://www.nytimes.com/2008/02/11/technology/11facebook.html? pagewanted=all&_r=0 ("Some users have discovered that it is nearly impossible to remove themselves entirely from Facebook, setting off a fresh round of concern over the popular social network's use of personal data."); *Facebook Opens Profiles to Public*, BBC NEWS (Sept. 6, 2007), http://news.bbc.co.uk/2/hi/technology/6980454.stm (discussing criticism of Facebook policy changes that added a public search element).

124. When a friend asked Zuckerberg how he compiled information of his Harvard classmates, Zuckerberg reportedly replied, "I don't know why [people submitted the information] . . . They 'trust me' . . . Dumb f[–]cks." Nicholas Carlson, *Well, These New Zuckerberg IMs Won't Help Facebook's Privacy Problems*, BUS. INSIDER (May 13, 2010, 11:19 AM), http://www.businessinsider.com/well-these-new-zuckerberg-ims-wont-help-facebooks-privacy-problems-2010-5.

125. *See id.*

A. WHY CONTRACT?

Why is contract law an important and viable component of a consumer privacy safety net? In analyzing consumer privacy questions, courts recognize that privacy harm arises from a failed commercial exchange. As a practical matter, courts generally begin any consumer privacy inquiry with contract law analysis, asking whether a contract has been formed allowing particular information access.[126] Except for very limited circumstances,[127] contract law is not preempted even by copyright law when an agreement exists between the parties. As explained in *ProCD, Inc. v. Zeidenberg*,[128] when a contract between the parties exists, contract law is not preempted, regardless of whether the subject matter is copyrightable.[129] In other words, courts always begin a consumer privacy inquiry by determining whether a contract was properly formed—requiring an offer, acceptance, and legally sufficient consideration.[130] As Part II explained,

126. *E.g.*, Doe v. SexSearch.com, 551 F.3d 412, 416 (6th Cir. 2008); Greer v. 1-800-Flowers.com, Inc., No. H-07-2543, 2007 U.S. Dist. LEXIS 73961, at *5–6 (S.D. Tex. Oct. 3, 2007).

127. In *Rano v. Sipa Press, Inc.*, the Ninth Circuit held that copyright preempted state law relating to the at-will termination of a license with an indefinite duration because when "California law and federal law are in direct conflict, federal law must control." Rano v. Sipa Press, Inc., 987 F.2d 580, 585 (9th Cir. 1993). Assignability of a licensee's rights would provide another preemption basis because federal law prohibits such rights from being assigned in a nonexclusive license without the consent of the licensor. *Compare In re* CFLC, Inc., 89 F.3d 673, 679 (9th Cir. 1996) ("[F]ederal law governs the assignability of patent licenses because of the conflict between federal patent policy and state laws, such as California's, that would allow assignability."), *with* Chamberlain v. Cocola Assocs., 958 F.2d 282, 283 (9th Cir. 1992) (applying California statute regarding transfer of tangible object in the case of transfer of intangible rights to use object).

128. ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1454 (7th Cir. 1996). *ProCD* was the first appellate ruling dealing with the enforceability of shrinkwrap licenses and held that the contract restrictions placed on the use of a noncopyrightable database were not preempted by copyright law. *Id.* at 1453–55. *See also* Altera Corp. v. Clear Logic, Inc., 424 F.3d 1079, 1089–90 (9th Cir. 2005) (citing *ProCD*, 86 F.3d at 1454–55) (holding that copyright does not preempt contract enforcement); Davidson & Assocs. v. Jung, 422 F.3d 630, 638–39 (8th Cir. 2005) (holding that user's license was not preempted by fair use); DaimlerChrysler Servs. N. Am., LLC v. Summit Nat'l, Inc., 144 F. App'x 542, 548 (6th Cir. 2005) (holding that copyright defenses are irrelevant to contract enforcement); Bowers v. Baystate Techs., Inc., 320 F.3d 1317, 1323 (Fed. Cir. 2003) (holding that the license was not preempted by fair use).

129. In reaching that conclusion, the *ProCD* court compared the case to *Aronson v. Quick Point Pencil Co.*, 440 U.S. 257 (1979), in which "enforcement . . . would not withdraw any information from the public domain." *ProCD*, 86 F.3d at 1455. As such, the *ProCD* court explained:

> Everyone remains free to copy and disseminate all 3,000 telephone books that have been incorporated into ProCD's database. Anyone can add SIC codes and zip codes. ProCD's rivals have done so. Enforcement of the shrinkwrap license may even make information more readily available, by reducing the price ProCD charges to consumer buyers.

Id.

130. The data aggregator defendant argues consent through contract, asserting that the data subjects have consented to the full panoply of the company's conduct when they executed the end user license agreement or terms of use. As such, courts begin the inquiry with a traditional contract interpretation discussion, in which courts are amply experienced and something they prefer over the

consumers have indeed offered access to their information—a form of legally sufficient consideration—in exchange for access to certain services from a company.[131] However, as I have argued elsewhere,[132] many end user license agreements, terms of use, and privacy policies raise serious questions about formation[133] and unconscionability.[134] Nevertheless, if courts find that a valid agreement exists, they almost always analyze the privacy inquiry as being governed by the terms of that agreement.[135] As such, a key component of any successful consumer privacy law regime by necessity involves addressing the privacy harms that happen *inside* contractual relationships.

Consumer privacy law currently lacks the types of consumer protection measures and implied ground rules of reasonable commercial conduct found in contract law. Traditional contract law is already emboldened by various consumer protection measures against unscrupulous conduct of "merchants"—commercial parties with greater business sophistication and bargaining power than an average consumer.[136] In addition to the doctrinal and conceptual fit between contract and consumer privacy, as already discussed, contract law approaches to privacy allow consumers to operate within a legal space accustomed to the presence of implied promises. Other contracting contexts, such as those around sales of goods and landlord-tenant relationships, offer insight as to the potential of implied promises to neutralize the power imbalances between consumers and data aggregators. Further, contract approaches provide a useful supplement to tort approaches to privacy, filling in gaps where tort law falls short without offending the First Amendment. Even scholars skeptical of consumer privacy rights as a concept conclude that contract-based approaches to privacy are feasible. As one skeptic concluded, "[P]rivacy protection secured by contract turns out to be constitutionally sound."[137]

uncertainty of technology law or privacy inquiries.

131. *See supra* Part II.

132. *See* Matwyshyn, *supra* note 27, at 548–56 (analyzing limitations to meaningful consumer digital contracting).

133. *Id.* at 550–54.

134. *Id.* at 554–56.

135. Although courts often find these contracts problematic, they generally enforce them. *Id.* at 550–56 (discussing several cases which represent a "sliding scale of User Agreement enforceability"). For a discussion of the relationship of contract and privacy, see Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1645 (2011) (suggesting that user privacy is threatened whenever courts "solely rely on standard-form contracts" and "ignor[e] other elements of the contractual relationship between the website and user").

136. *See* U.C.C. § 2-104 (2011–2012) (describing merchants as persons who hold themselves out as "having knowledge or skill peculiar to the practices or goods involved in the transaction").

137. Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of*

1. The Importance of Consumer Protective Implied Terms

As the previous section explained, contract theory offers a framing for the consumer privacy discourse that balances economic autonomy and consumer protection.[138] Although courts work to enforce contracts in line with the individual deals of parties, they simultaneously acknowledge the need for a baseline of fairness and consumer protection in contract formation and performance.[139] Contract law recognizes that not all bargaining situations are ideal.[140] Despite its flexibility and overall liberality with regard to deal terms, strong implied rules exist in contract law in the United States, both through state statutes and in case law.[141] In other words, statutory approaches and case law have evolved to balance economic concerns with moral and relational ones in contract.[142] However, this evolution is not yet visible in privacy law.

State statutes embody numerous implied consumer protection rules for contracting in various contexts, including consumer goods transactions,[143] lending transactions,[144] real estate sales and leases,[145] securities

a Right to Stop People from Speaking About You, 52 STAN. L. REV. 1049, 1049 (2000).

138. In an ideal contracting situation, one party negotiates with another party on terms idiosyncratic to the transaction, with the so-called master of the offer dictating both the terms of the offer and the manner of acceptance. *See* 2 WILLISTON, *supra* note 25, § 6:28 (describing how certain manifestations of acceptance may not constitute legal acceptance when the offer specified a particular manner, time, or place of acceptance). Another hallmark has traditionally been the comparative predictability of contract law. Because of contract law's preference for objective, not subjective, interpretations, competent counsel can frequently guide clients effectively as to structuring relationships in an enforceable manner.

139. For a discussion of consumer protection in contracting, see, for example, Larry Bates, *Administrative Regulation of Terms in Form Contracts: A Comparative Analysis of Consumer Protection*, 16 EMORY INT'L L. REV. 1, 28–33 (2002).

140. For a discussion of bargaining imbalances, see, for example, Larry A. DiMatteo & Blake D. Morant, *Contract in Context and Contract as Context*, 45 WAKE FOREST L. REV. 549, 565 (2010).

141. For a discussion of implied promises in contract, see, for example, 23 WILLISTON, *supra* note 25, § 63:21.

142. *See, e.g.*, Ian R. Macneil, *Relational Contract Theory: Challenges and Queries*, 94 NW. U. L. REV. 877, 881–92 (2000) (outlining the idea that all contracts must be analyzed by reference to the relations in which their underlying transactions are embedded in order to ensure a complete understanding of relations and transactions).

143. For a discussion of consumer goods transactions, see, for example, Richard H. Nowka, *Allowing Dual Status for Purchase-Money Security Interests in Consumer-Goods Transactions*, 13 TRANSACTIONS: TENN. J. BUS. L. 13, 13–15 (2011) (discussing the relationship between Article 9 of the UCC and consumer-goods transactions).

144. *See, e.g.*, 47 C.J.S. *Usurious Contracts and Transactions* § 156 (2005) (stating that usury laws generally apply to all loan transactions unless expressly exempted by state statutes).

145. *See, e.g.*, Jonathan M. Purver, *Modern Status of Rules as to Existence of Implied Warranty of Habitability or Fitness for Use of Leased Premises*, 40 A.L.R. 3d 646, § 1 (1971) (noting that courts have relied upon statutory provisions to impose an implied warranty of habitability that protects tenants).

transactions[146] and many other specific types of contracts. It was these concerns over building broader structures of trusted exchange in goods that led to the drafting of the Uniform Commercial Code and its embodiment in some form by every state.[147] Contract case law, perhaps surprisingly, is a frequent locus of morality discussions as to social desirability and correctness of certain actions.[148] Contract law on occasion seeks to punish parties who take advantage of knowledge disparities to the detriment of the other party, as well as denying the contractual fruits of economic autonomy to those who "damage" society with respect to the types of agreements they execute.[149] Further, contract law is often more interested in building and preserving relationships rather than unwinding or terminating them.[150] Indeed, consumers do not always wish to simply terminate a contract; instead, they often wish to recalibrate the relationship on "fair" terms. This relational focus is precisely at issue in consumer privacy contexts.[151] In

146. *See, e.g.*, Joseph C. Long, *State Securities Regulation—An Overview*, 32 OKLA. L. REV. 541, 543 (1979) (referring to blue sky laws as "the first consumer protection statutes").

147. Various states' versions of the UCC contain implied provisions granting consumers a more protective set of contract rules than the rules merchants can choose to apply in their transactions with each other. These implied terms vary state to state, as does the extent to which parties can contract out of them. 18 WILLISTON, *supra* note 25, § 52:86.

148. Consequently, statutory law and case law have aimed to balance individual party agency with broader structural trust through, for example, creating the distinction between consumer and merchant contracting norms in goods, the norm of contra proferentem in interpretation, and the implied covenants of good faith and fair dealing in performance and enforcement.

149. *See, e.g.*, Syester v. Banta, 133 N.W.2d 666, 676 (Iowa 1965) (affirming a jury award of exemplary damages to plaintiff elderly widow in light of "the evidence of greed and avariciousness on the part of the defendants" who compelled plaintiff to enter into a contract via fraud); RESTATEMENT (SECOND) OF CONTRACTS § 178 (1981) (describing the various factors courts should take into account when deciding whether a contract is unenforceable on grounds of public policy); *id*. § 347 (describing the measurement of damages based on an injured party's expectation interest); Joseph M. Perillo, *Restitution in a Contractual Context and the Restatement (Third) of Restitution & Unjust Enrichment*, 68 WASH. & LEE L. REV. 1007, 1010–11 (2011) (describing the doctrines of unjust enrichment and quantum meruit as means of securing a plaintiff's reliance recovery).

150. *See, e.g.*, RESTATEMENT (SECOND) OF CONTRACTS § 178 (directing courts to assign weight to factors supporting enforceability when deciding whether or not to enforce contract terms on grounds of public policy).

