American University Law Review

Volume 60 | Issue 6 Article 2

2011

Website Design as Contract

Woodrow Hartzog
whartzog@samford.edu

Website Design as Contract

WEBSITE DESIGN AS CONTRACT

WOODROW HARTZOG*

TABLE OF CONTENTS

INTRODUCTION

When courts seek to determine a website user's privacy expectations and the website's promises to that user, they almost invariably look to the terms of use agreement or to the privacy policy.[1] Courts rarely look to the

* Assistant Professor, *Cumberland School of Law at Samford University*; Affiliate Junior Scholar, Center for Internet and Society, *Stanford Law School*. The author would like to thank Daniel Solove, William McGeveran, Chris Hoofnagle, Ryan Calo, Cathy Packer, Anne Klinefelter, Nancy Kim, Jen King, Fred Stutzman, Dean Smith, Jennifer Hartzog, Danielle Citron, Marcia Hofmann, Will DeVries, Lauren Willis, Jennifer Urban, Deven Desai, the Cumberland School of Law faculty, the participants of the Third Annual Privacy Law Scholars Conference, and the participants of Samuelson Law, Technology & Public Policy Clinic's Privacy Scholars Speakers Series.

1. *E.g.*, McVicker v. King, 266 F.R.D. 92, 95–96 (W.D. Pa. 2010) (looking to the privacy policy and terms of service to find that a blog created an expectation of privacy for its users); Sedersten v. Taylor, No. 09-3031-CV-S-GAF, 2009 WL 4802567, at *1, *3 (W.D. Mo. Dec. 9, 2009) (finding a website privacy policy does not waive a user's right to anonymous free speech); *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299,

privacy settings or other elements of a website where users specify their privacy preferences because these settings and elements are typically not considered part of any contract or promise to the user.[2] Yet studies have shown that few users actually read or rely upon terms of service or privacy policies.[3] In contrast, users regularly take advantage of and rely upon privacy settings.[4]

Consider Facebook. The social networking site has a Terms of Use Agreement with a section titled "privacy."[5] The agreement references Facebook's privacy policy, a separate document.[6] Many users, however, do not rely on these documents when establishing the privacy they expect when using Facebook.[7] When a user sets up a Facebook profile, the user can set a series of privacy settings that allow the user to control how widely accessible the profile is.[8] The user's profile can be viewed by friends only—those people explicitly invited to see the profile—or by "friends of

---

325 (E.D.N.Y. 2005) (examining an airline's privacy policy to determine whether plaintiffs had a claim for reliance); Dyer v. Nw. Airlines Corp., 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004) (finding that plaintiffs failed to allege that they read, understood or relied upon the privacy policy and thus failed to allege contractual damages); *In re* Nw. Airlines Privacy Litig., No. 04-126(PAM/JSM), 2004 WL 1278459, at *6 (D. Minn. June 6, 2004) (holding that the privacy statement did not constitute a unilateral contract and that plaintiff must have read the policy to rely on it).

2. *See infra* Part II.A.2 (discussing courts' treatment of privacy settings and elements in determining the existence of a contract); *see also infra* Part II.A.4 (proposing the use of website design as a contract and discussing the accompanying issues).

3. TABREEZ GOVANI & HARRIET PASHLEY, STUDENT AWARENESS OF THE PRIVACY IMPLICATIONS WHEN USING FACEBOOK pt. 5.3 (2005), http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf (finding that 80% of the users surveyed for the study had not read the Facebook Privacy Policy); Andy Greenberg, *Who Reads the Fine Print Online? Less Than One Person in 1000*, FORBES (Apr. 8 2010, 3:15 PM), http://blogs.forbes.com/firewall/2010/04/08/who-reads-the-fine-print-online-less-than-one-person-in-1000/ (noting that studies have found that only 0.11% of users will view a site's terms of service by clicking on a link).

4. MARY MADDEN & AARON SMITH, PEW INTERNET & AM. LIFE PROJECT, REPUTATION MANAGEMENT AND SOCIAL MEDIA: HOW PEOPLE MONITOR THEIR IDENTITY AND SEARCH FOR OTHERS ONLINE 2 (2010), http://www.pewinternet.org/Reports/2010/Reputation-Management.aspx (finding that "71% of social networking users ages 18–29 have changed the privacy settings on their profile to limit what they share with others online").

5. *Statement of Rights and Responsibilities*, FACEBOOK, http://www.facebook.com/terms.php?ref=pf (last revised Apr. 26, 2011) (stating, in the first term of the agreement, that "[y]our privacy is very important to us" and referring users to the website privacy policy).

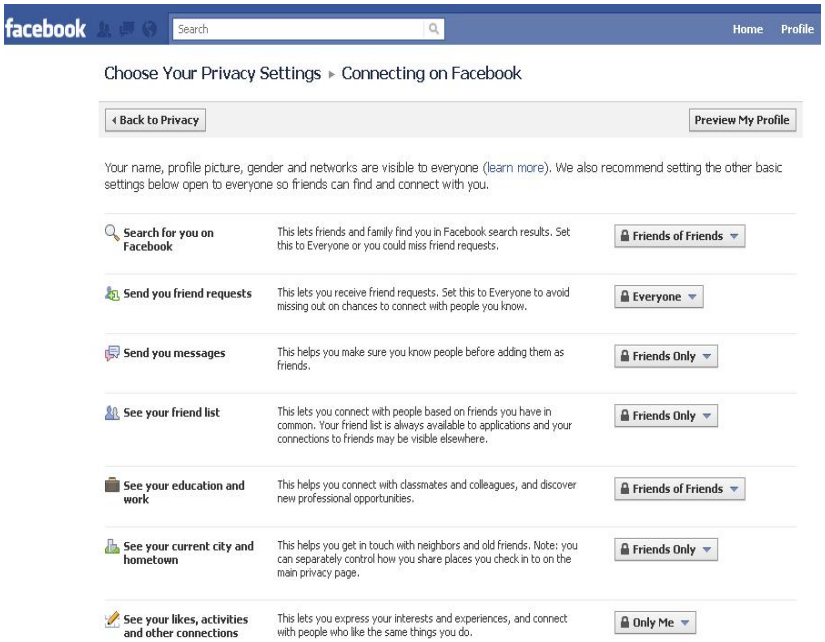
6. *See id.* (directing users to click a link to view the privacy policy); *Facebook's Privacy Policy*, FACEBOOK, http://www.facebook.com/policy.php (last revised Dec. 22, 2010) (informing users of how the website uses and shares users' information, along with extensive other terms).

7. *See* JOSEPH TUROW ET AL., THE FTC AND CONSUMER PRIVACY IN THE COMING DECADE 2, 12 (FTC Tech-ade Workshop 2006), http://www.law.berkeley.edu/files/FTC_Consumer_Privacy.pdf (finding that only 1.4% of study participants reported reading the terms of standard-form electronic agreements often and thoroughly, 66.2% rarely read or browse these agreements, and 7.7% stated that they have never noticed or read them).

8. *See Controlling How You Share*, FACEBOOK, http://www.facebook.com/privacy/Explanation (last visited Aug. 9, 2011) (enabling users to control, via customization, the accessibility of their Facebook profile).

friends," which expands the exposure much further, to anyone linked to the user's friends.[9] If the user wants to expose personal information to all Facebook users, the profile can be set to be public.[10] The user can also specify whether the profile appears in Internet search results.[11]

Figure 1:
Screenshot of Facebook's Privacy Settings (June 2011)



These settings, more than the vague, verbose, and often unread terms of service and privacy policy, are usually determinative of a user's privacy

9. *See id.* (describing the different sharing options, including sharing information with "Everyone," "Friends of Friends," and "Friends Only").

10. *See id.* (noting that the information that users do not protect, meaning "[i]nformation available to everyone," is viewable by anyone on the Internet). The fact that a profile is "public" can have significant legal consequences. *See* Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 861 (Ct. App. 2009) (noting that "once posted on myspace.com," Moreno's posting was "available to anyone with internet access"). In *Moreno*, the court held that a woman who posted a poem to her public profile on the social network site MySpace had no reasonable expectation of privacy because she "publicized her opinions . . . [on] a hugely popular internet site. [Moreno's] affirmative act made her article available to any person with a computer and thus opened it to the public eye." *Id.* at 862.

11. *See Controlling How You Share*, *supra* note 8 (noting that the "[p]ublic search" option "controls whether things [users have] specifically chosen to share with everyone show up in searches" on the Internet).

expectations when using Facebook. A user relies on these settings.[12] Indeed, without the ability to set a profile to be viewable only by friends, a user might not sign up to use Facebook at all, or would reveal far less intimate information in the online profile.[13] Should the privacy settings be considered part of the agreement between the user and Facebook? In an age where website interactivity is the hallmark of many sites, courts must re-think what constitutes an online agreement.

This Article proposes that website features and design should, in some contexts, be considered enforceable promises. Code-based negotiations for confidentiality can form implied-in-fact contracts or give rise to a claim for promissory estoppel.[14] The so-called "Web 2.0"[15] has provided individuals with a greater ability to negotiate terms regarding their own privacy by accepting offers to delete personal information, remove identifying tags, and use privacy settings—online activities that clearly indicate a user's desire to control the flow of her personal information.[16] Yet courts often fail to recognize these code-based promises, instead considering them little more than luxuries offered by websites.[17] This is the case even though these features are often couched in a contractual setting.[18]

Doctors, lawyers, financial professionals, priests, and even intimate partners regularly make implicit promises to respect the privacy of others based upon the context of their relationship.[19] Yet on the Web, courts seem

---

12. *See* Complaint at 2, 12, Del Vecchio v. Amazon.com, Inc., No. 2:11-cv-00366-RSL (W.D. Wash. Mar. 2, 2011) (describing users' use of privacy settings, and alleging that Amazon circumvented the settings established by users); Complaint at 2, 7, Ferguson v. Classmates Online, Inc., No. 2:10-cv-00365-RAJ (W.D. Wash. Mar. 5, 2010) (alleging a claim for, among others, breach of contract for failing to keep confidential information protected by privacy settings).