151. The goal of facilitating trust in the marketplace and predictable exchange leads courts to try to salvage relationships when possible. In seeking to balance the interests of the individual parties, courts deciding contract disputes do not presume irreconcilable animus between the parties. It is a default rule of contract interpretation to salvage the existence of a contract whenever possible. As Ian Macneil correctly highlighted in his work on relational contract, contract law and contractual relations are motivated by an iterated process in many cases. It benefits both the parties and economic relations as a whole to preserve contracts and the underlying relationships whenever possible. *See* Macneil, *supra* note 142, at 899 (suggesting that relational contract law may serve to maintain contractual relationships when the common behavior and norms between parties otherwise required to uphold the relationship have fallen apart). Contract law tends not to presume that the relationship of the parties is at an end and instead tries to embody default rules intended to help parties amicably resolve differences. Contract law includes numerous cases where business partners litigated disputes with each other in the short term but

some types of consumer information sharing contracts, just as in a landlord-tenant relationship, consumers may not want to permanently sever the contractual relationship with the data aggregator. Rather, they seek "livable" conditions and primarily wish to improve the relationship under an indirect form of legal "supervision." As demonstrated by consumers' reluctance to close their Facebook accounts and leave the website despite filing FTC complaints and expressing anger over privacy practices, consumer information contracting is an iterated, relational process.[152]

By way of example, let us turn to a contracting context with historical bargaining and power imbalances that are perhaps similar to those in privacy—landlord-tenant relationships—which illustrates the potency of implied terms as a method of consumer protection in contract law. Because of the form contracts used in residential leasing, the largely take-it-or-leave-it nature of negotiations, and the significant difference in bargaining positions between landlords and tenants, courts and legislatures began to craft implied promises of landlord conduct as nonwaivable warranties into contract law. As Williston explains:

> The widespread promulgation of state legislation governing, to one degree or another, residential leases, including statutes broadly imposing an implied warranty of habitability in such leases, has to a great extent modified and undercut the harshness of the common-law rule as applied to the typical residential lease. Moreover, in many jurisdictions, the courts, either following the lead of their legislatures or moving independently, have judicially declared the existence of an implied warranty of habitability, thereby making the landlord responsible to repair or maintain premises, before the inception of the landlord-tenant relationship, during its continuance or both.[153]

Landlord-tenant implied warranties offer an example of a consumer protection regime that corrected the types of problems that currently exist in consumer privacy.[154] Just as people want safe physical spaces to inhabit,

continued their working relationship in the long term. *See, e.g.*, E. Air Lines, Inc. v. Gulf Oil Corp., 415 F. Supp. 429, 431 (S.D. Fla. 1975) (describing the relevant controversy as threatening to disrupt a decades-long and "historic" mutually advantageous relationship between the parties).

152. The lack of legal liability for deficient information stewardship has resulted in a lack of corporate investment and management attention to information security inside some companies. *See, e.g.*, Dissent, *Knock, Knock. Who's There? No One.*, DATA LOSS DB (Feb. 22, 2013), http://datalossdb.org/incident_highlights/57-knock-knock-who-s-there-no-one (detailing an episode in which the author attempted to inform a hospital of a security breach related to patient records, only to find that the hospital had no one to respond to or even process the alert).

153. 15 WILLISTON, *supra* note 25, § 48:11 (footnote omitted).

154. Further discussion of lessons from landlord-tenant law for privacy and information security will be provided in Part IV.

they also want safe digital spaces. This type of consumer protection regime of implied promises is what consumers want—and what is currently missing in consumer privacy law. As the discussion of consumer complaints against Facebook in Part III illustrates, consumers do not want to disengage completely from Facebook; instead they want fair disclosure and fair process. They want Facebook to honor the terms of the deal they believed themselves to be entering and which further caused them to become upset due to what they perceived as Facebook's unilateral and opaque alteration of the contracts. In particular, consumers feel incapable of understanding the ambiguities in their information sharing contracts when they click "yes," and they believe these ambiguities are then leveraged by the drafters against them at an unknown future time.

Let us turn to an example of how judicially or legislatively crafted implied contract promises of data privacy and information security might dramatically improve the consumer protection situation: the recent harmonization of over sixty privacy policies across Google products.[155] When Google announced this harmonization, consumers became concerned about the impact of this change on their information, yet they felt helpless in understanding esoteric legal changes across over sixty privacy policies and corresponding user agreements.[156] Once the new harmonized policy was launched, mass confusion reigned about the meanings of potentially conflicting terms, and regulators' calls for investigation added to the consumer discomfort.[157] Asking consumers to read and process over sixty privacy policies and user agreements and then compare each against a new set of contracts seems farcical at best, particularly when even privacy experts cannot agree on the implications of the changes.[158]

Now, let us imagine a parallel universe where implied consumer protective privacy and information security promises are embedded in every contract by law. While users still may not be able to comprehend the individual changes to the policies, consumers' confidence remains intact—they know that ultimately a certain floor of data protection remains in place regardless of any other contractual changes. Just as renters might know that, no matter what happens, they will not freeze during winter because

155. *See* Bianca Bosker, *Google Privacy Policy Changing For Everyone: So What's Really Going To Happen?*, HUFFINGTON POST (Feb. 29, 2012), http://www.huffingtonpost.com/2012/02/29/google-privacy-policy-changes_n_1310506.html (reviewing Google's updated policy).

156. *Id.*

157. Amberhawk Training, *Google's Privacy Policy: Incoherent and Confusing*, REGISTER (Mar. 6, 2012), http://www.theregister.co.uk/2012/03/06/why_google_privacy_policy_is_so_difficult_to_follow/.

158. *Id.*

their landlord is legally required to provide heat to their apartment,[159] so too consumers in this parallel universe have confidence that regardless of how the company subsequently interprets its terms of use and privacy policies, their data is reasonably protected as a matter of law because of implied promises of data privacy and security.

2. Filling Tort Law's Gaps

Scholarship on consumer privacy usually favors tort remedies in line with William Prosser's four seminal privacy torts.[160] In light of this trend, one might ask why am I advocating a contract-based approach to privacy rather than simply a different tort-based approach? Firstly, the two approaches are not mutually exclusive, and a tort regime is likely still necessary. The contract approach advocated here is intended to supplement other approaches, not to supplant them. However, and secondly, a tort regime alone simply cannot reach all aspects of consumer privacy. As Part IV illustrates, there are aspects of consumer privacy that a contract regime can address more effectively than a tort-only regime.

As Neil Richards and Daniel Solove have argued, Prosser's privacy tort legacy is mixed at best.[161] Causality problems plague plaintiffs as an evidentiary matter in tort actions, and actual quantifiable damages are similarly difficult to prove for purposes of a tort recovery.[162] But, even assuming causality and damages problems can be overcome in a tort approach, three of Prosser's privacy torts—intrusion, public disclosure of private facts, and false light—usually require that the disclosed information be "offensive" to reasonable persons.[163] As such, their effectiveness for unwanted disclosures of factual or opinion information such as your social security number, mother's maiden name, or favorite color inside a

159. *See, e.g.*, Purver, *supra* note 145, § 5.

160. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

161. Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1890 (2010) ("Prosser's legacy is a mixed one: Although Prosser gave tort privacy order and legitimacy, he also stunted its development in ways that have limited its ability to adapt to the problems of the Information Age."). Diane Zimmerman further suggests that the right of privacy as developed by Samuel Warren and Louis (later Justice) Brandeis "has actually had a pernicious influence on modern tort law because it created a cause of action that, however formulated, cannot coexist with constitutional protections for freedom of speech and press." Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 293 (1983) [hereinafter Zimmerman, *Requiem for a Heavyweight*]; *See also* Diane Leenheer Zimmerman, *Musings on a Famous Law Review Article: The Shadow of Substance*, 41 CASE W. RES. L. REV. 823, 828 (1991) ("Constitutional privacy and the right to protect private information [as developed by Warren and Brandeis] have little in common.").

162. *See* Richards & Solove, *supra* note 161, at 1922–23 (discussing improvements to tort law).

163. *Id*. at 1919.

contractual relationship is limited.

Although the fourth of Prosser's privacy torts, commercial appropriation, perhaps offers the best fit for harms arising out of disclosures of factual and opinion information of the sort described above, it still poses an unsatisfying approach standing alone. When constructed as requiring an intentional act of appropriation,[164] the tort of commercial appropriation fails to reach consumer privacy harms arising from neglect, such as harms from data breaches due to failures of rudimentary updates to information security systems. Even when an unintentional basis for commercial appropriation can sustain liability, courts usually require a "publication" to have occurred.[165] Scholars likely push the logical limits of the legal argument when they argue that a "publication" is created whenever an information criminal obtains social security numbers because of substandard encryption protocols.

In the spirit of Prosser's torts, some authors advocate imposing a duty of confidentiality into certain types of intimate relationships. Richards and Solove support the imposition of a duty of confidentiality upon intimate relationships to resolve disputes—a confidentiality tort modeled on British law.[166] Andrew McClurg, on the other hand, argues that "[m]ass dissemination of private information acquired during an intimate relationship is an indecent and irresponsible breach of trust—and contract."[167] However, neither of these arguments reaches questions of consumer privacy, especially if a contract already exists between the parties.[168] Nevertheless, tort solutions for privacy harms, though difficult to craft for the reasons above, can indeed successfully address a limited set of harms arising out of the privacy-troubled relationships in the marketplace.

164. *See, e.g.*, 3 RESTATEMENT (SECOND) OF TORTS § 652C (1977) ("One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.").

165. *See id.* cmt. b ("The common form of invasion of privacy under the rule here stated is the appropriation and use of the plaintiff's name or likeness to advertise the defendant's business or product, or for some similar commercial purpose.").

166. Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 156–58, 181–82 (2007).

167. Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887, 938 (2006).

168. Consumer privacy turns on an infringement of personally identifiable information, or PII, which is a concept of central importance in privacy law since many privacy statutes and regulations limit their protection to it alone. But PII is a notoriously malleable concept. Schwartz & Solove, *supra* note 58, at 1816. Thus, Schwartz and Solove advocate expanding the definition of PII into one that "protects information that relates either to an identified or identifiable person, and associates different legal interests with each category." *Id.* at 1894.

However, the toughest set of privacy harms for a tort regime to address arguably arises from the scenario in which a data subject gives a limited contractual consent pursuant to an ongoing business relationship. As evidenced by the public outcry over Facebook's Beacon and Instant Personalization programs,[169] even when consumers knowingly enter into a contractual relationship, they frequently understand their consent in less expansive ways than does the company collecting information. It is these harms in particular that a contract-based approach of implied promises modeled on trade secrecy can better address.[170]

3. Avoiding First Amendment Pitfalls

As *Sorrell*[171] reminds us, data privacy regulation can easily run afoul of the First Amendment. Yet, in *Sorrell*, the Supreme Court also acknowledged that the data privacy consumer protection concerns expressed by state legislatures are legitimate, stating that "[p]erhaps the State could have addressed physician confidentiality through 'a more coherent policy.' For instance, the State might have advanced its asserted privacy interest by allowing the information's sale or disclosure in only a few narrow and well-justified circumstances."[172] From the tenor of this language, it is fair to say that the Court is not inherently hostile to all forms of data protection approaches in law. The question instead turns on which forms of data protection comport with the First Amendment. According to *Sorrell*, "[P]rivate decisionmaking can avoid governmental partiality and thus insulate privacy measures from First Amendment challenge."[173] With this language, the Court embraced the viability of contract as a method of consumer privacy protection.

In other words, a contract-based construction of privacy avoids the First Amendment pitfalls that may accompany many tort-based and other statutory approaches. Diane Zimmerman explores the legacy of Samuel Warren and Louis (later Justice) Brandeis's privacy torts and identifies the promise of a contract-based approach, stating:

> In the context of private commercial and professional services, however, a careful identification of particularly sensitive situations in which

169. Pascal-Emmanuel Gobry, *Is This a New "Beacon Moment" for Facebook?*, BUS. INSIDER (Apr. 28, 2010, 6:33 AM), http://www.businessinsider.com/us-senate-pokes-facebook-wants-them-to-make-their-new-service-opt-in-2010-4.

170. *See infra* Part III.B.

171. Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011).

172. *Id.* at 2668 (citation omitted) (quoting Greater New Orleans Broad. Ass'n v. United States, 527 U.S. 173, 195 (1999)).

173. *Id.* at 2669.

> personal information is exchanged, and an equally careful delineation of the appropriate expectations regarding how that information can be used, could significantly curtail abuses without seriously hampering freedom of speech. At the very least, this possibility merits considerably more thought as an alternative to the Warren-Brandeis tort than it has received thus far.[174]

Eugene Volokh, a privacy law skeptic, also takes up the question of information privacy rules and agrees that privacy protections secured by contract are constitutionally sound even assuming that broader information privacy rules may violate the First Amendment.[175]

Viewed from a different First Amendment perspective, consumer privacy concerns trigger questions regarding consumer speech and economic self-realization—an autonomy-based rationale articulated in First Amendment literature on commercial speech.[176] When consumer privacy questions are reframed as questions of consumers selecting the commercial context for their "speech," a conceptual parallel to First Amendment arguments becomes evident: consumers want the ability to control the audience for their online speech in the ways they would otherwise be able to control in physical space.

The practical dynamics of the consumer privacy debate are driven in large part by this consumer interest in limited self-commodification and controlled economic self-realization. However, these consumer goals conflict with data aggregators' interest in maximal commodification of the consumer's information. Thus, the consumer privacy discussion can be reframed in terms of consumer speech interests: consumers seek control over "selectively embedding" their identities and information into various economic contexts—an act of economic self-realization.[177] As Paul

174. Zimmerman, *Requiem for a Heavyweight*, *supra* note 161, at 364.

175. Volokh, *supra* note 137, at 1057–61.

176. For a discussion of various theories of free speech and their connection to commercial speech and self-realization, see, for example, Martin H. Redish, *The Value of Free Speech*, 130 U. PA. L. REV. 591, 596–601, 630–35 (1982); and see also, for example, C. Edwin Baker, *Scope of the First Amendment Freedom of Speech*, 25 UCLA L. Rev. 964, 966 (1978) [hereinafter Baker, *Scope*] (arguing that the development of individual self-realization and self-determination is the key value of free speech); and C. Edwin Baker, *Commercial Speech: A Problem in the Theory of Freedom*, 62 IOWA L. REV. 1, 34–36 (1976) [hereinafter Baker, *Commercial Speech*] (emphasizing that speech functions as a manifestation of the self and that, on account of the profit requirement, corporations cannot be considered as possessing the same interests in self-expression as other individuals or entities).

177. Consumers want to share the name of their favorite beer for a $5 coupon, take the "Which Muppet Baby Are You" quiz on Facebook, and have a feeling of data control too. These activities are arguably acts of economic self-realization and commercial speech. If so, they would merit constitutional protection because, according to Martin Redish, they aid consumers in making economic decisions that affect their lives and thus contribute to their ability to self-realize. Redish, *supra* note 176, at 630. *See*

Schwartz correctly explains, in practice, consumers are already commodifying their data.[178]

Yet, the dynamics of consumers' desire to economically self-realize while maintaining control over context are not unique. Parallel dynamics play out for corporate persons in trade secret law. By modeling a consumer privacy approach on trade secret law—a different data protection contracting context, we can realize the potential of contract law to offer consumer protection in privacy and information security contexts.

B. SELECTIVE EMBEDDING: A CONTRACT MODEL INSPIRED BY TRADE SECRET LAW

As the previous sections explained, contract law offers a viable legal vehicle for privacy protection that has been used in other consumer protection contexts. A contract approach to privacy also nicely complements a tort approach because it can reach undesirable conduct without offending the First Amendment. Perhaps most importantly, contract law is built around an iterative and relational paradigm that is well suited for consumer privacy. Consumers seek an ability to self-commodify through data sharing while maintaining a safety net of consumer protection that gives them a modicum of control. In other words, consumers are seeking the type of "contextual integrity"[179] rights that trade secret holders possess when they selectively choose to share access to their proprietary information. This section explains the interest in contextual integrity and presents trade secret law as a model for a contract-based approach to consumer privacy protection.

1. Contextual Integrity

Judge Posner has asserted that "when people today decry lack of privacy, what they want . . . is mainly something quite different from seclusion: they want more power to conceal information about themselves that others might use to their disadvantage."[180] He is half, but not fully,

also, *e.g.*, Baker, *Scope*, *supra* note 176, at 990–1009 (describing self-fulfillment as one of the key values protected by the First Amendment); Baker, *Commercial Speech*, *supra* note 176, at 3–6 ("[P]rofit-motivated or commercial speech lacks the crucial connections with individual liberty and self-realization which exist for speech generally, and which are central to justifications for the constitutional protection of speech . . . ." (footnote omitted)).

178. Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2069–72 (2004).

179. For a discussion of contextual integrity and privacy, see generally Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).

180. RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 271 (1983).

correct. In the context of consumer data sharing, he is correct that when consumers speak of "privacy" today, they frequently mean something quite different from seclusion. However, he is incorrect that the consumer privacy interest is solely in concealment in commercial contexts. Consumers, just like intellectual property owners, instead want to be able to *selectively* embed and commercially exploit their information. The consumer interest rests in *controlled economic self-realization* and *preservation of contextual integrity*.[181]

Let us consider an example of an attorney sitting next to a college student on an airplane to London. The attorney travels to London weekly on business, but this is the college student's first trip. As a gesture of kindness, the attorney allows the college student to friend him on a social network website in case the student needs advice during his travels. Neither party intends on becoming close friends, nor do the two have much in common. Further, the attorney does not know that the student engages in extensive illegal home-grow marijuana operations and that he purchases the equipment for this illegal enterprise through the Internet. However, noting at least two points of purchasing behavior in common—airplane tickets and sundries in London—and the existence of the social network relationship, advertisers conclude that the two consumers are similar and begin to push hemp and drug treatment clinic advertisements to the attorney. Perturbed but powerless, the attorney does not understand why these advertisements are arriving to him. He is unable to deduce the behavioral connection to the student because the connection is not transparent to him—only the aggregator knows it. The attorney fears that his reputation will be sullied as his involuntary association with the advertising list of "potheads" spreads. Particularly in light of employer background checks that increasingly use commercial databases as part of an employment inquiry,[182] this association, he fears, could cost him a job in the future. He also worries that numerous networks of professional contacts will now be served advertisements with his picture saying, "One of your friends is thinking about starting a BC Bud home-grow operation. Maybe you should too!"[183]

181. If a "concealment" interest of any sort exists, it perhaps pertains to consumers' desire to prevent false information and unfair negative associations from damaging their reputations and employment prospects.

182. Joe Bonné, *Most Firms Now Use Background Checks*, TODAY NEWS (Jan. 21, 2004, 6:41 PM), http://today.msnbc.msn.com/id/4018280/ns/today-today_news/t/most-firms-now-use-background-checks/.

183. As this example demonstrates, websites do not always analyze a consumer's intent in consenting to a service in a manner consistent with the consumer's subjective intent. *See* Eric Goldman, *A Coasean Analysis of Marketing*, 2006 WIS. L. REV. 1151, 1205–07 (discussing that consumer intent changes over time or is inaccurate due to insufficient information).

Consumer privacy scholarship demonstrates a growth in literature about the importance of context in assessing digital information. Helen Nissenbaum convincingly argues in favor of legal approaches that preserve the contextual integrity of information. She writes, "Contextual integrity ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it."[184] Taking up questions of contextual control in light of user-generated videos and online social networks, Jacqueline Lipton "identifies gaps in privacy law with respect to online-video privacy . . . . [and] notes that current tort laws are ill-suited to the digital age and are globally disharmonized."[185] She cautions that denying the data subject an opportunity to create context can

184. Nissenbaum, *supra* note 179, at 119. Nissenbaum's highlighting of contextual integrity is both insightful and important. However, her application of the analysis to the context of commercial information collection perhaps slightly mischaracterizes certain norms of data collection and excludes others. Taking up the case study of commercially collected information in the context of contextual integrity, she asserts:

> In the past, it was integral to the transaction between a merchant and a customer that the merchant would get to know what a customer purchased. . . . [C]ompetent merchants, paying attention to what customers wanted, would provide stock accordingly. Although the online bookseller Amazon.com maintains and analyzes customer records electronically, using this information as a basis for marketing to those same customers seems not to be a significant departure from entrenched norms of appropriateness and flow. By contrast, the grocer who bombards shoppers with questions about other lifestyle choices—e.g., where they vacationed, what movies they recently viewed, what books they read, where their children attend school or college, and so on—does breach norms of appropriateness. The grocer who provides information about grocery purchases to vendors of magazine subscriptions or information brokers like Seisint and Axciom is responsible not only for breaches of norms of appropriateness but also norms of flow.

Id. at 152–53.

Nissenbaum misses two distinctions between traditional brick-and-mortar booksellers and modern online booksellers: a bookseller in real-space does not follow patrons throughout the store, taking careful notes on every book they have touched and subsequently analyze any linkages. If a real-space bookseller did follow patrons around a store taking notes, they would notice it. Digital data collection, on the other hand, is invisible to users in most cases. But, take for instance, the case of Facebook Beacon, in which companies collaborated with Facebook to post users' purchase history on the users' Facebook pages, a location viewable by their friends. Lane v. Facebook, Inc., 696 F.3d 811, 816 (9th Cir. 2012). The operative norms in the Facebook scenario are far from clear. Just as lawyers argue about how to define the "market" in antitrust litigation, so too would a battle over the "norm" community ensue: Is an online bookseller such as Amazon subject to bookseller norms, Internet company norms, or contract law norms? The answer is unclear under the above scenario. With respect to the grocer, conversely, sharing with a "trusted affiliate" is a norm of retail today. Also, a private grocer commodifying a stream of data through private sharing with "affiliates" is arguably akin in some ways to a public company commodifying customer data through listing it as an "intangible asset" on its balance sheet for purposes of increasing shareholder investment value. The contours of the context and the operative norms for purposes of legislating with Nissenbaum's approach perhaps become a bit vague in their operationalization in the context of commercial information sharing pursuant to a digital contract.

185. Jacqueline D. Lipton, *"We the Paparazzi": Developing a Privacy Paradigm for Digital Video*, 95 IOWA L. REV. 919, 925 (2010).

result in misinterpretation.[186] Using the example of a video of a person entering an in vitro fertilization clinic ("IVF") clinic, she highlights that several very different motivations could exist for this behavior and may result in an incorrect inference that the person is attempting to become pregnant when in reality the person is obtaining information for a friend.[187]

Laura Heymann also cogently addresses the role of context in copyright. She asserts that technology has complicated the dynamics of copyright law, arguing that an increased focus on the concept of fixation is warranted in both copyright and privacy.[188] She points to using the rights for individuals to decide how they are represented to the public as a unifying inference, and an autonomy concern in line with traditional privacy torts.[189] As such, she correctly highlights the concept of an individual's agency with respect to his or her information. However, she goes on to assert that while the issues of control at the heart of copyright law are primarily economic ones, the issues of control at the heart of privacy law are not economic in nature.[190] Here, I must respectfully disagree. The issues at the heart of consumer privacy are indeed economic. Returning to the example of the attorney en route to London, the attorney's privacy concern is driven, at least in substantial part, by the fear of losing economic opportunities and being shunned by business contacts. Just as copyright involves an artist's embedding an idea into a tangible medium in the attempt to gain legal recognition for the work and potentially profit, so too do consumers seek to embed information about themselves into an economic context, frequently for monetary reasons. Using a mundane example, the average consumer would probably perceive the act of sharing one's favorite brands with a website in order to receive weekly email coupons as an act that is primarily economically motivated.[191]

186. *Id.* at 927–28.

187. *Id.* at 928.

188. Heymann, *supra* note 37, at 831.

189. *Id.* at 837–38. In particular, Heymann notes:

> The unifying character of interference with the plaintiff's autonomy is important, for it represents not simply the right "to be let alone" but a more active interference with the plaintiff's autonomy: the right to decide for oneself how one is represented to the public. At the heart of this claim is the question of who is to exercise this control, and commentators contesting the validity of such claims criticize them on precisely this ground—that they deceitfully seek to hide information that might be relevant to others' decision making.

Id. at 837 (footnote omitted).

190. *Id.* at 837–38 ("Unlike copyright law, however, the control at the heart of privacy law is motivated by individual and spiritual concerns rather than economic ones.").

191. *See* Jason M. Solomon, *Judging Plaintiffs*, 60 VAND. L. REV. 1749, 1767 (2007) ("In the common-law privacy tort of public disclosure of private facts, a plaintiff's efforts to keep certain facts private are assessed in determining liability.").

Because the consumer privacy debate involves dynamics of selective embedding for economic self-realization, trade secret law—a body of law that enables corporate persons to selectively embed information for economic self-realization—offers an auspicious model for a contract-based approach to consumer privacy protection.