13. *See, e.g.*, MADDEN & SMITH, *supra* note 4, at 2 (noting that the majority of social network site users have utilized privacy settings to limit what they share online).

14. *See, e.g.*, McVicker v. King, 266 F.R.D. 92, 96 (W.D. Pa. 2010) (finding that "the terms of service of the blog create an expectation of privacy for any registered user"); Complaint at 23–24, *Del Vecchio*, No. 2:2011-cv-00366-RSL (alleging that Amazon's privacy policy and privacy notice constituted promises to users that their privacy settings would function as users' expected).

15. *See* Tim O'Reilly, *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, O'REILLY NETWORK (Sept. 30, 2005), http://oreilly.com/web2/archive/what-is-web-20.html (describing the meaning of the term "Web 2.0").

16. *See Controlling How You Share*, *supra* note 8 (noting that Facebook users can control what parts of their profile and corresponding information are viewable, and to whom).

17. *See, e.g.*, Dyer v. Nw. Airlines Corp., 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004) (looking only to the privacy policy itself, as opposed to code-based promises, to determine whether a breach of contract related to privacy had occurred); *see also infra* Part II.A.1 (describing types of "code-based promises," such as padlock images on websites).

18. *See* Lauren Gelman, *Privacy, Free Speech, and "Blurry-Edged" Social Networks*, 50 B.C. L. REV. 1315, 1341 (2009) (noting that even where websites "create the illusion of limited publication and control," there is no way for users to utilize that control nor is there any law that recognizes those user decisions); *Controlling How You Share*, *supra* note 8.

19. *See, e.g.*, Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship*

to recognize only boilerplate terms of use when analyzing contractual agreements.[20] The central thesis of this Article is that by primarily relying on standard-form terms to analyze online agreements, courts risk ignoring the full agreement between the parties. This approach has inhibited contract-based solutions to protect the flow of personal information. The advent of highly interactive website design compels a re-examination of the contractual relationship between websites and their users. No area is in greater need of increased scrutiny than user privacy.

This Article introduces a new theory into contract doctrine and the surprisingly-neglected intersection of online agreements and confidentiality. This Article contains three proposals to refocus the law away from standard-form doctrine to an approach that more accurately reflects the agreements between websites and users. First, to the extent website design is incorporated into, or is consistent with, a website's terms of use, or to the extent website design induces reliance, courts should consider these design features enforceable promises. Second, courts should expand their analysis of unconscionability to include consideration of malicious interfaces that manipulate, exploit, or attack users in areas of a website beyond the terms of use. Third, website design should be seen as a subsequent agreement, or "operational reality," between the parties. This Article concludes by proposing that a more nuanced analysis of online agreements is necessary when highly interactive websites implicate an individual's privacy. While online agreements can threaten an individual's privacy, the extension of contract doctrine to website design represents an opportunity for users to regain at least some control over the flow of personal information.

I. CHOKING ON FORM CONTRACTS

Courts often ignore website design and interactive features as implicit and explicit aspects of the agreement between the website and the user. This is a significant omission, since the only other contractual terms on virtually every website are standard-form.[21] This section will review the doctrine surrounding online contracts and caution against ignoring much of

---

Privacy Through Implied Contracts of Confidentiality, 74 U. CIN. L. REV. 887, 913 (2006) (observing that "[c]onfidential relationships are recognized by the law in a variety of contexts, including familial, friendship, and business relationships" and that each relationship contains an "implicit promise of confidentiality" characterized by reasonable expectations, customs, and reliance).

20. *See* Robert A. Hillman & Jeffery J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. REV 429, 434 (2002) (stating that the principal legal issue in interpreting both paper and virtual contracts is the effect that should be given to boilerplate terms).

21. *See id.* at 429 (recognizing the proliferation of boilerplate language in agreements on websites).

the website-user relationship by relying solely on the text in terms of use and privacy policies.

A primary function of the Internet is connecting people. These connections can create a privity of contract between websites and users.[22] Contracts between websites and users are typically found in the form of terms of use.[23] With online agreements on a number of websites, the 74% of Americans online each day[24] may enter into dozens of contracts that impact the flow of their personal information. These agreements are adjudicated under standard-form contract doctrine because they are perceived as non-negotiable.[25] This means users are regularly bound by terms they did not read or understand—a common critique of all standard-form contracts.[26]

Much, if not all, online communication falls within the ambit of a website's terms of use or privacy policy. Behavioral restrictions regulate users' interactions with other users. Privacy policies dictate how personal information and browsing activity will be stored and used.[27] Terms of use disclaim liability for a large swath of website activity and inaccuracies.[28] These terms are purportedly contracts; moreover, these contracts are found on virtually every website on the Internet.[29]

Before the Internet, most standard-form contracts, which were largely adhesive in nature, were typically used in high-volume consumer sales transactions.[30] These contracts enabled mass commerce because they

---

22. Privity is defined as "[t]he connection or relationship between two parties, each having a legally recognized interest in the same subject matter." BLACK'S LAW DICTIONARY 1320 (9th ed. 2009).

23. *See* Molnar v. 1-800-Flowers.com, Inc., No. CV 08-0542 CAS (JCx), 2008 WL 4772125, at *2, *6 (C.D. Cal. Sept. 29, 2008) (looking to a website's "Terms of Use" to find a contract between the defendant website and the plaintiff, a website user).

24. *74%—America Online*, PEW INTERNET & AM. LIFE PROJECT, http://pewresearch.org/databank/dailynumber/?NumberID=948 (last visited June 3, 2011).

25. *See* Burcham v. Expedia, Inc., No. 4:07cv1963 CDP, 2009 WL 586513, at *2 (E.D. Mo. Mar. 6, 2009) (providing that "[a] customer on notice of contract terms available on the internet is bound by those terms," just as with any binding contract).

26. *Id.*; *see also* Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1174, 1179 (1983) (noting that with contracts of adhesion, such as standard-form contracts, "the adhering party is in practice unlikely to have read the standard terms before signing the document and is unlikely to have understood them if he has read them").

27. *See, e.g.*, *Facebook's Privacy Policy*, *supra* note 6.

28. *See* Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 460 (2006) (indicating that terms of use "control (or purport to control) the circumstances under which buyers of software or visitors to a public Web site can make use of that software or site").

29. *See, e.g.*, David Mirchin, *Terms of Use: The Rules Have Changed*, INFO. TODAY, Oct. 2007, at 1 ("Virtually every commercial and noncommercial Web site has Web site 'Terms and Conditions,' or Terms of Use.").

30. *See* NANCY S. KIM, 'WRAP CONTRACTS AND PRIVACY 1 (Association for the Advancement of Artificial Intelligence Press Technical Report SS-10-05, 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1580111 (observing that "as mass market sales became possible with industrialization, so did mass consumer form contracts"

managed risk well and lowered the cost of transactions.[31] Websites created a new venue for standard-form contracts in the form of terms of use. Site administrators use them to limit liability through traditional means—such as arbitration clauses and disclaimers of warranties—while maximizing the benefit of user participation by restricting user behaviors and remedies and requiring a relinquishment of rights, including certain privacy and intellectual property interests.[32] As websites became ubiquitous, so did terms of use. As a result, an overwhelming amount of online activity is not governed by default law but rather through agreement between the parties.[33]

The omnipresence of standard-form contracts can be troubling. According to the great scholar Friedrich Kessler, standard-form contracts allow businesses "to legislate in a substantially authoritarian manner without using the appearance of authoritarian forms."[34] Kessler found that this power "enabl[es] [businesses] to impose a new feudal order of their own making upon a vast host of vassals."[35] This "orgy of contract formation"[36] has significant consequences for information privacy. To properly frame the contractual significance of code-based promises in privacy disputes, a brief review of online contract doctrine is in order.

---

because it was generally easier "to create standard terms for standard business transactions" where communication with individual customers was impracticable).

31. *See* Rakoff, *supra* note 26, at 1230 (noting that contracts of adhesion, such as standard-form contracts, create cost savings and lower prices that result from placing the risk on the consumer or adherent).

32. JOSEPH BONNEAU & SÖREN PREIBUSCH, THE PRIVACY JUNGLE: ON THE MARKET FOR DATA PROTECTION IN SOCIAL NETWORKS 24 (The Eighth Workshop on the Economics of Information Society 2009), http://preibusch.de/publications/Bonneau_Preibusch__Privacy_Jungle__2009-05-26.pdf (concluding that the authors' study of various website privacy policies revealed "few meaningful rights [were] assigned to users," while website operators "reserved many data collection and sharing rights for themselves"); Sandra Braman & Stephanie Roberts, *Advantage ISP: Terms of Service as Media Law*, 5 NEW MEDIA & SOC'Y 422, 438 (2003) (discussing the ways that Internet Service Providers limit their own liability, while also infringing on user rights).

33. *See* Braman & Roberts, *supra* note 32, at 423 (noting that subscribers or users of Internet Service Providers do so on the basis of a contractual agreement with the provider).