2. Lessons from Trade Secret Law

Is a consumer's control over his or her information akin to the way companies control their trade secrets? Yes, it is. Like a company with a trade secret, consumers seek to selectively share information while simultaneously maintaining a reasonable measure of protection over it. Trade secret law offers three valuable lessons for crafting a successful model of consumer privacy. First, trade secret law protects information without ascertaining whether any possible property interest exists in the information. In Part II, I argued that it is not necessary to identify the exact legal nature of the right that consumers hold in their information to be able to contractually protect it.[192] While this argument may seem unduly contractarian and legalistic, it is at the heart of trade secret law. Trade secret law is a method of intellectual property protection that is based on the concept of selective sharing using reasonable care *without* determining ex ante whether any property interest also exists in the information.[193] A trade secret involves information of a category stipulated in the coverage of a trade secret statute, which derives independent economic value from not being publicly known and having reasonable measures of protection.[194] As such, a particular intangible asset—be it a database, a client list in some states, a research project in process, or various other types of sensitive information that are not necessarily protectable under other intellectual property law regimes—can receive state level protection as a trade secret.[195]

192. *See supra* Part II.A.1.

193. *See* Bonito Boats, Inc. v. Thunder Crafts Boats, Inc., 489 U.S. 141, 155 (1989) ("[C]ertain aspects of trade secret law operated to protect *non-economic interests* outside the sphere of congressional concern in the patent laws. As the Court noted, '[A] most fundamental human right, that of privacy, is threatened when industrial espionage is condoned or is made profitable.'" (alteration in original) (emphasis added) (quoting Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 487 (1974))); 1 MELVIN F. JAGER, TRADE SECRETS LAW § 1:5 (2013) ("The fundamental human right of privacy is elevated by *Bonito* to the position of a significant additional public policy reason for the protection of trade secrets by state law.").

194. *See* 1 JAGER, *supra* note 193, § 3:2 ("The single most important requirement of the law is the obvious one that the trade secret *must in fact be secret*.").

195. The legal analysis turns on whether the holder has treated it as a secret through affirmative protective steps during the information's life. For a discussion of trade secret law and reasonable protection measures, see, for example, Elizabeth A. Rowe, *Contributory Negligence, Technology, and*

Second, trade secret law is driven by a paradigm of selective embedding and contextual control over information in order to preserve its economic value.[196] The unifying concept between both consumer privacy and trade secret is the idea of control through selective embedding: the possessor of information exercises control over the embedding of information into a trusted commercial context—the selective embedding of a "thing of value" for economic gain. The legal consumer privacy inquiry can be reframed at least in part around this type of economic autonomy interest. Specifically, to find a protectable trade secret interest, courts must retrospectively examine the level of care used by the holder throughout the life of the alleged trade secret with respect to its selective embedding.[197] Courts analyze whether the holder of the secret took reasonable affirmative steps to maintain its secrecy.[198] When consumers share data, they envision it to be part of some sort of licensing/privacy regime that is intended to provide them with similar control over the selective embedding of their information and to assure that their information is maintained with care.[199]

Third, trade secret law relies heavily on contract law to operationalize this selective embedding of corporate information.[200] Contracts, specifically nondisclosure and confidentiality agreements, are the dominant legal tools trade secret owners point to as an example of care in their treatment of secret information.[201] Confidentiality agreements grant the trade secret holder the ability to selectively disclose information to "trusted" parties. Pursuant to the terms of an agreement, the receiving party

Trade Secrets, 17 GEO. MASON L. REV. 1, 5–13 (2009).

196. *See id.* at 5 ("A trade secret can be any information of value used in one's business that has been kept secret and provides an economic advantage over competitors.").

197. For a discussion of trade secret basics, see, for example, 1 JAGER, *supra* note 193, §§ 3:1–2.

198. *Id.* § 3:2 (stating that one of the six factors to be considered in determining whether a trade secret exists is "the extent of measures taken by [the holder] to guard the secrecy of the information" (internal quotation marks omitted)).

199. *See* Cecilia Kang, *Google Announces Privacy Changes Across Products; Users Can't Opt Out*, WASH. POST (Jan. 24, 2012), http://articles.washingtonpost.com/2012-01-24/business/35440035_1_google-web-sites-privacy-policies (quoting a privacy advocate as stating that "[t]here is no way a user can comprehend the implication of Google collecting across platforms for information about your health, political opinions and financial concerns").

200. In particular, by negotiating a confidentiality agreement, a holder of information seeks to "to maintain the economic or competitive value of its information by reducing the risk that [a] recipient will use the information to its own advantage, or to the disadvantage of the provider." Margaret Lewis Meister & Daniel M. Alsup, *Confidentiality Agreements and Due Diligence*, ROCKY MTN. MIN. L. FOUND., no. 3, 2010. Moreover, "[a]n agreement between private parties can work to safeguard confidential and proprietary information from disclosure by the parties to the agreement" and could therefore protect the information's status as a trade secret. *Id.* at 3.

201. *Id.* (discussing the purpose and importance of confidentiality agreements); 1 JAGER, *supra* note 193, § 5:21 (same).

agrees to exercise care in data handling in exchange for access to the information.[202] It is precisely this type of contract approach to selective embedding that can also work in the consumer privacy context.

When we analyze consumer privacy through the lens of trade secret law, we can reconceptualize terms and conditions of use and privacy policies as contracts intended to operationalize selective embedding of valuable information. However, the key difference between the trade secret context and the consumer privacy context turns on which party is permitted to stipulate the terms of sharing: in the trade secret context, the holder of the information dictates the terms of the information sharing from the outset. This information dynamic is backwards in the consumer privacy context.

In consumer privacy contexts, commercially reasonable negotiated measures of information care and security are absent. Due to their non-negotiability, terms of use and privacy policies reflect an imbalance in favor of the drafter—the data aggregator—whose interests are not aligned with those of the consumer.[203] In other words, consumers cannot counteroffer to terms of use and privacy policies by saying, "I will share my data with your website, but only if you promise to take care of my information and encrypt it in storage." Yet, that is precisely the type of dickering that would occur in a trade secret sharing situation: a company would include reasonable measures of information protection in the confidentiality agreement.[204] As such, terms and conditions of use and privacy policies should be analyzed as the unnegotiated first draft of a confidentiality agreement, in which the core language necessary to protect the confidentiality of the secret information has not yet been included. For these reasons, trade secret law offers a viable model for a contract law regime to protect consumer privacy. By modeling how companies protect their most secret information using contracts in trade secret law, a consumer privacy approach can be crafted through implied contractual promises. Especially because data aggregators' future uses and care for information are unforeseeable, a safety net of implied promises offering consumers contextual control is a necessary solution. The next part offers eight doctrinal and statutory sets of implied promises—a "reasonable data

202. Meister & Alsup, *supra* note 200.

203. *See* 11 WILLISTON, *supra* note 25, § 32:12 (noting that ambiguities are resolved in favor of the nondrafting party since language is within the control of the drafting party).

204. *See* Meister & Alsup, *supra* note 200 ("The tension between the interests of the provider and the interests of the recipient influence the form the confidentiality agreement ultimately takes. Most of the duties in a confidentiality agreement burden the recipient of information.").

stewardship" approach modeled on the types of typical data-care promises visible in corporate confidentiality agreements in trade secret contexts.[205]

IV. THE REASONABLE DATA STEWARDSHIP MODEL OF CONSUMER PRIVACY AND INFORMATION SECURITY

When reasons of public policy dictate, courts have a duty to reappraise old doctrines in the light of the facts and values of contemporary life—particularly old common law doctrines which the courts themselves created and developed.

—Echo Consulting Services, Inc. v. North Conway Bank[206]

Historically, contract law has been concerned with restoring balance in situations when one party is disadvantaged due to different levels of sophistication and expertise.[207] As Part III explained, one key vehicle used by contract law to accomplish this rebalancing has been the use of consumer protective implied terms.[208] In this part, I propose an operationalization of a contract theory of consumer privacy using implied promises—a model of "reasonable data stewardship" that is inspired by trade secret law.[209]

205. Since the early days of databases, contracts have been the dominant governance structures in technology-mediated spaces. As I have demonstrated elsewhere with empirical evidence, end user license agreements, terms and conditions of use, and privacy policies have become more draconian and restrictive across time. Matwyshyn, *supra* note 16, at 79–82. This result has presumably arisen in part from the lack of negotiability of these agreements. *Id.* at 80–81. This is a typical form contracting concern echoed in other areas of contract law. *See* 2 WILLISTON, *supra* note 25, § 6:18 (analyzing acceptance of one-sided offers). However, as I have argued elsewhere, this concern is exacerbated in technology contexts. Andrea M. Matwyshyn, *The Law of the Zebra*, 28 BERKELEY TECH. L.J. 155, 160 (2013) [hereinafter Matwyshyn, *The Law of the Zebra*]. I have also argued that the comprehensibility of information licenses is poor for an average consumer and court-imposed reasonableness standards would ensure greater fairness in information contracting. Matwyshyn, *supra* note 27, at 532. Specifically, I advocated that these standards be constructed based on empirical testing of consumer understanding in a manner modeled on trademark consumer confusion inquiries. *Id.* at 531–34.

206. Echo Consulting Servs., Inc. v. N. Conway Bank, 669 A.2d 227, 232 (N.H. 1995) (alterations and internal quotation marks omitted); 15 WILLISTON, *supra* note 25, § 48:10.

207. Rules of contract, for example, differ between merchants and consumers. For a discussion of different parties' status in contract, see, for example, U.C.C. § 2-207 (2011–2012) (articulating different rules when the transaction is between two merchants or between a merchant and consumer).

208. Much like Bourdieu, contract law has also struggled with the dichotomies of objectivity versus subjectivity and agency versus structure. Contract formation questions have pushed courts to temper objective analysis with a recognition of the subjective perception of individual parties. Meanwhile, contract enforcement questions have asked courts to balance the agency of the individual within the constraints of broader social organization.

209. The principles of the reasonable data stewardship model align with the seven consumer privacy rights articulated by the White House in its Consumer Privacy Bill of Rights: individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability. WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR

The "reasonable data stewardship" model applies the insights of trade secret law from Part III to the traditional contract doctrines of consideration,[210] contra proferentem,[211] and good faith in performance.[212] Further, it challenges the assumption that blanket deference to the drafter in consumer information privacy contracts is optimal.[213] The reasonable data stewardship model also borrows an idea from another contract context with information imbalances—real estate leasing and landlord tenant law[214]—to propose a new statutorily implied warranty of "digital usability and quiet enjoyment." Finally, the model borrows the copyright concept of optional statutory damages and trade secret punitive damages to bridge two remaining gaps in consumer privacy. Broadly, the "reasonable data stewardship" model proposed here asks courts and legislatures to examine consumer privacy contract formation problems in light of changed technological reality and the need for reasonable care in information security.

The reasonable data stewardship model is composed of the following eight doctrinal or statutory shifts in contract law:

1. Doctrinally acknowledging that data transfers constitute legally sufficient consideration.
2. Doctrinally treating a data breach notice as presumptive evidence of a breach of contract by the data aggregator.
3. Doctrinally reviving contra proferentem.
4. Doctrinally or statutorily extending the duty of good faith in performance to include information handling.
5. Doctrinally or statutorily creating an implied warranty of digital usability and quiet enjoyment.
6. Doctrinally or statutorily deeming any data-handling change to constitute a request for amendment requiring affirmative consent and potentially additional consideration.
7. Doctrinally or statutorily creating meaningful termination

PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 1 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

210. *See supra* Part II.

211. *See infra* text accompanying note 228.

212. *See infra* text accompanying note 238.

213. A successful contract-based consumer privacy approach must honor traditional contract theory concerns about consumer protection and imbalanced bargaining power. As such, the reasonable-data-stewardship approach incorporates a new set of consumer-protective implied terms.

214. *See supra* Part III.

rights.

8. Doctrinally or statutorily creating minimum statutory damages for data loss modeled on intellectually property damages.

These implied promises reflect the types of reasonable data stewardship obligations consumers would negotiate into their data sharing agreements if they were able to do so. These terms also mirror the types of provisions trade-secret holders negotiate into their confidentiality agreements when selectively embedding secret corporate information. By crafting a set of nonwaivable, implied terms, courts and legislatures would assist consumers in selectively embedding their information into commercial contexts, and thus ensure reasonable consumer privacy protection.[215]

A. PROPOSAL 1: ACKNOWLEDGING THAT DATA TRANSFERS CONSTITUTE LEGALLY SUFFICIENT CONSIDERATION

Although Part II established that access to consumer information constitutes legally sufficient consideration, courts have been slow to explicitly recognize it as such.[216] This recognition provides an important initial piece toward crafting a set of data stewardship obligations in contract. Specifically, from the consumer's perspective—but not necessarily from the aggregator's—any privacy or information security promises made to the consumer anywhere on the website, regardless of whether these promises are expressly reiterated in the user agreement, constitute material promises that induce the data sharing. Therefore, when consumers give access to their information—a "thing of value"—it is reciprocally, conventionally induced by the aggregator's promises of privacy and information security.

Indeed, this consumer perception is in line with the spirit of traditional

215. Similar to the way that almost all state legislatures have adopted versions of the Uniform Trade Secrets Act, so too states can adopt versions of a so-called "Uniform Consumer Privacy Act," which would include the statutory provisions suggested in Part IV. As such, the Uniform Law Commission should undertake drafting model legislation of this sort to assist states in this enterprise. For a discussion of the Uniform Trade Secrets Act, see generally Sharon K. Sandeen, *The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act*, 33 HAMLINE L. REV. 493 (2010); Elizabeth A. Rowe, *Trade Secret Litigation and Free Speech: Is It Time to Restrain the Plaintiffs?*, 50 B.C. L. REV. 1425 (2009).

216. *See* Jerry Kang et al., *Self-Surveillance Privacy*, 97 IOWA L. REV. 809, 846 (2012) ("[D]amages due to breach of privacy terms are more properly considered emotional or psychic losses, forms of harm that courts generally do not recognize as contractual damages unless the contract or the breach is of such a kind that serious emotional disturbance was a particularly likely result." (quoting RESTATEMENT (SECOND) OF CONTRACTS § 353) (internal quotation marks omitted)).

contractual interpretation. As Williston articulates,

> [A]bsent anything to indicate a contrary intention, written instruments executed at the same time, by the same contracting parties, for the same purpose, and in the course of the same transaction will be considered and construed together as one contract or instrument, even though they do not by their terms refer to each other. . . . Likewise, when the execution of one contract depends on the execution of other contracts, the contracts must be construed together . . . .[217]

In other words, whatever the data aggregator offers as terms of exchange, including privacy policy terms and representations about information security made anywhere on the website—whether in words or in code—should be analyzed as together constituting the full and complete understanding of the parties on issues of privacy and information security.[218] Thus, a breach of any of these obligations constitutes a breach of the contract made with the consumer. In particular, a data breach should presumptively be considered a breach of the promises of data stewardship that induced the consumer's data sharing.

B. PROPOSAL 2: TREATING A DATA BREACH AS PRESUMPTIVE EVIDENCE THAT AGGREGATORS HAVE BREACHED A CONTRACT

Courts should construe the existence of a data breach, indicated by, for example, a data breach notification, as preliminary evidence of a possible breach of material implied and express promises of data stewardship. However, because information security breaches can occur despite the highest degree of care, this presumption can be rebutted: proof that the data aggregator used reasonable care in data handling and breach mitigation should be recognized as an affirmative defense or mitigating factor. In this way, the legal burden shifts, as the data aggregator is put in the position of refuting the presumption of breach through a demonstration of reasonable care in information handling.[219] In the event of a minor breach, the nonbreaching party can still receive a substantial benefit from the bargain and therefore hold fewer recourse rights.[220] Courts should construe the

217. 11 WILLISTON, *supra* note 25, § 30:26 (footnotes omitted).

218. For a discussion of incorporating website design as part of contract promises, see Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1650–55 (2011).

219. Contract law has constructed two types of breaches with varying consequences: material breaches and minor breaches. 23 WILLISTON, *supra* note 25, § 63:3. A material breach occurs when the nonbreaching party cannot receive the substantial benefit of the bargain. *Id.* Consequently, the nonbreaching party can terminate performance while maintaining the right to all remedies available at law or in equity. *Id.*

220. The determination of whether a breach is material or minor is generally a question of fact. *Id.* Using a blended, sliding-scale approach, courts tend to look at five types of factors to determine

existence of a data breach as preliminary evidence that the aggregator has breached contractual promises of privacy and data care to consumers.[221] For example, a material breach might be demonstrated by the mailing of legally required, data-breach notifications.[222] This idea is also borrowed from trade secret law, in which information holders preserve secrecy so long as they offer proof of reasonable care. If a breach results from an unforeseeable event, such as a hacker using a "zero day" exploit about which the entity was not informed,[223] the information holder is less blameworthy for the loss of secrecy. However, if the loss of secrecy resulted from obvious neglect and lack of care in the holding of the data or a failure to patch systems known to have vulnerabilities,[224] the holder has materially breached the agreement and contract remedies are appropriate. In this way, a rebuttable presumption that information security and privacy breaches are material potentially gives rise to a right to contract damages for harmed consumers.

By requiring data aggregators to demonstrate that they undertook reasonable data stewardship measures to protect consumer information, the

whether a breach is material. First, courts assess the extent to which the nonbreaching party will be deprived of the benefit it reasonably expected—the greater the benefit already received, the less material the breach. *Id.* Second, courts look to the adequacy of damages—if monetary damages are indeed effective to compensate for injury, the breach is deemed less material. *Id.* In this way, contract law recognizes that the worst types of breaches are those that money cannot heal, a paradigm well suited to a privacy inquiry. Third, courts assess the likelihood that the breaching party will cure its failure—the greater the likelihood of cure, the less material the breach. *Id.* Fourth, courts assess the extent to which the parties' behavior complied with the standards of good faith and fair dealing. *Id.* Finally, courts assess the hardship imposed on the breaching party if it performs its remaining obligations. *See id.* The lesser the hardship, the more likely a breach is material. *See id.*

221. A privacy breach tends to be a material breach because damages cannot fully make a plaintiff whole. *See id.*

222. For a discussion of state data breach notification requirements, see Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 275–76, 292–94 (2011).

223. A "zero day" or "0day" exploit is a method of capitalizing on a security problem that had previously been unknown to the information security community at-large. *See* Ryan Naraine, *Teenager Hacks Google Chrome with Three 0day Vulnerabilities*, ZDNET (Mar. 9, 2012), http://www.zdnet.com/blog/security/teenager-hacks-google-chrome-with-three-0day-vulnerabilities/10649 (reporting a teenage hacker's victory in a Google-sponsored competition to locate weaknesses in the Google Chrome browser).

224. Some data breaches are easily determined by information security experts to constitute a severe lack of care in data storage and a failure to update systems. *See* Agreement Containing Consent Order, *In re* TJX Companies, Inc., F.T.C. No. 0723055, *available at* http://www.ftc.gov/os/caselist/0723055/080327agreement.pdf (ordering clothing retailer to build comprehensive data-security programs as a result of having about 50 million credit and debit card numbers stolen from its databases); Jaikumar Vijayan, *TJX Data Breach: At 45.6M Card Numbers, It's the Biggest Ever*, COMPUTERWORLD (Mar. 29, 2007, 12:00 PM), http://www.computerworld.com/s/article/9014782/TJX_data_breach_At_45.6M_card_numbers_it_s_the_biggest_ever?pageNumber=1.

court shifts the burden of proof from the potentially harmed consumer to the data aggregator—the party with better information about the breach.[225] This doctrinal shift, which creates the rebuttable presumption that data breaches are material contract breaches,[226] would immediately encourage data aggregators to improve privacy and information security practices. Each time data aggregators experience a data breach, they risk a court deciding that a material contract breach has occurred for all similarly situated consumers under the same user agreement.[227] Since the same terms of use agreement and privacy policy apply to all users, the relevant class of plaintiffs could include all of the company's customers. However, ongoing responsible data stewardship and speedy corrective responses to data leakages by the data aggregator can preserve consumer relationships and perhaps avoid additional litigation. A new type of balance would result in increased incentives for reasonable care in information handling and data stewardship.

C. PROPOSAL 3: REVIVING CONTRA PROFERENTEM

Contra proferentem, or construction of a contract against the drafter, is a firmly-rooted doctrine in contract law that attempts to correct a potential power imbalance between the party selecting contractual language and the party acceding to it.[228] In particular, when one side has not been offered the

225. Much like a situation in which a secret corporate database is copied without permission and disseminated, a data breach copies and disseminates a consumer's information. As such, this type of act constitutes a breach of the privacy policy and user agreement, including an "implied warranty of digital quiet enjoyment," which will be proposed in the following sections.

226. Although this approach may seem unorthodox, it is akin to the mechanism that contract law uses to determine the severity of a breach. The legal burden of proving the severity of a breach is at least shared by the defendant in a contract law determination. As such, the rebuttable presumption puts the data aggregator in the position in which it must demonstrate that it exercised reasonable care in handling information.

227. The danger of form contracts is that the efficiency created on the transactional side is mirrored on the litigation side in instances of breach. Indeed, some scholars advocate that consumers use their own set of standard forms when contracting with data aggregators. *See* Clayton P. Gillette, *Rolling Contracts as an Agency Problem*, 2004 WIS. L. REV. 679, 720–21 (arguing that "buyers could present governmentally generated standard forms to sellers, just as sellers now present them to buyers" or "simply use the forms to make comparisons with terms offered by sellers").

228. 11 WILLISTON, *supra* note 25, § 32:12. Courts interpret contracts in accordance with six general rules of construction. First, they construe contracts as a whole. *Id.* § 32:5. As Proposal 1 explained, the whole contract in the case of a digital agreement involves deeming privacy promises and terms that benefit a data aggregator as contingent upon each other. Second, as discussed above, courts prefer to construe a contract as a valid and enforceable set of mutually reinforcing obligations. *See* 17A AM. JUR. 2D *Contracts* § 715 (2d ed. 2004) (discussing when a party may continue performance after breach). Third, according to the doctrine of contra proferentem, ambiguities in drafting are to be construed against the drafter. 11 WILLISTON, *supra* note 25, § 32:12. Ambiguity refers to the situation in which a small number of discrete meanings are possible for a term and the contract sheds no light on

ability to participate in the negotiation or drafting of an agreement, as is the case in the consumer privacy context, this norm serves to rebalance a situation with unequal bargaining power between the parties. Yet, courts to date have been hesitant to apply the doctrine in privacy and information security contexts.

A contract drafter is generally perceived to possess an advantage. When a severe information imbalance exists between data aggregators and consumers with respect to how the aggregator handles and cares for data, contracts are potentially more susceptible to ambiguity,[229] fraud or misrepresentation,[230] and intentional nondisclosure.[231] As such, if only one side is aware of an ambiguity, a contract will be enforced according to the intention of the party unaware of the ambiguity using a subjective consent analysis.[232] Hence, despite a dominance of objective contractual interpretation, courts look to a subjective test of intent in situations leveraging power imbalances.[233] In line with these doctrinal approaches, in consumer privacy disputes that arise from drafting problems in a privacy policy or terms of use agreement, either a consumer's subjective privacy expectations or those of a "reasonable digital consumer" should control.[234]

intent as to which meaning. *See, e.g.*, Frigaliment Importing Co. v. B.N.S. Int'l Sales Corp., 190 F. Supp. 116, 117 (S.D.N.Y. 1960) (discussing several interpretations of a purchase order for "chicken"). Additionally, the ordinary meanings of words are presumed unless the words are explicitly otherwise defined. 11 WILLISTON, *supra* note 25, § 32:3. In the case of an inconsistency of provisions, if some terms are form contract terms and some not, the terms that are negotiated prevail. *Id.* § 32:13. Finally, courts look to custom and usage of terms generally and in particular industries. *Id.* § 32:4.

229. For a discussion of statutory ambiguity, see generally Ward Farnsworth, Dustin F. Guzior & Anup Malani, *Ambiguity About Ambiguity: An Empirical Inquiry into Legal Interpretation*, 2 J. LEGAL ANALYSIS 257 (2010).

230. For a discussion of fraud and contract, see Norwood P. Beveridge, *Interested Director Contracts at Common Law: Validation Under the Doctrine of Constructive Fraud*, 33 LOY. L.A. L. REV. 97, 101–04 (1999).

231. For a discussion on nondisclosure, see generally Christopher T. Wonnell, *The Structure of a General Theory of Nondisclosure*, 41 CASE W. RES. L. REV. 329 (1991).

232. In circumstances in which a court finds that one party has engaged in fraud or material misinformation for its own benefit, the other party's subjective perceptions of the terms tend to win, and the contract is frequently deemed voidable at the discretion of the misinformed party.

233. If an ambiguity arises out of the contract and both parties are on equal footing, there is no contract unless both parties interpret the ambiguity the same way. *See* RESTATEMENT (SECOND) OF CONTRACTS § 201 (1981). Sophisticated parties usually include a boilerplate provision which stipulates that provisions should not be construed against the drafter. But in a business-to-consumer transaction governed by a take-it-or-leave-it agreement which carries hallmarks of possible unfair surprise or oppression, courts should be willing to construe provisions against the sophisticated party in favor of the consumer. This invocation has sometimes been predicated on the possibility of a violation of the doctrine of good faith and fair dealing implicit in the agreement.

234. I have argued elsewhere in favor of a reasonable digital consumer standard empirically constructed through testing modeled on trademark law confusion inquiries. *See supra* note 205 and accompanying text.

In other words, the contract should be construed against the drafter.