34. Friedrich Kessler, *Contracts of Adhesion—Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629, 640 (1943).

35. *Id.*

36. This phrase was borrowed from Guido Calabresi in his 1982 book *Common Law for the Age of Statutes*. Calabresi stated, "The last fifty to eighty years have seen a fundamental change in American law. In this time we have gone from a legal system dominated by the common law, divined by courts, to one in which statutes, enacted by legislatures, have become the primary source of law." GUIDO CALABRESI, COMMON LAW FOR THE AGE OF STATUTES 1 (1982). Calabresi himself borrowed the phrase from Grant Gilmore when he argued that this "orgy of statute making" had significant consequences for American jurisprudence. The current "Age of Contracts" similarly threatens to alter the dominant form of law governing individuals online.

A. A Brief Review of "Wraps"

It has become a truism that virtually no one reads standard-form online agreements. A recent study found that less than one in 1000 e-commerce website users read the terms of use.[37] Even Supreme Court Chief Justice John Roberts has admitted he does not read the fine print on websites.[38] Yet these agreements are routinely enforced, although not without great debate.[39]

Online standard-form contracts are typically categorized as "clickwrap" or "browsewrap" agreements, although that distinction can be blurred at times.[40] A clickwrap agreement requires some kind of affirmative act like the click of a mouse on a button indicating an assent prior to accessing a website.[41] Browsewrap agreements dictate that additional browsing past the homepage constitutes acceptance of the contract.[42] Terms of use agreements, which often incorporate privacy policies, are types of clickwrap and browsewrap agreements.

These agreements contain many standard terms, such as arbitration clauses, damage limitations, and warranty disclaimers.[43] Increasingly, terms of use also include consent to spyware clauses,[44] vague behavioral restrictions,[45] and severe limitations on the use of content from the website.[46]

---

37. YANNIS BAKOS ET AL., DOES ANYONE READ THE FINE PRINT? TESTING A LAW AND ECONOMICS APPROACH TO STANDARD FORM CONTRACTS 2 (NYU Center for Law, Economics and Organization, Law & Economics Research Paper Series, Working Paper 09-40, 2009), *available at* http://ssrn.com/abstract=1443256; *see also* Greenberg, *supra* note 3.

38. Debra Cassens Weiss, *Chief Justice Roberts Admits He Doesn't Read the Computer Fine Print*, ABA JOURNAL LAW NEWS NOW (Oct 20, 2010, 7:17 AM), http://www.abajournal.com/news/article/chief_justice_roberts_admits_he_doesnt_read_the_computer_fine_print/. Chief Justice Roberts also stated that standard-form agreements were a problem without a clear answer. *Id.*

39. *See, e.g.*, Nancy S. Kim, *Clicking and Cringing*, 86 OR. L. REV. 797, 800 n.10 (2007) (citing Richard Craswell, *Property Rules and Liability Rules in Unconscionability and Related Doctrines*, 60 U. CHI. L. REV. 1, 9–10 (1993)); Juliet M. Moringiello, *Signals, Assent and Internet Contracting*, 57 RUTGERS L. REV. 1307, 1311 (2005).

40. *See, e.g.*, Hotels.com v. Canales, 195 S.W.3d 147, 155 (Tex. Ct. App. 2006) (resolving that the user agreement on the Hotels.com website could not "neatly be characterized as either a 'click-wrap' or 'browse-wrap' agreement").

41. *See* Kim, *supra* note 39, at 799.

42. *See* Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 429 (2d Cir. 2004); Specht v. Netscape Comm. Corp., 306 F.3d 17, 22 n.4 (2d Cir. 2002) (describing "click-wrap" agreements); Pollstar v. Gigmania Ltd., 170 F. Supp. 2d 974, 981–82 (E.D. Cal. 2000).

43. Wayne R. Barnes, *Toward a Fairer Model of Consumer Assent to Standard Form Contracts: In Defense of Restatement Subsection 211(3)*, 82 WASH. L. REV. 227, 229 (2007).

44. Wayne R. Barnes, *Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance*, 39 U.C. DAVIS L. REV. 1545, 1547 (2006) (articulating that consumers often agree to have spyware loaded onto their computers without realizing it).

45. *See, e.g.*, *Statement of Rights and Responsibilities*, *supra* note 5 ("You will not post content or take any action on Facebook that infringes or violates someone else's rights.").

46. *See, e.g.*, *Terms of Use*, VOICE OF SAN DIEGO (Jan. 25, 2005), http://www.voiceofsandiego.org/terms_of_use/ (asserting that users cannot "reuse, republish

The parties' state of mind during the formation of these agreements is irrelevant. Rather, courts consider what the parties objectively conveyed to each other in what is known as "the objective theory of contract."[47] Only external acts and manifestations, not subjective, internal intentions, determine mutual assent to a contract.[48] When a website contains the phrase, "we respect your privacy," it does not matter what the website intended.[49] The question is what a reasonable person in the user's position would have understood from that communication.[50] Thus, online, courts should consider the entire user experience to adequately understand the average user.

Although courts analyze online contracts according to traditional principles of contract law, two special problems arise in the context of online agreements: requirements of noticeable presentation of offers and formations of assent. Both problems arise due to the unique features of websites. In interpreting online contracts, courts "focus on whether the plaintiff had reasonable notice of and manifested assent to the online agreement."[51] Specifically regarding browsewrap agreements, courts have held that whether these agreements are valid depends on the website user's "actual or constructive knowledge" of the terms and conditions employed by the site, prior to using it.[52] Thus, to be bound, parties need not have an actual "meeting of the minds."[53] Rather, a reasonable communication of the terms will suffice.[54]

The reasonable communication requirement is a combination "of reasonable notice of the contractual nature of the offered terms and the opportunity to review those terms," which serves as a "proxy for the offeree's clear manifestation of assent."[55] A reasonable communication of

---

or otherwise distribute the content or any modified or altered versions of it, whether over the Internet or otherwise, and whether or not for payment," without the written permission of the website or a third-party copyright holder).

47. Moringiello, *supra* note 39, at 1311.

48. Wayne Barnes, *The Objective Theory of Contracts*, 76 U. CIN. L. REV. 1119, 1119–20 (2008).

49. *See id.* at 1120 (noting that "contract formation depends on what is communicated, not what is merely thought").

50. *Id.* at 1125.

51. Burcham v. Expedia, Inc., No. 4:07CV1963 CDP, 2009 WL 586513, at *2 (E.D. Mo. Mar. 6, 2009) (citing Specht v. Netscape Comm. Corp., 306 F.3d 17, 28–30 (2d Cir. 2002); Feldman v. Google, Inc., 513 F. Supp. 2d 229, 236 (E.D. Pa. 2007)).

52. *Id.* at *3 n.5 (citations omitted).

53. *See* RESTATEMENT (SECOND) OF CONTRACTS § 17 cmt. c (1981) (noting that although the element of agreement in contracts is also known as the "meeting of the minds," "it is clear that a mental reservation of a party to a bargain does not impair the obligation he purports to undertake").

54. *See, e.g.*, Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 429 (2d Cir. 2004) (detailing that by using Register.com's Internet product, the end user received both "notice and presentation of the proposed terms").

55. Moringiello, *supra* note 39, at 1314.

terms gives rise to what is commonly referred to as the offeree's "duty to read."[56] In other words, if the terms of a contract are reasonably communicated, the offeree cannot be absolved from liability for failing to read them because the offeree had a legal duty to do so.[57]

The notice requirement is fulfilled differently for clickwrap agreements and browsewrap agreements.[58] While notice for clickwrap agreements can be satisfied by using code to prohibit a user from proceeding without first having the opportunity to review the contract, notice in browsewrap agreements "is given through the conspicuous display of the contract."[59]

Assent to a contract is typically manifested in the process of offer and acceptance,[60] both of which are demonstrated by "an outward manifestation of intent to be bound."[61] By manifesting intent to be bound by a contract, adherents assume the duty to read.[62] The practical result of this duty is that individuals who objectively agreed to be bound by contract will be deemed to have agreed to all terms contained in the writing, regardless of whether they read the terms or understood them.[63]

Courts appear to have reached a loose consensus in applying standard-form doctrine to online agreements. Courts tend to enforce clickwrap agreements that require an action on the part of the user, but they tend to shy away from enforcing browsewrap agreements that require no outward manifestation of asset.[64] Courts oscillate on "notice sentence browsewraps," which provide users with a link to terms of use but do not require users to acknowledge that they have seen them.[65]

Thus, standard-form contract doctrine on the Web, while controversial, is relatively stable. Courts relying on this doctrine give great weight to the specific language of the terms, often with little regard to other

---

56. *Id.*

57. *See id.* at 1314–15 (observing that courts will typically enforce standard-form contracts so long as the user has notice of the terms, subject to limited exceptions, such as unconscionability).

58. Ian Rambarran & Robert Hunt, *Are Browse-Wrap Agreements All They Are Wrapped Up To Be?*, 9 TUL. J. TECH. & INTELL. PROP. 173, 176 (2007).

59. *Id.*

60. Edith R. Warkentine, *Beyond Unconscionability: The Case for Using "Knowing Assent" as the Basis for Analyzing Unbargained-for Terms in Standard Form Contracts*, 31 SEATTLE U. L. REV. 469, 475 (2008).

61. *Id.*

62. *Id.* at 476.

63. *Id.*

64. Andrea M. Matwyshyn, *Mutually Assured Protection: Toward Development of Relational Internet Data Security and Privacy Contracting Norms*, *in* SECURING PRIVACY IN THE INTERNET AGE 78–79 (Anupam Chander et al. eds., 2008); *see also* Juliet M. Moringiello & William L. Reynolds, *Survey of the Law of Cyberspace: Electronic Contracting Cases 2007–2008*, 64 BUS. LAW. 199, 218 (2008) ("After some early forays into a separate set of legal principles for electronic transactions, it is now clear that common law rules fit them well.").