D. PROPOSAL 4: EXTENDING THE DUTY OF GOOD FAITH IN PERFORMANCE TO INCLUDE INFORMATION HANDLING

The traditional contract doctrine of good faith in performance can be interpreted to encompass reasonable data stewardship and a duty to engage in sound information-handling practices. The general thrust of the duty of good faith in performance is the imposition of an affirmative duty of reasonableness in commercial conduct. Therefore, if a company chooses to engage in data aggregation as part of its commercial enterprise, it assumes a duty of data stewardship.

Courts have recognized that every contract imposes the duty of good faith and fair dealing to protect the parties' reasonable expectations.[235] This approach serves to legally solidify the idea that rules of exchange should reflect reasonable business conduct. Extending the duty of good faith and fair dealing into data stewardship obligations is perhaps particularly well suited to cases in which no adequate consumer remedy exists at law.[236] To wit, incorporating an expanded duty of good faith into the terms of use and privacy policies would in essence impose an affirmative duty of reasonable care on data aggregators.[237] Consequently, a data aggregator who accesses

235. Although application of the doctrine varies by jurisdiction, numerous courts have found that each contract contains an implied duty of good faith and fair dealing in performance and enforcement. *E.g.*, Sanders v. FedEx Ground Package Sys., Inc., 188 P.3d 1200, 1203 (N.M. 2008) ("New Mexico courts have held that every contract imposes a duty of good faith and fair dealing on the parties with respect to the performance and enforcement of the terms of the contract."). *See also* Steven J. Burton, *Breach of Contract and the Common Law Duty to Perform in Good Faith*, 94 HARV. L. REV. 369, 369 (1980) ("A majority of American jurisdictions, the Restatement (Second) of Contracts, and the Uniform Commercial Code (U.C.C.) now recognize the duty to perform a contract in good faith as a general principle of contract law." (footnotes omitted)); Clayton P. Gillette, *Limitations on the Obligation of Good Faith*, 1981 DUKE L.J. 619, 626–30, 632, 642–43, 649–50 (arguing that an expansive interpretation of the good faith obligation does not produce commercial benefits, creates unpredictability, and violates the bargained-for risk allocation); Robert S. Summers, *The General Duty of Good Faith—Its Recognition and Conceptualization*, 67 CORNELL L. REV. 810, 812 (1982) ("By the late 1960s, . . . the accumulation of case law imposing a duty of contractual good faith outside contexts of 'good-faith purchase' was considerable.").

236. *See* Leder v. Shinfeld, 609 F. Supp. 2d 386, 400–01 (E.D. Pa. 2009) (citing Parkway Garage, Inc. v. City of Phila., 5 F.3d 685, 700–02 (3d Cir. 1993)) (holding that Pennsylvania law does not permit causes of action for breach of good faith when there already exists adequate legal remedies for the breach).

237. For example, class actions alleging breach of the duty of good faith and fair dealing have survived motions to dismiss when the plaintiffs have alleged overcharging for services included within the terms of the contract at issue. In *Payday Advance Plus, Inc. v. FindWhat.com, Inc*., an advertising customer brought a putative class action against a search engine operator for breach of contract, alleging that the operator violated the covenant of good faith and fair dealing implicit in all agreements. Payday Advance Plus, Inc. v. Findwhat.com, Inc., 478 F. Supp. 2d 496, 499, 503 (S.D.N.Y. 2007). The

consumer data but fails to secure it properly against foreseeable harms would fail to act in a commercially reasonable manner consistent with this expanded good faith and fair dealing.[238]

Bad faith in performance can appear in many forms, whether overt or in the form of inaction, subterfuges, or evasions.[239] In cases in which a defendant has not informed a plaintiff of a substantial risk, courts have found that the defendant may have violated its duty of good faith and fair dealing, even in instances in which a contract specifically addresses the subject matter of the risk.[240] The covenant of good faith and fair dealing

Payday court denied the defendant's motion to dismiss the claim, holding that, based on the alleged facts, the defendant may indeed have violated the implied covenant of good faith and fair dealing when it inflated the bidding prices for search terms and directed an advertising provider to generate gratuitous clicks on the plaintiff's website. *Id.* at 504. In particular, the *Payday* court found that because the alleged actions would have conferred a benefit to the defendant but not the plaintiff, the plaintiff may have been injured under the contract. *Id. See also, e.g.*, Trevino v. Merscorp, Inc., 583 F. Supp. 2d 521, 534 (D. Del. 2008) (permitting plaintiffs' breach of duty of good faith and fair dealing claim when a mortgagee overcharged for services included in the mortgage).

Courts have generally rescinded contracts when defendants have breached the duty of good faith and fair dealing by failing to observe a common purpose consistent with a plaintiff's justified expectations. For example, one court found that if a real estate transaction is contingent upon a special permit, a purchaser's failure to obtain the permit may constitute a breach of the duty of good faith and fair dealing, even if the contract did not explicitly require the purchaser to do so. JCV 671, LLC v. MMA Mgmt., LLC, 579 F. Supp. 2d 909, 912 (N.D. Ohio 2008). Even with at-will employment contracts, some courts have denied motions for summary judgment on grounds that an employer may have breached the implied covenant of good faith and fair dealing. *See* Willard v. Khotol Servs. Corp., 171 P.3d 108, 113–14, 123 (Alaska 2007) ("[T]he covenant of good faith and fair dealing . . . is implied in all employment contracts in Alaska."). Similarly, courts have found that a genuine issue of material fact exists as to whether a defendant violates the duty of good faith when its actions have obstructed a plaintiff's ability to mitigate losses from a deal. *See* Mem'l Hosp. of Laramie Cnty. v. Healthcare Realty Trust Inc., 509 F.3d 1225, 1236–37 (10th Cir. 2007) (denying landlord's summary judgment against hospital's claim of breach of good faith duty when the hospital alleged that landlord concealed its building's unprofitability by nondisclosure and misrepresentations).

238. Some states offer separate recovery under bad faith statutes, which derive primarily from tort law, and the duty of good faith and fair dealing implicit in every contract. *See* Ash v. Cont'l Ins. Co., 932 A.2d 877, 883–85 (Pa. 2007) (discussing the existence of separate causes of action under a bad faith insurance statute and the common law cause of action for breach of the contractual duty of good faith). Although courts have sometimes disagreed over the applicability of the duty of good faith and fair dealing, they generally distinguish the duty from recovery in tort. *Id.* at 883 n.2. Hence, tort and contract recovery are both available.

239. 2 RESTATEMENT (SECOND) OF CONTRACTS § 205 cmt. d ("Subterfuges and evasions violate the obligation of good faith in performance even though the actor believes his conduct to be justified."). *See also* N. Star Alaska Hous. Corp. v. United States, 76 Fed. Cl. 158, 193 (2007) ("Bad faith may also be exhibited by conduct—both that which explicitly violates the contract and that which simply violates the covenant of good faith and fair dealing.").

240. *See* Scott Timber, Inc. v. United States, 86 Fed. Cl. 102, 112–13 (2009) (holding that suspension clause in timber sales contract did not relieve parties' duties to cooperate and not to hinder performance mandated by the covenant of good faith and fair dealing), *rev'd on other grounds*, 692 F.3d 1365 (Fed. Cir. 2012).

can even supersede explicit contractual language that would otherwise limit a plaintiff's recovery.[241] Courts have reasoned that, as a matter of public policy, a party should not benefit from a bargain it performed in bad faith and, consequently, that the covenant of good faith and fair dealing prevails despite carve-outs existing in a particular agreement.[242] Courts have also looked to the totality of the circumstances to determine whether a defendant acted disingenuously in interpreting its obligations under an existing contract.[243] In other words, expanding or interpreting the duty of good faith in performance to include implied promises of data stewardship offers a logical extension. Companies that choose to update systems only sporadically or fail to patch widely known vulnerabilities, for example, would run afoul of this expanded duty of good faith in performance that includes data stewardship and expose themselves to potential suit.

E. PROPOSAL 5: CREATING AN IMPLIED WARRANTY OF DIGITAL USABILITY AND QUIET ENJOYMENT

As I have argued elsewhere,[244] digital spaces and products may harbor hidden flaws or dangers known to the author of the code, but not to consumers. I have advocated for extending to digital products a notice-based duty to warn, protect, and repair, borrowing from the duties owed to licensees that visit land.[245] Now, borrowing from a different limited-use context—real estate leasing and landlord-tenant law, I argue in favor of incorporating the implied warranties of habitability and quiet enjoyment into the consumer privacy context. The agreements formed in terms of use and privacy policies reflect many of the same negotiability, unfair surprise, and oppression concerns present in landlord-tenant situations. These

241. *See* Airfreight Express Ltd. v. Evergreen Air Ctr., Inc., 158 P.3d 232, 239–42 (Ariz. Ct. App. 2007) (holding that, while a party could contract to limit liability in damages for nonperformance of promises, such a provision cannot be enforced when that party acted fraudulently or in bad faith).

242. *Id.*

243. *E.g.*, Century Packing Corp. v. Giffin Specialty Equip. Co., 438 F. Supp. 2d 16, 27 (D.P.R. 2006) ("[T]he true intention of the parties and the spirit or purpose permeating over the [contract] . . . may be inferred from the concurrent circumstances and the total behavior of the interested parties."). For example, landlords who fail to reasonably cooperate with their tenants may be sued for breaching the implied duty of good faith and fair dealing. *See* Speedway SuperAmerica, LLC v. Tropic Enters., Inc., 966 So. 2d 1, 4 (Fla. Dist. Ct. App. 2007) (requiring landlord to act in a commercially reasonable manner even though lease agreement gave it substantial discretion over tenant's assignment); Century Partners, LP v. Lesser Goldsmith Enters., Ltd., 958 A.2d 627, 633–35 (Vt. 2008) (holding that landlord breached duty of good faith and fair dealing by arbitrarily refusing to discuss tenant's plans for expansions when landlord knew that tenant leased property for the sole purpose of expansion).

244. Andrea M. Matwyshyn, *Hidden Engines of Destruction: The Reasonable Expectation of Code Safety and the Duty to Warn in Digital Products*, 62 FLA. L. REV. 109, 111–14 (2010).

245. *Id.* at 136–37.

concerns about unequal bargaining power and inability for meaningful tenant recourse caused states and municipalities to incorporate statutory protections into real estate leases.[246] As such, applying this idea to privacy, one viable approach to addressing consumer privacy may be by doctrinally or statutorily crafting a nonwaivable[247] implied warranty of "digital usability and quiet enjoyment."

Specifically, landlords breach the warranty of habitability or constructively evict tenants whenever they fail to furnish basic living space necessities such as "heat, light, power, water, an adequate cooling or heating system, satisfactory plumbing and sewage disposal."[248] In addition to ensuring these utilities, landlords must make more than a "token effort" to exterminate vermin or insects and, in some circumstances, protect tenants from "criminal acts, such as burglary or assault."[249] In other words, the implied warranty requires landlords to provide every residential lease and some commercial leases the basic necessities related to living or operating in the leased space.[250] For contracts in digital spaces, promises of data stewardship are equivalent to real world promises of necessities such as those described above. Indeed, we can draw a very direct parallel in the information security context that is consistent with the spirit of the habitability protections: consumers engaging in a commercial exchange with a data aggregator should be protected from "vermin" such as malware and technology-driven "criminal acts."

246. New York, for example, has deemed that residential tenants cannot waive their rights to the implied warranty of habitability. Morris v. Flaig, 511 F. Supp. 2d 282, 297 (E.D.N.Y. 2007). *See also* Contex Homes v. Buecher, 95 S.W.3d 266, 274 (Tex. 2002) ("[T]he warranty of habitability can be waived only to the extent that defects are adequately disclosed. Thus only in unique circumstances, such as when a purchaser buys a problem house with express and full knowledge of the defects that affect its habitability, should a waiver of this warranty be recognized.").

247. As Williston explains,

> The widespread promulgation of state legislation governing, to one degree or another, residential leases, including statutes broadly imposing an implied warranty of habitability in such leases, has to a great extent modified and undercut the harshness of the common-law rule as applied to the typical residential lease. Moreover, in many jurisdictions, the courts, either following the lead of their legislatures or moving independently, have judicially declared the existence of an implied warranty of habitability, thereby making the landlord responsible to repair or maintain premises, before the inception of the landlord-tenant relationship, during its continuance or both.

15 WILLISTON, *supra* note 25, § 48:11 (footnote omitted).

Williston also points out that where courts expanded the implied warranty of habitability, "the legislature had signaled its concurrence that landlords ought to respond quickly to correct substandard residential housing by its passage of [another] statute" and "judicial imposition of the implied warranty was completely consistent with and complementary to the legislative goals embodied in that act." *Id.*

248. *Id.* (footnotes omitted).

249. *Id.*

250. *Id.*

Remedies under such an implied warranty of digital usability could arise not only in contract, but also in tort depending on how states operationalize the claim.[251] Punitive damages might also be possible.[252] Courts may frame the implied warranty in some cases as the enforcement of a broader public interest in information security, in much the same way that some courts have framed a public interest in safe housing.[253]

Meanwhile, in the context of landlord-tenant contracts, the implied warranty of quiet enjoyment refers to the landlord's affirmative obligation to prevent the tenant from being deprived of use of the leased premises for their intended purpose.[254] Accordingly, to "state a claim for a breach of quiet enjoyment, the severity of interference must be such that the premises become unfit for the purpose for which they were leased."[255] This pleading requirement is rooted in the notion that when a leased property is unfit for its intended purpose, consideration for the lease is impaired.[256]

The interference does not need to arise from a landlord's intentional act, and courts generally adopt the perspective of the tenant when deciding whether a loss of use has happened.[257] If a tenant is deprived of this use, a constructive eviction has occurred.[258] As Williston describes the implied warranty of quiet enjoyment:

> It is well established that the landlord's conduct, and not his intentions, is controlling. . . . [E]ven though no intent was or could have been found, courts have found a constructive eviction where a nuisance outside the leased premises . . . was attributable to, though not affirmatively undertaken by, the landlord. . . .
>
> . . . [E]ven without any affirmative activity on the landlord's part, courts have found a constructive eviction where the landlord fails to perform a lease covenant, fails to perform statutory obligations, or fails to perform a duty that is implied from the circumstances.[259]

251. Mississippi law, for example, entitles tenants to pursue both contract and tort remedies for a landlord's breach of the implied warranty of habitability. Moorman v. Tower Mgmt. Co., 451 F. Supp. 2d 846, 850 (S.D. Miss. 2006).

252. Some states, such as New York, allow punitive damages for breaches of the implied warranty of habitability when the landlord's behavior was particularly egregious. *E.g.*, Morris v. Flaig, 511 F. Supp. 2d 282, 296 (citing N.Y. REAL PROP. LAW § 235-b (McKinney)) (reasoning that punitive damages are available because they "enforce important *public* rights to safe and appropriate housing").

253. *Id.*

254. 15 WILLISTON, *supra* note 25, § 48:10.

255. *Id.* (quoting Winrock Inn Co. v. Prudential Ins. Co. of Am., 928 P.2d 947, 570 (N.M. Ct. App. 1996)) (internal quotation marks omitted).

256. 49 AM. JUR. 2D *Landlord and Tenant* § 630 (2006).

257. 15 WILLISTON, *supra* note 25, § 48:10.

258. *Id.*

259. *Id.* (third ellipses in original) (internal quotation marks omitted).

Courts and legislatures can adapt this concept of deprivation of use in an intended manner to the context of the safe use of digital "premises." When consumers grant access to information pursuant to the terms of use and privacy policy, they should be able to quietly enjoy the digital spaces to which they have purchased access in reasonable safety. State courts' or legislatures' incorporation of an implied warranty of digital usability and quiet enjoyment would also be entirely consistent with and complementary to the legislative goals of state data breach notification statutes.[260] In other words, courts could hold that data aggregators deprive consumers of use and quiet enjoyment of digital "premises" whenever they fail to adequately ensure good information security practices and perform the privacy promises made to consumers. Through a statutory or doctrinal implied warranty of digital usability and quiet enjoyment, consumers gain a basis to sue for breach of contract when data stewardship failures arise.

F. PROPOSAL 6: DEEMING ANY DATA HANDLING CHANGE AS CONSTITUTING A REQUEST FOR AMENDMENT REQUIRING AFFIRMATIVE CONSENT AND, POTENTIALLY, ADDITIONAL CONSIDERATION

Due to the lack of negotiability of digital agreements, privacy and terms of use agreements have evolved to look very different in substance from negotiated agreements relating to similar subject matter between equally situated merchant-bargaining parties. Yet, in the spirit of the Uniform Commercial Code ("UCC"), which distinguishes rights for consumers and merchants in goods transactions,[261] consumers should expect, in theory, to be *better* protected—not worse off—than merchants entering into a similar services transaction. As such, courts or legislatures should deem an implied term to exist in digital agreements requiring clear, conspicuous, and seasonable notice of modifications to agreements, explaining any changes in plain language and requiring affirmative consent and, potentially, additional consideration.

Courts have dealt cautiously with unilateral amendment in digital contracts. In *Douglas v. U.S. District Court for the Central District of*

260. As of August 2012, forty-six states have passed data-breach notification statutes. *State Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx (last visited Oct. 6, 2013). Moreover, Congress has considered statutes that address privacy and data security, and several states have passed data aggregation and marketing restrictions. Jeffrey S. Tenenbaum, *Restrictions on Association Fax and Email*, CENTER FOR ASS'N LEADERSHIP (Nov. 2011), http://www.asaecenter.org/Resources/whitepaperdetail.cfm?ItemNumber=12142.

261. *See, e.g.*, 72 AM. JUR. 2D *Statute of Frauds* § 106 (2012) (noting that UCC § 201 is a special provision governing contracts between merchants).

California, the Ninth Circuit held that Douglas, a subscriber to Talk America's long distance telephone service, was not bound by changes to the subscriber agreement made by Talk America without Douglas's consent or sufficient notice to him.[262] Talk America had simply posted a revised standard contract on its website.[263] The court stated that "a party can't unilaterally change the terms of a contract; it must obtain the other party's consent before doing so."[264] Although the Ninth Circuit is correct in its analysis, the agreement in question did not contain a provision that permitted unilateral modifications by the drafter.[265] Hence, some courts and contracts scholars may consider this an open question in the area of "rolling contracts."[266]

When a data aggregator modifies its terms of data stewardship unilaterally and without additional consideration, such modifications should appropriately fall within the pre-existing duty rule. The pre-existing duty rule states that an agreement to perform a pre-existing duty, such as pursuant to an existing contract, is insufficient to constitute consideration for a change to that contract.[267] In order to be bound to new terms, the party must either explicitly agree to enter into essentially a new agreement on those terms or otherwise receive some benefit.[268] Another privacy-related context in which the pre-existing duty rule frequently comes into play relates to confidentiality and noncompetition agreements.[269] When an employee arrives to begin work at a new employer, the consideration for a

262. Douglas v. U.S. Dist. Court for the Cent. Dist. of Cal., 495 F.3d 1062, 1066–67 (9th Cir. 2007).

263. *Id.* at 1065.

264. *Id.* at 1066.

265. *See id.* at 1065.

266. For a discussion of rolling contracts, see generally Gillette, *supra* note 227. According to Gillette, rolling contracts are arrangements that "essentially permit parties to reach agreement over basic terms, such as price and quantity, but leave until a later time, usually simultaneous with the delivery or first use of the goods, the presentation of additional terms that the buyer can accept . . . or reject." *Id.* at 681.

267. 3 WILLISTON, *supra* note 25, § 7:36 ("[W]hen a party does simply what it has already obligated itself to do under a contract, it cannot demand any additional compensation or benefit, and . . . if the party takes advantage of the situation and obtains a promise for more, the law [generally] regards it as not binding as lacking consideration."). *See also* RESTATEMENT (SECOND) OF CONTRACTS § 73 (1981) ("Performance of a legal duty owed to a promisor which is neither doubtful nor the subject of honest dispute is not consideration; but a similar performance is consideration if it differs from what was required by the duty in a way which reflects more than a pretense of bargain.").

268. 3 WILLISTON, *supra* note 25, § 7:36.

269. For background information on confidentiality agreements, see 2 JAGER, *supra* note 193, § 13:3. For a discussion of consideration and noncompetition agreements, see generally Norman D. Bishara, *Fifty Ways to Leave Your Employer: Relative Enforcement of Covenants Not to Compete, Trends, and the Implications for Employee Mobility Policy*, 13 U. PA. J. BUS. L. 751, 775–76 (2011).

confidentiality agreement is generally construed to be the offer of employment, provided that the employee executes the agreement prior to starting work.[270] If, however, the employee is presented with the agreement after commencing work, many courts have found that such agreements are not enforceable unless new consideration was offered to support the agreement.[271] Continued employment is inadequate consideration in many cases.[272]

This approach should be adopted in cases in which data aggregators attempt to unilaterally amend terms of consumer information contracts. Regardless of whether the terms of agreement include an assertion that the terms may change, courts should require additional consideration to support any such modification. Particularly in consumer-facing contracts, concerns over unfair surprise and oppression loom large.[273] If one side can modify every provision of the agreement at its sole discretion and the other side cannot fully extract itself from the relationship because of data collection, the entire theory of contract as a bargained-for exchange is subverted. Does a consumer consent to even extreme, subsequent modifications to the terms? Is there a limit to the types of information collection obligations that will be enforced after a unilateral modification? What about a new onerous obligation such as requiring consumers to ship their computer to the company for data mining at their own expense once a month?[274]

Consequently, any material change to the privacy terms of a consumer information contract should be deemed to constitute a major modification to the deal terms, therefore requiring affirmative consent and potentially new consideration. In the absence of both, the contract can be deemed at an end. Because access to the consumer data stream is, at least in part, consideration for the ongoing services of a data aggregator, the end of the services also constitutes (or should constitute) the cessation of the stream of

270. Bishara, *supra* note 269, at 775, 791.

271. *Id.* at 776, 792.

272. *Id.*

273. A bilateral amendment provision in a contract is traditionally viewed as an agreement to cooperate in good faith regarding any modifications to a contract. Far from being an agreement to cooperate, a unilateral amendment provision is a blank-check reservation of rights solely for the benefit of one party without stipulating the nature of that benefit. As such, it grants one party unfettered power to alter deal terms in its favor. *See, e.g.*, David Horton, *The Shadow Terms: Contract Procedure and Unilateral Amendments*, 57 UCLA L. Rev. 605, 645–60 (2010) (arguing that unilateral modifications undermine efficiency and create perverse incentives for drafters).

274. The vagueness of such provisions can render them unenforceable. When a reasonable person cannot objectively discern the meaning of a term, a provision becomes suspect on the basis of vagueness and can be struck down by a court. 17A AM. JUR. 2D *Contracts* § 337 (2013).

consideration.

There remains an open question from the privacy standpoint: logistically, how do consumers delete their accounts and their data in the data aggregator's possession without needing to consent to new contract terms in order to do so? Currently, for example, in order for consumers to gain access and manually delete their information, they may have to click "yes" to a clickwrap agreement,[275] or they may continue past the page with a notice browsewrap[276] of term changes. Thus, in the process of deleting their account, users may be deemed to have first accepted the new terms. Further, some methods of tracking consumers may continue to follow them after they have discontinued use. Hence, there also exists a need for statutory termination rights with respect to data privacy.

G. PROPOSAL 7: CREATING MEANINGFUL TERMINATION RIGHTS

When a data aggregator materially breaches terms of use or a privacy policy or modifies terms in a manner that consumers find undesirable, a question arises regarding what happens to consumers' previously shared information. Does a data aggregator retain use of the shared information indefinitely? Can a data aggregator continue to collect new data from various tracking technologies installed on a consumer's machine even if the consumer no longer uses the service? If we conceptualize a data sharing relationship pursuant to a consumer information contract as an exchange of services, the answer to the second question is obviously no. No new services will be provided, and no new data should be collected. If consumers have terminated the relationship, their intent is clear: they do not wish to selectively embed any new information with the data aggregator. As for the data selectively embedded in the past, consumers' desires on this matter will vary. An approach that allows consumers the

275. Clickwrap agreements involve a pop-up box which ask the user to click "I agree" before obtaining access to content. Matwyshyn, *supra* note 27, at 550 n.95. For a discussion on the enforceability of clickwrap agreements, see Mark Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 466–67 (2006) ("Because the user has 'signed' the contract by clicking 'I agree,' every court to consider the issue has held clickwrap licenses enforceable. There is nothing inherently troubling about enforcing clickwrap licenses." (footnotes omitted)).