65. Matwyshyn, *supra* note 64, at 79.

understandings and representations that arise within relationships.[66] These terms have great significance for user privacy, but they do not always reflect the complete understanding between the parties. Professor Mark Lemley criticized online terms of use, stating "more and more courts and commentators seem willing to accept the idea that if a business writes a document and calls it a contract, courts will enforce it as a contract even if no one agrees to it."[67]

B. The Danger of Over-Reliance on Standard-Form Contracts

Courts that solely rely on standard-form contracts threaten user privacy by ignoring other elements of the contractual relationship between the website and user. Of the many ways that standard-form contracts threaten privacy, this section will address liability shields created by a standard-form contract, the problem of presumed consent, and standard-form contracts superseding the weak existing legislation on the issue.

Fundamentally, contracts exist to bind parties to promises by creating legal obligations.[68] On a website, these promises can be made in nearly any form and can appear anywhere. Promises made as part of a negotiation can be more attractive for users; negotiation is typically deliberative, thus negotiated terms are presumably understood and satisfactory to contract adherents. The same cannot regularly be said for terms in standard-form contracts.

Scholars writing about intellectual property, alternative dispute resolution, and limitations on liability have all observed the impact of standard-form contracts.[69] Those areas typically have a standard "default" position in the absence of contractual provisions.[70] If a website's terms of use fail to grant the appropriate licenses, then implied licenses will exist to govern the use of intellectual property, and the parties will retain their rights.[71] If a contract fails to include an arbitration clause, then courts are the default arbiter of disputes. Similarly, the Uniform Commercial Code

---

66. *See, e.g.*, cases cited *supra* note 1 (noting that courts look to the language of the privacy policy to determine whether the right to privacy was waived).

67. Lemley, *supra* note 28, at 459.

68. E. ALLAN FARNSWORTH, CONTRACTS § 1.1, at 4 (1999); *see also* RESTATEMENT (SECOND) OF CONTRACTS § 1 (1981) (defining a contract as "a promise or a set of promises for the breach of which the law gives a remedy, or the performance of which the law in some way recognizes as a duty").

69. *See* Barnes, *supra* note 44, at 1547–48; Lemley, *supra* note 28, at 459–62.

70. *See generally* Ian Ayres & Robert Gertner, *Filling Gaps In Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 87 (1989) (postulating that default rules serve as gap-fillers in contracts that are incomplete); Robert E. Scott, *A Relational Theory of Default Rules for Commercial Contracts*, 19 J. LEGAL STUD. 597, 598 (1990) (describing the debate regarding default rules).

71. *See, e.g.*, Lemley, *supra* note 28, at 477.

(UCC) provides guidance for warranties and disclaimers.[72] Yet, the law regarding the default status of self-disclosed information online is inconsistent and unpredictable.[73] Thus, for good or bad, contracts that address privacy issues provide a degree of clarity.[74]

Duties of confidentiality may also extend to websites when they promise to protect users. These promises can often be found in a website's privacy policy. Privacy policies explain how a website will use a visitor's personal information.[75] While privacy policies, standing alone, are seen as unenforceable statements of policy, many websites incorporate the policy into their terms of use so that it binds users.[76] According to Professor Allyson Haynes, although privacy policies typically include "a slew of terms both relating to privacy . . . and relating to other rights of the consumer,"[77] many prominent court decisions addressing breach of contract claims arising from privacy policies have not enforced the privacy policy against the website owner.[78]

According to Haynes, such binding policies can actually provide a liability shield for companies looking to take advantage of users' failure to

---

72. *See* U.C.C. § 2–313 (1999) (describing the creation of express warranties); *see also* Warkentine, *supra* note 60, at 526.

73. *See* Woodrow Hartzog, *Promises and Privacy: Promissory Estoppel and Confidential Disclosure in Online Communities*, 82 TEMP. L. REV. 891, 891 (2009) (voicing that traditional remedies usually fail in online privacy claims); Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 921 (2005) (discussing how different states can have drastically different takes on individual privacy protection for information on social networks).

74. *See, e.g.*, Pamela Samuelson, *Privacy As Intellectual Property?*, 52 STAN. L. REV. 1125, 1127 (2000) (citing PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 8 (1998)). Swire and Litan took notice of this leverage, stating:

> Consider the incentives of a company that acquires private information. The company gains the full benefit of using the information in its own marketing efforts or in the fee it receives when it sells the information to third parties. The company, however, does not suffer losses from the disclosure of private information. Because customers often will not learn of the overdisclosure, they may not be able to discipline the company effectively . . . . It can be daunting for an individual consumer to bargain with a distant Internet merchant . . . about the desired level of privacy.

Id.

75. Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN ST. L. REV. 587, 594 (2007).

76. *Id.* at 596.

77. *Id.* at 597.

78. *See, e.g.*, *In re* Jet Blue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 316–17 (E.D.N.Y. 2005) (examining an airline's privacy policy to determine whether plaintiffs had a claim for reliance); Dyer v. Nw. Airlines Corp., 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004) (finding that plaintiffs failed to allege that they read, understood or relied upon the privacy policy and thus failed to allege contractual damages); *In re* Nw. Airlines Privacy Litig., No. Civ. 04-126(PAM/JSM), 2004 WL 1278459, at *6 (D. Minn. June 6, 2004) (finding that the privacy statement did not constitute a unilateral contract and that plaintiff must have read the policy to rely on it).

read by selling or sharing users' personal information.[79] The policies essentially allow websites to track and exploit user information.[80] Even users who attempt to educate themselves about websites' privacy policies often do not fully understand the policies and the powers they give websites regarding the use of personal information. Professor Nancy Kim observed that websites may respond to customer ignorance or inaction by inserting increasingly more aggressive and intrusive terms in "'wrap contracts."[81] A number of lawsuits have been filed by website users claiming breach of contract and promissory estoppel resulting from a website's violation of its privacy policy, with mixed results.[82]

Applying a strict standard-form contract analysis, a number of courts have denied any meaningful recovery for a website breaking promises it made in a privacy policy.[83] As will be discussed in Part II, by focusing solely on language in the terms, courts are excluding aspects of the relationship between the user and the website that could aid in the interpretation of vague terms in the policy or give rise to additional implied promises of confidentiality.[84]

Another danger of standard-form contracts, and one of their most powerful uses, is obtaining user consent.[85] This consent is often relied upon by websites when they deploy "spyware"—software that collects and transmits personal information and is often surreptitiously downloaded

---

79. Haynes, *supra* note 75, at 588.

80. KIM, *supra* note 30, at 1.

81. *Id.*

82. *E.g.*, Complaint at 18–19, Strickland-Saffold v. Plain Dealer Publ'g Co., No. CV-10-723512 (Ohio Ct. Com. Pl. Apr. 7, 2010), *dismissed by plaintiffs*, Notice of Dismissal with Prejudice Under Rule 41(A)(1)(a) of the Ohio Rules of Civil Procedure (Dec. 30, 2010); *cf.* McVicker v. King, 266 F.R.D. 92, 97 (W.D. Pa. 2010) (denying motion to compel a website's anonymous users' identities); Sedersten v. Taylor, No. 09-3031-CV-S-GAF, 2009 WL 4802567, at *3 (W.D. Mo. Dec. 9, 2009) (denying motion to compel anonymous poster's identity from a news website).

83. *See, e.g.*, *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d at 327 (holding that the plaintiffs had no reasonable expectation to be compensated for their personal information and therefore could not sustain their breach of contract claim); *Dyer*, 334 F. Supp. 2d at 1200 (finding that plaintiffs failed to allege that they read, understood, or relied upon the privacy policy and failed to allege contractual damages); *In re Nw. Airlines Privacy Litig.*, 2004 WL 1278459, at *6 (finding that the privacy statement did not constitute a unilateral contract and that plaintiff must have read the policy to rely on it).

84. *See also* McClurg, *supra* note 19, at 888 (discussing the threat to intimate relationships posed by the Internet and lack of enforcement of the public disclosure tort); Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 156–58 (2007) (arguing that the breach of confidentiality tort has been limited, not reaching its potential).

85. Andrea M. Matwyshyn, *Technoconsen(t)sus*, 85 WASH. U. L. REV. 529, 548 (2007) ("The legal nexus of digital consent is contract law. For many bodies of law, the technology revolution has added a complicating factor to the legal equation; in contract law, the uneasy peace of doctrine around form contracts/contracts of adhesion has been permanently disrupted.").

onto an individual's computer.[86] According to Professor Wayne Barnes, consumer assent to spyware installation is rarely debated, but in truth "the privacy implications of spyware are profound."[87] Individuals typically receive some modest benefit, such as software that entertains or offers a service, and as consideration, the user agrees to let the program install spyware.[88]

Central to the issue of consent is the possible failure of the users to adequately understand the consequences of their consent—or to recognize that they are consenting to anything at all.[89] The significance of an individual's contractual consent stretches beyond the actions and remedies in contracts and into statutes, common law, and even constitutional law.[90] But consent can also frustrate a user's claim for breach of contract. By looking only at the terms providing for consent to the collection and use of information,[91] courts potentially exclude elements important for valid consent. For example, did the website promise to respect a user's privacy preferences? If so, has the user revoked consent to the collection or use of certain pieces of information by expressing those preferences? Additionally, was the website designed in such a way as to frustrate or corrupt consent to the proposed terms?