276. Browsewrap agreements are terms of use presented to users as a link on the page. Matwyshyn, *supra* note 27, at 552 n.107. They come in two varieties: notice browsewraps, which consist of a sentence asserting something akin to "By continuing past this page you agree to the terms of use," and a mere link to the agreement. *Id.* at 553. Notice browsewraps are likely enforceable, while a mere link to an agreement is not. *Id.* For a discussion on the enforceability of browsewraps, see Lemley, *supra* note 275, at 472–80 (arguing that recent decisions concerning browsewraps likely bind businesses but not consumers, and create problems for commercial litigation).

option to require deletion makes the most sense.[277]

Further, in physical space, no new information is shared after the parties have terminated an information sharing relationship. Similarly, at the end of a business relationship, the standard drafting of confidentiality agreements requires that the party receiving information is contractually bound to return any received information, or if return is not possible, the party is bound to destroy the information. For example, if Company A was sharing revenue figures with Company B and they terminate their relationship, Company A will not provide any further revenue figures to Company B, and Company B will be required to return or destroy any information of Company A with which it was entrusted as a consequence of the business relationship. However, this termination of accessing a consumer's information does not currently happen in digital environments. When consumers have terminated their relationship with a data aggregator, the company should cease all future tracking. However, because the consumers had previously consented (at least in theory) to various tracking methods using digital means, the code created to collect information about them may still reside on their machines or still follow them around the Internet. In other words, a data aggregator may retain technological capability to collect information about consumers long after they have ended their relationship with that company and withdrawn consent to tracking. A stream of future consideration may be extracted from consumers without their knowledge and without providing anything of value in return. Any information collected through such means following a clear consumer termination of the agreement should be deemed to constitute nonconsensual information collection—potentially an act of computer intrusion.[278]

Therefore, states should statutorily craft an implied set of terms regarding obligations upon termination of the agreement,[279] mirroring what

277. This type of option embodies, through contract law, the idea of the "right to forget" pervasive in the discourse around data privacy, particularly in the European Union and United Kingdom. For a discussion of the "right to forget," see generally VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (2011).

278. *See* Matwyshyn, *supra* note 27, at 545–48 (detailing the relationship between computer intrusion law and security-invasive digital rights management technologies). For further discussion of the relationship between contract and computer intrusion, see generally Matwyshyn, *The Law of the Zebra*, *supra* note 205 (arguing in favor of a restrained approach that separates the spheres of contract law and Computer Fraud Abuse Act enforcement).

279. *See* Meister & Alsup, *supra* note 200, at 9 ("If the parties ultimately decide not to go through with the transaction, the recipient is usually obligated under the confidentiality agreement to return all documents obtained during due diligence to the provider or to destroy such information in its possession.").

would have been negotiated in a services transaction between equals in the trade secret context. These rights should include a consumer right of deletion of existing data and a right to nonidentification in the future. Specifically, in the private sector, data sharing agreements such as confidentiality agreements typically require that each party returns or destroys any shared proprietary information upon termination of the relationship.[280] Information is usually broadly defined to include all information shared in most cases, regardless of protectability as a matter of intellectual property law.[281] Crafting a statutory right of deletion as an implied term of the data sharing agreement would provide consumers a parallel right to demand destruction of shared information.

H. PROPOSAL 8: CRAFTING DAMAGES REMEDIES FOR CASES OF DATA LOSS

Perhaps one of the most problematic questions for demonstrating privacy harms has been the question of damages. What if the database containing information that my favorite beer is Young's Double Chocolate Stout—information that I have selectively embedded—is "stolen" and distributed? If the corporate holder of that database sues the thief in tort, contract, trade secret, or under the Computer Fraud and Abuse Act for the taking of the information, damages would pertain.[282] The appropriate amount of these damages would be determined by an industry expert and could be doubled at the court's discretion.[283] Or if I have written a haiku extolling why I like Young's Double Chocolate Stout and the writing is copied and used, statutory copyright damages pertain.[284] A parallel set of

280. For example, confidentiality agreements executed prior to the start of negotiations regarding a major transaction require destruction or return of all information. *Id.*

281. In particular, facts about revenues, projections, and insider opinion documents are contemplated within these definitions of proprietary information. *See id.* at 2–4. It is not a stretch to say that my favorite flavor of beer is parallel to a bit of information in the consumer privacy context.

282. *See, e.g.*, Delucca v. GGL Indus., Inc., 712 So. 2d 1186, 1187 (Fla. Dist. Ct. App. 1998) (per curiam) (finding that customer information not available through other means constitutes trade secrets); Kavanaugh v. Stump, 592 So. 2d 1231, 1232 (Fla. Dist. Ct. App. 1992) (recognizing that customer lists can constitute trade secrets if they are not just a compilation of information commonly available to the public); E. Colonial Refuse Serv., Inc. v. Velocci, 416 So. 2d 1276, 1278 (Fla. Dist. Ct. App. 1982) (same); Unistar Corp. v. Child, 415 So. 2d 733, 734 (Fla. Dist. Ct. App. 1982) (same).

283. *See, e.g.*, Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268, 1326 (S.D. Fla. 2003) (awarding compensatory damages of about $2 million for misappropriated customer information, and exercising discretion under the Uniform Trade Secrets Act to double the compensatory damages award in light of intentional computer-hacking activities), *aff'd in part, rev'd in part*, 138 F. App'x 297 (11th Cir. 2005) (unpublished table decision).

284. Yet, if I attempted to sue the company or the thief on the basis of the lost information rather than a copyright interest, a court would likely find no basis for awarding damages, other than perhaps actual credit monitoring costs. *E.g.*, Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1021 (D.

damages remedies may be needed in consumer privacy and information security contract breach actions, and crafting such remedies does not present an insurmountable challenge.

Contract law doctrine has evolved to quantify damages in several ways—restitution damages, reliance damages, expectation damages, and punitive damages.[285] Restitution damages generally involve a calculation of damages based not on the plaintiff's loss but rather on the extent of the defendant's unjust enrichment. Therefore, in cases involving a breach of implied promises of data stewardship, a defendant's self-stipulated value of a database of consumer information as it appears on the company's balance sheets can become the operative basis for calculation of harm, just as the valuation of this database would be used in a trade secret case litigating the theft of the database.[286] After all, the data's value induced the data sharing relationship.[287] Either consumer data holds some individual value, as Part II argued, or the databases of preferences which comprise the core asset of enterprises, such as Facebook, are worthless in the aggregate.[288] Dividing the self-stipulated value of the database by the number of users in the database will result in one possible value for each individual user's records.

Reliance damages seek to put plaintiffs in the position they would have been in had the promise never been made.[289] This typically includes

Minn. 2006) (dismissing a claim alleging negligent protection of data for lack of "present injury or reasonably certain future injury").

285. Additionally, contract law offers a tradition of equitable remedies when courts find that contract remedies are unavailable. Examples of possible equitable remedies include equitable reliance or promissory estoppel, quantum meruit, restitution or unjust enrichment, and specific performance. For a discussion of equitable remedies, see generally Mark R. Hinkston, *Written Contract Alternatives*, WIS. LAW., Feb. 2000, at 14 (discussing the various forms of equitable remedies available for plaintiffs who performed valuable services but did not execute a written agreement).

286. If the defendant has not recently been involved in trade secret litigation over the database, its value can be found, for example, on the balance sheets exchanged during the defendant's last major transaction. A goodwill calculation will certainly be listed, which includes the self-projected value of databases of customers. Alternatively, the database valuation may be included under intangible assets if the company believes it to be a trade secret or copyright protected. For a discussion of valuation, see generally Bernard Trujillo, *Patterns in a Complex System: An Empirical Study of Valuation in Business Bankruptcy Cases*, 53 UCLA L. REV. 357 (2005).

287. *See supra* Part II.

288. This statement is based on a simple mathematical reality: $0 multiplied by 50,000,000 users would still equal $0. If the company asserts on its balance sheets that x times 50,000,000 users equals something other than zero, then, solving for x as the value of an individual user's data, the value of x cannot equal zero. Even assuming a multiplier effect happens because of the size of databases, the value of an individual user's data still cannot equal zero.

289. *See, e.g.*, RESTATEMENT (SECOND) OF CONTRACTS § 349 (1981) (stating that reliance interest includes "expenditures made in preparation for performance or in performance, less any loss that the party in breach can prove with reasonable certainty the injured party would have suffered had the contract been performed").

restitution damages, as well as other "out-of-pocket" and "overhead" expenses.[290] In the case of a privacy violation, a court's calculation would again potentially start with a defendant's self-stipulated database value but also add to it any costs the consumer may have incurred as a consequence of the relationship. Such costs could perhaps include any penalty fee for terminating a previous contractual relationship the consumer incurred in order to use the defendant's service or the cost of the consumer's Internet service that allows the plaintiff to use the defendant's services.[291]

But perhaps some courts will struggle with the fact-intensive or battle-of-the-experts nature of the database valuation inquiry. Or, maybe some legislatures will believe that the damages awards are undervaluing the privacy interest violated when a breach of consumer information contract occurs with respect to privacy. These legislatures can adopt a statutory damages approach modeled on intellectual property law.[292] Under such an approach, in situations with uncertain data valuation, a harmed consumer would have the election of either actual demonstrated damages, or statutory damages as determined by the legislature—just as plaintiffs do in copyright litigation.[293]

The rationale behind offering a choice of statutory damages or actual value damages awards in copyright was simple: perhaps my ode to chocolate stout, though valuable to me, simply was not very good from the standpoint of commercial viability and would never have earned me a penny.[294] Yet, it is still mine to control and, hence, valuable. Therefore,

290. *See id.* cmt. a (illustrating examples of reliance damages).

291. *Id.*

Expectation or compensatory damages aim to put a plaintiff in the position he would have been in had contract (or the promise) been fulfilled. *Id.* § 347. This typically means that plaintiffs are awarded the profits they would have made had the promise been kept. However, interestingly, in the case of a privacy promise violation, courts could leverage an expectation damages calculus not only to offer monetary damages but perhaps to offer the true "benefit of the bargain"—good privacy practices—as a type of specific performance-like damages remedy in addition to a monetary damages remedy. As our discussion of breach noted, privacy violations are likely to be deemed a material breach because money damages do not adequately compensate for the damage: once data is leaked, it is out there. *See supra* text accompanying notes 219–27. Actual costs incurred in mitigation of the breach, such as credit reporting service registration, would similarly be included in at least an expectation damages calculus of consumer information contract privacy damages. RESTATEMENT (SECOND) OF CONTRACTS § 347.

292. *See* Pamela Samuelson, *Is Copyright Reform Possible?*, 126 HARV. L. REV. 740, 754 (2013) (book reviews) (explaining that "[u]nder current law, a successful copyright claimant can opt for an award of statutory damages instead of actual damages. The normal range for statutory damage awards is between $750 and $150,000 per infringed work." (footnote omitted)).

293. *Id.* at 754–55.

294. *See* William W. Fisher III et al., *Reflections on the Hope Poster Case*, 25 HARV. J.L. & TECH. 243, 310–11 (2012). In particular, William Fisher and company explain that "[w]hen a copyright

borrowing from copyright law, legislatures should craft a minimum statutory damages amount in a sliding-scale approach, analyzing each lost data record as one instance of harm.[295] Thus, losing my favorite beer would be one instance while losing my favorite beer and my social security number would be two instances of data loss. Borrowing again from trade secret law, courts should be granted the discretion to double damages depending on the severity of the loss and to treble damages for repeat offenses, in a manner parallel to copyright.[296]

V. CONCLUSION

This Article has argued in favor of better protections for consumer data privacy and information security through a contract-based approach driven by implied promises of reasonable data stewardship. It challenged three "fatalisms" commonly held in the privacy literature about the viability of contract-based approaches to privacy concerns. Applying the theory of Pierre Bourdieu and marketing theory, the Article explained how consumer data, a "thing of value," is legally sufficient consideration that triggers promises from the data aggregator of services and data care. Finally, borrowing concepts from trade secret law, this Article proposed a model of "reasonable data stewardship" in contracting, which articulated a way to apply the existing doctrines of implied promises and optional statutory damages to address deficiencies in consumer information privacy.

owner is unable to prove his actual damages or the infringer's profits, he may, at any time before final judgment is rendered, elect to receive statutory damages instead, in a sum of not less than $750 or more than $30,000 as the court considers just." *Id.* at 310 (internal quotation marks omitted). Furthermore, they add that "the Copyright Act gives the court discretion to quintuple the statutory damages, to as much as $150,000 per infringement, in the event a defendant is found to have acted 'willfully,'" even though the Copyright Act does not define willfulness. *Id.* at 310–11.

295. For a discussion of copyright damages, see Alan E. Garfield, *Calibrating Copyright Statutory Damages to Promote Speech*, 38 FLA. ST. U. L. REV. 1, 10–12 (2010).

296. Although punitive damages are generally not awarded in commercial cases, they are sometimes awarded under extraordinary circumstances in noncommercial contract disputes. A privacy violation breach of contract action would indeed be a noncommercial contract dispute from the perspective of the consumer. Thus, even if a finder of fact were unwilling or unable to find a significant restitution component in the damages calculation, a nominal actual damages award could support the award of punitive damages as an addition. For a discussion of punitive damages, see generally Joseph A. Seiner, *Punitive Damages, Due Process, and Employment Discrimination*, 97 IOWA L. REV. 473 (2012) (analyzing punitive damages in the employment discrimination context).