Because online agreements are typically drafted to protect the website, they often have a negative effect on a website user's privacy.[92] Most privacy disputes involving online agreements look to the "consensual" aspect of the agreement.[93] Judges have struggled to support the privacy interests of individuals when those individuals have consented to surveillance, collection, or use of their information.[94]

---

86. Barnes, *supra* note 44, at 1545.
87. *Id.* at 1547.
88. *Id.*
89. *See id.* at 1595, 1597 (explaining that hardly any users bother to read or fully understand privacy agreements).
90. *See generally* Matwyshyn, *supra* note 85, at 531–32 (introducing the legal "noise" created by crossing legal disciplines). Matwyshyn proposed a "reasonable digital consumer" standard of consent created through empirical research instead of the current standard, which is something of a legal fiction.
91. *See infra* note 98 (highlighting cases where courts have looked to the terms of use in their decisions).
92. BONNEAU & PREIBUSCH, *supra* note 32, at 24 (explaining that privacy policies often reserve the right for websites to collect user data, such as IP addresses, while giving few meaningful rights to users); Barnes, *supra* note 44, at 1545 (noting that online agreements often include provisions in which users "consent" to have spyware placed on their computers); Woodrow Hartzog, *The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?*, 15 COMM. L. & POL'Y 405, 414 (2010) (asserting that users often have little understanding of what they are agreeing to because online agreements are typically long and filled with legalese).
93. *Cf.* Barnes, *supra* note 44, at 1571 (noting that virtually all existing or proposed laws applicable to spyware contain an element of consent).
94. *See infra* notes 98–99.

Courts vary in requiring that an individual have read a contract to effectuate consent, depending on the kind of legal challenge.[95] In Fourth Amendment disputes, most courts seem to hold users to their "duty to read."[96] Yet the Federal Trade Commission (FTC) has, in at least one dispute, held that, despite manifesting objective consent to be bound by an agreement, a website's failure to present terms that impact an individual's privacy clearly and conspicuously constituted an unfair and deceptive trade practice.[97]

However, many courts have typically found that terms of use can dispel an expectation of privacy regardless of whether the user actually read the terms.[98] Terms of use can also be used as evidence to destroy a user's anonymity.[99] Jonathan Sobel, Karen Petrulakis, and Denelle Dixon-Thayer have noted that the failure to enact an all-encompassing statutory regime to protect privacy has resulted in Congress turning to the contractual "concepts of notice, opt-out, and information access to protect privacy rights."[100] Contracts can also grant consent for activity otherwise prohibited by statute, such as government surveillance.[101] Ultimately, this patchwork of legislation reveals that standard-form contracts serve as the catalyst for a great deal of statutory provisions that can affect a user's

95. *See supra* note 78 (identifying cases where courts looked to whether the plaintiffs had read the agreements entered into).

96. *See, e.g.*, United States v. Hart, No. 08-109-C, 2009 WL 2552347, at *18 (W.D. Ky. Aug. 17, 2009) (finding the plaintiff's expectation of privacy destroyed by the terms of Yahoo!'s privacy policy); Lukowski v. County of Seneca, No. 08-CV-6098, 2009 WL 467075, at *10 (W.D.N.Y. Feb. 24, 2009) (noting that while users may have a subjective expectation of privacy, the terms of the service agreement are relevant to determine the objective expectation of privacy).

97. *See* Complaint at 5, *In re* Sears Holdings Mgmt. Corp., F.T.C. Docket No. C-4264 (F.T.C. Aug. 31, 2009), *available at* http://www.ftc.gov/os/caselist/0823099/index.shtm.

98. *See, e.g.*, Warshak v. United States, 532 F.3d 521, 526–27 (6th Cir. 2008) (discussing the various forms of terms and the resulting change in expectations of privacy); *Hart*, 2009 WL 2552347, at *18 (finding the plaintiff's expectation of privacy destroyed by the terms of Yahoo!'s privacy policy); *Lukowski*, 2009 WL 467075, at *10 (noting the importance of terms in a subscriber agreement in determining the expectation of privacy).

99. *See* Sony Music Entm't Inc. v. Does 1–40, 326 F. Supp. 2d 556, 566–67 (S.D.N.Y. 2004) (holding there was only a minimal expectation of privacy under the ISP's terms of service).

100. Jonathan K. Sobel et. al., *The Evolution of Data Protection as a Privacy Concern, and the Contract Law Dynamics Underlying It*, *in* SECURING PRIVACY IN THE INTERNET AGE 55, 57 (Anupam Chander et al. eds., 2008).

101. *See, e.g.*, Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 322 (2004) (explaining how websites protect non-copyrightable data through the terms agreed to by users to access the websites); Llewellyn Joseph Gibbons, *It's Nobody's Business, But You Still Cannot Lie About It: Criminalizing Innocent Attempts to Maintain Cyber-privacy*, 30 OHIO N.U. L. REV. 377, 382–83 (2004) (discussing the implications of lying about one's identity after consenting to terms to obtain access under the Computer Fraud and Abuse Act); Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1596 (2003) (explaining how breach of contract may now criminalize contract law on the Internet).

privacy. As a result, there has never been a greater need for enhanced scrutiny of online agreements.

II. THE CONTRACTUAL SIGNIFICANCE OF WEBSITE DESIGN

Courts should no longer ignore the contractual significance of website design. Standing alone, interactive features of a website might be little more than bells and whistles. However, many websites make user privacy and, by extension, user privacy settings, a central feature of the user's experience and a prominent part of the terms of use. Because websites that employ these features are in a contractual relationship with their users, website design should be part of an online agreement when it is incorporated into or consistent with the terms of use.

Contracts were a part of everyday life long before the Internet, but they were largely formed in the commercial or transactional contexts—not in the contexts of social interaction and media consumption.[102] After all, when one turns on the television, listens to the radio, or reads a newspaper, contractual relationships are not formed. Every time one picks up the phone or gossips in the hallway, no one presents long and confusing terms dictating what kinds of communications are acceptable. Yet virtually every time individuals access a website, they are asked to agree to a cadre of terms against which their only recourse has been simply to close their browser or go to a different website.

As our experience online grows richer, our relationships with websites and other website users become more nuanced. Courts should better consider these nuances and the context in which information is disclosed when interpreting online agreements. This section explores the under-analyzed elements of online agreements that exist outside of websites' explicit terms of use and privacy policies. Recognition of these elements—code-based promises, malicious interfaces, and the operational reality of the contracting parties—could reduce the schism between contracts as a source of, and solution for, privacy problems online.

The threats to privacy posed by online agreements are created by the same problem inherent in employing contracts as a solution to regulate privacy: lack of meaningful choice.[103] Professor Jerry Kang recognized

---

102. *See generally* Raymond T. Nimmer, *Breaking Barriers: The Relation Between Contract and Intellectual Property Law*, 13 BERKELEY TECH. L.J. 827, 832 (1998) (recognizing that the underlying purpose of contracts is to conduct commerce and transactions).

103. *See, e.g.*, DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 105–06 (2004) (arguing that providing people with opt-out rights and privacy policies does not give those people control); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1464, 1502 (2000) (stating that total secrecy is impractical today and expecting individuals to contract for confidentiality is unrealistic); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1229

this hurdle, stating "[t]he strongest challenge to the market solution [to privacy harms] is that 'consent' is coerced and not truly voluntary in the marketplace."[104] This coercion essentially forces users to relinquish control of their personal information, even when they would rather not.[105] Although website users can reject the contract wholesale, the choice becomes meaningless when services, important information, and social networks are only available on a single website. For example, Facebook users cannot re-create their network on a different social network website without convincing the other Facebook users to leave as well.

That a pure standard-form contracts approach to protecting privacy leaves little opportunity for meaningful choice does not mean that the contractual approach to protecting privacy should be abandoned. Rather, a more nuanced contractual approach that provides users with the ability to tailor the contract to suit them could be beneficial.[106] Such flexibility affords users a meaningful choice.[107] Indeed, Professor Pamela Samuelson stated that contracts as a legal tool provide flexibility to "accommodate the multiple interests people have in personal information, the contextual nature of determinations about the appropriateness of collection or use of personal data, the significance of consent as a factor in determining appropriate uses, and the evolutionary nature of social understanding about information privacy."[108] On the Internet, individuals can exercise a higher degree of control over personal data.[109]

Before this level of control may be exercised, however, new practices must be put into place.[110] According to Professor Matwyshyn, the "new legal construction should be inherently relational; it should create confluence of interests in data security between content providers and users and better reflect the commercial value of user data."[111]

While consent to the use of personal information is regularly found in terms of use via an omnibus or blanket level of assent to *all* terms,[112] it typically remains a legal fiction. Most individuals simply do not read the

---

(1998) (explaining how user information can be tracked with detail as standard elements of browsing the Internet); William McGeveran, Note, *Programmed Privacy Promises: P3P and Web Privacy Law*, 76 N.Y.U. L. REV. 1812, 1818–20 (2001) (noting the ease in which personal data can be collected on the Internet because of its characteristics).

104. Kang, *supra* note 103, at 1265.

105. *Id.*

106. *See* Steven A. Bibas, Annual I.H.S.–Eberhard Student Writing Competition Winner, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591, 609 (1994).

107. *Id.*

108. Samuelson, *supra* note 74, at 1172.

109. *Id.*

110. Matwyshyn, *supra* note 64, at 74.

111. *Id.*

112. *See supra* notes 23, 25.

terms,[113] and even if they did, most individuals have difficulty fully comprehending what they actually agreed to and the risk they inherited by that consent.[114] Broad, sweeping agreements that control the use of personal information lack the specificity to be truly effective in providing meaningful control over the flow of personal information because users often disclose both sensitive and innocuous personal information on the same website.

Privacy-related agreements could be much more effective on a micro-level. Smaller, discrete agreements for confidentiality regarding specific pieces of information could be more effective than one all-encompassing agreement regarding the protection of personal information. Because individuals do not consider all information they disclose to be uniformly public or private, it is not surprising that contracts forcing them to do just that are of limited effectiveness.[115] This Article offers three related suggestions for the analysis of online agreements. These proposals are not advocating extreme modifications to established rules of contract formation and interpretation. Rather, they are suggestions for a magnified examination of the true relationship between websites and users.

First, courts should broaden their consideration of what constitutes a promise by better recognizing when websites have clearly offered to keep information confidential through website design, icons, or features.[116] For example, in some contexts, features such as privacy settings or icons such as padlocks could reasonably be perceived as offers by the website to protect certain pieces of information. Second, courts should better recognize the role that malicious website interfaces play in invalidating true agreements between the parties.[117] Features such as misleading links, disabled back buttons, unnecessary and confusing forms, and pop-ups covering desired content could all frustrate contract formation. Third, if

---

113. *See* JOSHUA GOMEZ ET AL., KNOWPRIVACY 11 (2009), *available at* http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf (stating that privacy policies are not usually read, in part, because users cannot understand them); Lee Goldman, *Contractually Expanded Review of Arbitration Awards*, 8 HARV. NEGOT. L. REV. 171, 192 (2003) (believing that consumers will not read disclosures or form agreements but will simply sign where told to sign); Rakoff, *supra* note 26, at 1179 (finding a near universal scholarly and empirical consensus that consumers do not read contracts prior to signing them); Sobel, *supra* note 100, at 66 (noting that contract law is an imperfect tool because most contracts are not usually read); Warkentine, *supra* note 60, at 469 (introducing the article with the statement that standard-form contracts are rarely read by their signers).

114. *See* Shmuel I. Becher, *Behavioral Science and Consumer Standard Form Contracts*, 68 LA. L. REV. 117, 121 (2007) (finding that consumers are unlikely to give the terms the full meaning and importance they deserve).

115. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 125–26 (2010) (arguing against what she refers to as the "public/private" dichotomy).

116. *See infra* Part II.A.

117. *See infra* Part II.B.

online agreements are offered as evidence in privacy disputes, courts should not limit their analysis to the explicit terms of use. Instead, courts should consider the "operational realities" outside of the terms of use that induced reliance on a promise of confidentiality, such as whether other parts of the website either contradicted the terms or filled in ambiguous terms.[118]

A. Design as Promise

A promise does not have to be in words to be binding.[119] A promise can be any "manifestation of intention to act or refrain from acting in a specified way, so made as to justify a promisee in understanding that a commitment has been made."[120] Promises as part of an otherwise valid contract or one detrimentally relied upon can be enforced by law.[121]

It is puzzling that courts have focused almost entirely on the language in terms of use and privacy policies when analyzing online agreements. Those terms are not the only reasonably perceived promises in a website. In some contexts, website code—page design, icons, or features—can reasonably be perceived as an offer or promise by the website to protect certain pieces of information.

1. Privacy indicators

A growing body of literature in the field of human-computer interaction has focused on what are known as "privacy indicators"—designs such as logos, icons, settings, and seals used to intuitively convey a website's policy regarding collection and use of personal information.[122] For

---

118. *See infra* Part II.C.

119. *See* RESTATEMENT (SECOND) OF CONTRACTS § 4 (1981) ("A promise may be stated in words either oral or written, or may be inferred wholly or partly from conduct."); *id.* § 19(1) ("The manifestation of assent may be made wholly or partly by written or spoken words or by other acts or by failure to act."); *see also* McClurg, *supra* note 19, at 912–13 (stating promises can be inferred from conduct).

120. RESTATEMENT (SECOND) OF CONTRACTS § 2(1) (1981).

121. *See id.* §§ 2(1), 90(1) (outlining that a promise may be a manifestation of intention, such as a provision in a contract or which the promisor should reasonably expect to induce action or forbearance).

122. *See* SERGE EGELMAN ET AL., STUDYING THE IMPACT OF PRIVACY INFORMATION ON ONLINE PURCHASE DECISIONS 1 (2006) (describing P3P privacy policies and the use of Privacy Finder to identify websites with privacy settings matching a user's preferences); SERGE EGELMAN ET AL., TIMING IS EVERYTHING? THE EFFECTS OF TIMING AND PLACEMENT OF ONLINE PRIVACY INDICATORS 1 (2009) (observing that consumers took into account privacy indicators, when available, when purchasing from websites); JULIA GIDEON ET AL., POWER STRIPS, PROPHYLACTICS, AND PRIVACY, OH MY! 1 (2006) (finding that privacy policy comparison information had an impact on non-privacy-sensitive purchases but more influence on privacy-sensitive purchases); JANICE TSAI ET AL., SYMBOLS OF PRIVACY 2 (2006) (concluding that even ambiguously defined privacy symbols made users more comfortable with doing business with a website); Lorrie Faith Cranor, *What Do They "Indicate?" Evaluating Security and Privacy Indicators*, INTERACTIONS, May–June 2006, at 45 (noting the disappointing effectiveness of privacy indicators because of the ease in

example, padlock icons located in the bottom right corner of web browsers often indicate the presence of a secure sockets layer (SSL) connection between the browser and a website.[123] Similar padlock icons are used on Facebook to indicate that certain settings have been adjusted to restrict access to, or otherwise protect, information.[124] A number of websites employ "privacy seals" like TRUSTe to assure users of the website's responsible privacy practices.[125] Amazon.com allows users to create a public profile and "private wish lists." Amazon reinforces the confidential nature of these private lists by encouraging users to also create lists that friends can see.[126] Twitter provides that only followers approved by the user will receive a user's tweets when giving users the option to protect their disclosures.[127] (Is Twitter representing that they will not share these protected disclosures with any other parties? After all, Twitter did not include "protected tweets" when they gave the Library of Congress every tweet from every public account for archival.[128])

These indicators are designed to improve consumer confidence and instill consumer trust in a website's privacy practices.[129] Researchers like Victoria Groom, M. Ryan Calo, and Alessandro Acquisiti have found that many of these icons can elicit a visceral response from website users.[130] Calo has observed how anthropomorphic features in code can affect a user's perception of website privacy because "[h]uman-computer interfaces

---

fooling humans). A full explication of code-based promises is outside the scope of this Article but will be addressed in future research.

123. Cranor, *supra* note 122, at 45.

124. *Help Center*, FACEBOOK, http://www.facebook.com/home.php#!/help/?ref=pf (last visited Aug. 9, 2011) (representing the "Safety Center" link with a padlock).

125. EGELMAN ET AL., TIMING IS EVERYTHING? THE EFFECTS OF TIMING AND PLACEMENT OF ONLINE PRIVACY INDICATORS, *supra* note 122, at 2.

126. *Making Your Wish List Searchable*, AMAZON.COM, http://www.amazon.com/gp/help/customer/display.html?nodeId=501094 (last visited Aug. 9, 2011); *Your Account*, AMAZON.COM, https://www.amazon.com/gp/css/homepage.html?ie=UTF8&ref_=topnav_ya (last visited May 21, 2011).

127. *Account Settings*, TWITTER, http://twitter.com/settings/account (last visited Aug. 9, 2011).

128. *See* Benny Evangelista, *Tweets Preserved for All Time Under Library of Congress Deal*, SFGATE, Apr. 16, 2010, http://articles.sfgate.com/2010-04-16/business/20851780_1_tweets-biz-stone-library ("The only exceptions are tweets from a small percentage of protected accounts.").

129. EGELMAN ET AL., TIMING IS EVERYTHING? THE EFFECTS OF TIMING AND PLACEMENT OF ONLINE PRIVACY INDICATORS, *supra* note 122, at 2; TSAI ET AL., *supra* note 122, at 1.

130. *See* VICTORIA GROOM & M. RYAN CALO, USER EXPERIENCE AS A FORM OF PRIVACY NOTICE: AN EXPERIMENTAL STUDY (forthcoming 2011) (on file with author); M. Ryan Calo, *Against Notice Skepticism*, 87 NOTRE DAME L. REV. (forthcoming 2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1790144 (fearing that most adults who see the terms "privacy policy" assume the website safeguards information, regardless of the website's actual practice); Leslie K. John, Alessandro Acquisti & George Lowenstein, *Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information*, 37 J. OF CONSUMER RES. 858, 868 (2011) (finding that privacy concern was incommensurate with the objective dangers of disclosure).

that introduce an apparent person at the site of collection may resolve the notice [of a privacy threat] problem in a direct and more salient way: through a visceral reminder that the data being collected will be used and shared."[131] Judges should better recognize that users exposed to anthropomorphic features are generally more receptive to the information conveyed and, thus, might internalize that information better than fine-print legalese.

Regardless of accuracy, many users believe that websites with privacy indicators have adopted consumer-friendly practices.[132] A team of researchers from the Annenberg Public Policy Center and the Samuelson Law, Technology, and Public Policy Clinic found in a 2006 study that when users see the term "privacy policy" on a website, "they assume that a web site will not share their personal information."[133]

This research demonstrates that users can perceive (or misperceive) website features, short phrases, icons, and other privacy indicators as representative of a website's privacy promises. In some contexts, these representations should become part of an online agreement. To the extent a website promises in language or in code to respect a user's preferences for privacy, user actions such as deleting information and adjusting privacy settings could be considered acceptances of offers to protect information.

Because users are constrained by code (they generally cannot effectively negotiate with a website using words), the online interaction takes on additional significance. Instead of simply meaning "I wish to delete this information," user activity could mean "I wish to protect this information, so I am accepting your offer to take it down and keep it confidential."

2. Working with the fine print

By failing to recognize code-based promises, courts risk ignoring the many ways that contracts can be formed digitally. Recognition of code-based acceptances, such as use of privacy settings, could also fulfill the desired "modicum of bilaterality" capable of defeating some claims of unconscionability.[134] In light of online communication, many courts are already beginning to deviate from the old theoretical framework[135] and

131. M. Ryan Calo, *People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship*, 114 PENN ST. L. REV. 809, 849 (2010); *see also* Calo, *Against Notice Skepticism*, *supra* note 130.

132. EGELMAN ET AL., TIMING IS EVERYTHING? THE EFFECTS OF TIMING AND PLACEMENT OF ONLINE PRIVACY INDICATORS, *supra* note 122, at 2.

133. TUROW ET AL., *supra* note 7, at 2.

134. *Cf.* Ting v. AT&T, 319 F.3d 1126, 1149 (9th Cir. 2003) (discussing that the "modicum of bilaterality" required in arbitration agreements).

135. Amelia Rawls, Comment, *Contract Formation in an Internet Age*, 10 COLUM. SCI. & TECH. L. REV. 200, 219 (2009) (discussing that businesses are using new technologies to avoid liability and courts have begun to distance themselves from old theoretical

"have endorsed the view that while 'some contracts are formed and their terms fully defined at a single point in time, many transactions involve a rolling or layered process.'"[136] This more nuanced analysis of contract formation could recognize a privacy policy or terms of use as one layer and code-based promises as additional layers of the agreement.

No matter how many layers are perceived, an offer must be included for a contract to be formed. The great contracts scholar Arthur Corbin defined an offer as "an act whereby one person confers upon another the power to create contractual relations between them."[137] Under this Article's proposal, the option provided by the website in code could be interpreted by the courts as an offer to keep information confidential. As discussed previously, the objective theory of contracts holds that it is not the subjective intent of the website that dictates the parties' obligations but rather what the expression of intent objectively *conveys* to the other party.[138] Corbin stated, "[w]hat kind of act creates a power of acceptance and is therefore an offer? It must be an expression of will or intention. It must be an act that leads the offeree reasonably to believe that a power to create a contract is conferred upon him."[139]

This objective expression of intent for website design to be part of a contract can be found in a website's terms of use and privacy policy. Terms of use and privacy policies often explicitly address ways a user can affect a website's collection and use of personal information. For example, Facebook's terms of use agreement limits the scope of the license granted to the website according to the user's privacy and application settings.[140] By incorporating references to the ability to alter personal information in an online agreement, these websites invite acceptance of offers of confidentiality. An offer to keep deleted or protected information confidential need not be explicit to form a contract so long as such a manifestation of intent was otherwise conveyed.[141]

---

frameworks).

136. *Id.* (citing Hill v. Gateway 2000, Inc., 105 F.3d 1147 (7th Cir. 1997); ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996); M.A. Mortenson Co. v. Timberline Software Corp., 998 P.2d 305 (Wash. 2000)).

137. Arthur L. Corbin, *Offer and Acceptance, and Some of the Resulting Legal Relations*, 26 YALE L.J. 169, 181 (1917). Corbin goes on to state that "the act of the offeror operates to create in the offeree a power . . . ; thereafter the voluntary act of the offeree alone will operate to create the new relations called a contract." *Id.* at 181–82.

138. *See* Barnes, *supra* note 48, at 1120 (explaining that, under the modern objective theory, manifestations of intent should be viewed from the point of view of a reasonable person as the other party).

139. Corbin, *supra* note 137, at 182.

140. *Statement of Rights and Responsibilities*, *supra* note 5 (outlining what permissions a user gives to Facebook in relation to the type of content the user provides).

141. *See* RESTATEMENT (SECOND) OF CONTRACTS § 24 (1981) ("An offer is the manifestation of willingness to enter into a bargain, so made as to justify another person in understanding that his assent to that bargain is invited and will conclude it.").

Many privacy policies, such as the one provided by *The New York Times*,[142] are given contractual effect through incorporation into the website's terms of use.[143] *The New York Times* privacy policy, which is part of the website's terms of use agreement, promises not to "share personal information about you as an individual to third parties without your consent."[144] Following that clause, under the heading "Your Privacy Choices," the agreement informs users "[t]o view and edit your personal information, please visit the appropriate part of any of our Web sites."[145] By offering "privacy choices" and promising to disclose only that information consented to by the user, *The New York Times* effectively promises to protect information designated as private by the user.

Promises can come in many forms on a website, but the fine print of privacy policies or terms of use and privacy settings have different effects on users. Users who read or even scan privacy policies are more judicious regarding the disclosure of information,[146] while users who utilize privacy settings tend to disclose *more* information than users who did not.[147] Researchers Fred Stutzman, Robert Capra, and Jamila Thompson have found that both privacy policy consumption and privacy behaviors, such as the utilization of privacy settings, were significant factors affecting disclosure on a social media site. Because privacy policies and code-based features such as privacy settings are intertwined, courts should not ignore these code-based features in their contractual analysis.

Some terms of use explicitly offer to protect the privacy of deleted or protected information. In its terms of use, Myspace promises protection to users who take advantage of privacy protection features, providing:

> After you remove your Content from the Myspace Services we will cease distribution as soon as practicable, and at such time when distribution ceases, the license will terminate. If after we have distributed your Content outside of the Myspace Services, you change the Content's privacy setting to "private," we will cease distribution of such "private" Content outside of the Myspace Services as soon as practicable after you make the change.[148]

Facebook has also given contractual authority to a user's privacy settings

---

142. *Privacy Policy Highlights*, THE NEW YORK TIMES, http://www.nytimes.com/content/help/rights/privacy/highlights/privacy-highlights.html (last updated Apr. 18, 2011).
143. *Terms of Service*, THE NEW YORK TIMES, http://www.nytimes.com/content/help/rights/terms/terms-of-service.html (last updated Mar. 16, 2011).
144. *Privacy Policy Highlights*, *supra* note 142.
145. *Id.*
146. FRED STUTZMAN ET AL., FACTORS MEDIATING DISCLOSURE IN SOCIAL NETWORK SITES 14 (unpublished manuscript) (on file with the author).
147. *Id.* at 14–18.
148. *Terms & Conditions*, MYSPACE.COM, June 25, 2009, http://www.myspace.com/help/terms.

in its statement of rights and responsibilities, stating in the terms of use that "[y]ou own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings" and that "[w]e require applications to respect your privacy."[149] This language could be interpreted to create a contractual obligation to respect a user's privacy preference because it has become a significant aspect of the contract between the user and the website.

Two recent complaints demonstrate how Internet users might perceive indirect privacy settings as promises. The complaint in *Ferguson v. Classmates.com* expresses a user's reliance on a website's promise of confidentiality via privacy settings, terms of use, and privacy policies.[150] This complaint, filed as a class action, asserted that Classmates.com, a school-based social network site, deceptively manipulated users' privacy settings to expose previously "private" profiles in an attempt to generate business.[151] Referring to the ability to protect information through privacy settings and statements made by the website, the complaint alleged that "[t]he promise of confidentiality and the ability of Classmates through various protections to deter unwanted intrusions and harassment have been important to Classmates' ability to attract and retain Users."[152] In the claim for, among other things,[153] breach of contract, the complaint asserts, "Before the recent events described in this Complaint, Classmates' policies did not allow the dissemination of Users' personal information to the general public, through undescribed 'Applications,' or otherwise. The privacy provisions in place when Users subscribed constitute material contractual terms by which Classmates was bound, and remains bound."[154] The inference of contractual obligation arising from promises to respect

---

149. *Statement of Rights and Responsibilities*, *supra* note 5. Facebook's terms of use agreement contains numerous references to the ability to control who sees your information via privacy settings:

> [S]ubject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ("IP License"). . . . You can use your privacy settings to limit how your name and profile picture may be associated with commercial, sponsored, or related content (such as a brand you like) served or enhanced by us. You give us permission to use your name and profile picture in connection with that content, subject to the limits you place.

Id. Yet, arguably, the default for some of the settings is contrary to the spirit of these terms. For example, the "Wall Photos" album is, by default, viewable by everyone. *Who Can See My "Wall Photos" Album?*, FACEBOOK, https://www.facebook.com/help/?faq=20139 (last visited June 3, 2011).

150. Class Action Complaint at 2, 4, Ferguson v. Classmates Online, Inc., No. 2:10-cv-00365-RAJ (W.D. Wash. Mar. 5, 2010).

151. *Id.* at 3.

152. *Id.* at 7.

153. The complaint also asserts claims under the Electronic Communications Privacy Act, the Washington Consumer Protection Act, and unjust enrichment. *Id.* at 13–17.

154. *Id.* at 15–16.

user preferences of privacy lies at the heart of this Article's proposal.

In *Del Vecchio v. Amazon.com, Inc.*,[155] the plaintiffs claimed relief under a theory of, among other things, promissory estoppel for promises to respect privacy settings.[156] The plaintiffs alleged that Amazon.com ignored users' Web-browser privacy settings to fraudulently collect personal information without permission and share it with other companies.[157] Essentially, the plaintiffs asserted they were tricked into believing the site emphasized privacy protection, when in reality the available privacy settings were useless.[158] The users asserted they "reasonably relied upon Amazon's promise to refrain from using cookies to collect PII and share PII with third parties without the user's consent and thereby caused Plaintiffs . . . to choose to visit and make purchases on Amazon's websites."[159]

Some courts have already enforced vague promises of privacy in terms of use and privacy policies. In *McVicker v. King*,[160] for example, the United States District Court for the Western District of Pennsylvania denied a request to compel the disclosure of records that could identify seven anonymous message-board commentators.[161] The plaintiff asserted that the terms of use were too ambiguous to create an expectation of privacy because they did not explicitly provide that the identity of the user would be protected.[162]

The court disagreed, finding instead that the terms of service listed for the blog gave the registered users an expectation of privacy.[163] The terms

---

155. Del Vecchio v. Amazon.com, Inc., No. 2:11-cv-00366-RSL (W.D. Wash. Mar. 2, 2011).

156. Complaint at 23–24, *Del Vecchio*, No. 2:11-cv-00366-RSL.

157. Nick Eaton, *Suit: Amazon Fraudulently Collects, Shares Users' Personal Info*, SEATTLEPI.COM (Mar. 2, 2011, 10:00 PM), http://www.seattlepi.com/business/article/Suit-Amazon-fraudulently-collects-shares-users-1040886.php#ixzz1JEgjzVWO.

158. *Id.*

159. Complaint at 23–24, *Del Vecchio*, No. 2:11-cv-00366-RSL.

160. 266 F.R.D. 92 (W.D. Pa. 2010).

161. *Id.* at 93.

162. *Id.* at 96. The relevant terms were actually located in the website's privacy policy, which was incorporated into the terms of use and stated that the website will use personally identifiable information

> only as permitted by law and [it] may be used to communicate with you about something you have posted, the community agreement, or privacy policy, products or services offered by YourSouthhills.com or the Company, administration of contests, processing e-commerce transactions or other topics the Company believes you may find interesting. Personally identifiable information collected on the Site may also be used for other purposes, including, but not limited to, trouble-shooting and site administration. Certain third parties, our e-mail service provider, for example, may access the information . . . . The Company may also disclose your information in response to a court order, at other times when the Company believes it is reasonably required to do so . . . .

Id. (citation omitted) (internal quotation marks omitted).

163. *Id.*

of use stated: "[p]rotecting consumer privacy online is important to us. By taking steps to protect the privacy of our members, we also hope to increase members' confidence in the site and as a result, increase their online activity."[164] The court found that "[t]he Privacy Policy clearly reflects that Trib Total Media will disclose its users personally identifiable information only in very limited situations" and thus gave users an expectation of privacy.[165] Are the general promises made in privacy policies such as "we will protect your privacy" and "we respect your privacy settings" any clearer than the impressions conveyed by website features that allow users to identify the information they want to protect?

This solution can be distilled to a simple proposition: if a website promises to respect a user's privacy preferences, then a user's expression of privacy preferences through website features like privacy settings should serve to make the website's promise binding. While this proposal is essentially a modified opt-out system, it has several benefits that existing opt-out systems do not. One benefit is that people who do not have time "to read through cumbersome documents describing obscure rules for controlling data"[166] can still protect their privacy. This way, unlike the current opt-out framework that, according to Professor Daniel Solove, "require[s] individuals to check a box, send a letter, make a telephone call, or take other proactive steps to indicate their preferences,"[167] a website user would only need to continue using website features to delete or protect personal information.[168]

Privacy scholars note that one of the largest problems with a contractual approach to privacy is the disparity in bargaining power between the parties.[169] They point out that individuals are largely "contract term takers" in their dealings with organizations[170] and that "[p]eople frequently accede to standardized contract terms without putting up much of a fight."[171]

---

164. *Id.* (internal quotation marks omitted).

165. *Id.*

166. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 160 (1999) (suggesting the creation of an electronic system to negotiate privacy policy terms).

167. SOLOVE, *supra* note 103, at 84; *see also* McGeveran, *supra* note 103, at 1852–53 (discussing whether opt-in mandates are overly burdensome).

168. Facebook has seen most of its users select some form of privacy protection through the privacy settings and ability to un-tag or delete personal information offered by the website. *Cf.* Ana Muller, *Updates on Your New Privacy Tools*, THE FACEBOOK BLOG (Dec. 9, 2009, 3:19 PM), http://blog.facebook.com/blog.php?post=197943902130 (requesting all 350 million users to update their privacy settings). Some websites, like Facebook, already keep track of this kind of information and would only need to quarantine the information and refrain from disclosing it. *Facebook's Privacy Policy*, *supra* note 6 (admitting that Facebook tracks certain actions such as adding connections or creating a photo album).

169. SOLOVE, *supra* note 103, at 82 (recognizing that when faced with a standard contract, individuals tend to accede without much debate or negotiation).

170. *Id.* (citing OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION 9 (1993)).

171. *Id.* (citing Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815,

The modified opt-out proposal offers users more meaningful control over the flow of their personal information notwithstanding standard-form contracts. The contractual leverage could allow users to be more than a passive party in the "meeting of the minds." A reciprocal outcome is not just desirable from a public policy perspective—it also has legal significance in states like California that hold a "modicum of bilaterality" in contracts can help nullify claims of unconscionability.[172]

3. The likelihood of reliance

A modified opt-out solution is grounded in the reliance interest in enforcing contracts. Websites' promises to protect information should be enforced if they induced detrimental reliance. Users virtually never read the terms of use, yet they routinely use privacy settings. Thus, it is likely that website users will rely on representations made by significant features of website design more often than boilerplate terms of use. This is particularly true when terms of use regarding privacy are vague.

One of the maxims of contract law is that ambiguities in contractual terms should be interpreted against the drafter.[173] Websites have the opportunity to craft terms of use, so this rule reflects an attempt to balance the inequities between two contractual parties. Websites have complete control over the ability of users to delete information, utilize privacy settings, and remove identifying tags. If websites choose to make these features available and promise to respect user preferences regarding privacy, should any ambiguities in an online agreement not be interpreted against the coder?

Regarding contractual protection for privacy, Professor Daniel Solove notes that:

> [i]ndividuals are often presented with an all-or-nothing choice: either agree to all forms of information collection and use or to none whatsoever. Such a limited set of choices does not permit individuals to express their preferences accurately. Individuals frequently desire to consent to certain uses of their personal information, but they do not want to relinquish their information for all possible future uses.[174]

The user-action proposal helps alleviate some of the "omnibus" problem posed by vague and expansive language in contracts by allowing users to

---

822–23 (2000)).

172. *See* Ting v. AT&T, 319 F.3d 1126, 1149 (9th Cir. 2003) (holding that contractual terms were unconscionable when they banned class action suits, required telecommunications customers to submit disputes to arbitration, required the customers to split the cost of the arbitration, and required confidentiality).

173. E. ALLAN FARNSWORTH ET. AL., CONTRACTS: CASES AND MATERIALS 600 (6th ed. 2001) ("One of the most time-honored maxims of contract interpretation is that a contract is to be interpreted *contra proferentem* (against its author or profferer).").

174. SOLOVE, *supra* note 103, at 85.

determine what information should be protected on a more granular level, depending on what options are provided by a website.

Ultimately, the user-action proposal simply suggests that courts take a more granular and contextual approach to contracts regarding privacy online. By considering the messages conveyed by website design, courts could recognize the simple micro-agreements and additional promises governing pieces of information.

4. The problems with website design as contract

This proposal is not without weaknesses. Increased website transparency would be required for the user to realize that an agreement with the website had been broken.[175] Damages for these kinds of privacy harms are notoriously difficult to recover.[176] However, a website's failure to adhere to these agreements could be punished by the FTC in the same manner that the FTC pursues those who fail to abide by their own privacy policies.[177] Additionally, the mere threat of a private cause of action could help deter reckless practices regarding a website's disclosure of user information.

Moreover, some evidence exists that users do not always understand exactly what information design features, like privacy settings, protect.[178] Thus, courts would need to make an additional finding as to what expectations of confidentiality or privacy were reasonable given the effectiveness of a particular design element. Such a granular analysis would have to occur on a case-by-case basis, which could be laborious and inconsistent. Although it is not always clear what each design feature protects, evidence that privacy settings are routinely deceiving website users only further supports the assertion that website design could lead to detrimental reliance—a hallmark of contract related doctrines such as

175. *See generally* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 916 (2007) (suggesting that federal guidelines for breach notifications from financial institutions could be used to create a similar system for privacy breaches); Preston Thomas, Comment, *Little Brother's Big Book: The Case for a Right of Audit in Private Databases*, 18 COMMLAW CONSPECTUS 155, 156 (2009) (noting that an audit system would have to start small and be made in a piecemeal manner).

176. *See, e.g.*, Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004) (finding that the plaintiffs failed to allege that they read, understood or relied upon the privacy policy and failed to allege contractual damages); *see also In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 330 (E.D.N.Y. 2005) (failing to find any viable claims against the defendant in relation to the defendant's deceptive practices).

177. *See, e.g.*, Cecilia Kang, *Google, FTC settle privacy case*, WASH. POST, Mar. 31, 2011, at A16 (reporting on a settlement with Google over, among other things, violation of its own privacy policies).

178. *See, e.g.*, MICHELLE MADEJSKI ET AL., THE FAILURE OF ONLINE SOCIAL NETWORK PRIVACY SETTINGS 14 (2011), https://mice.cs.columbia.edu/getTechreport.php?techreportID=1459 (concluding that every study participant had shared unintended information).

promissory estoppel.[179]

Websites might become discouraged from offering these features if they do not want to assume additional contractual obligation. However, websites need not remove privacy settings altogether. To avoid contractual obligation, websites should refrain from incorporating the settings into their terms of use and make clear that the designs, features, and icons should not be seen as promises by the website to protect information and should, therefore, be utilized accordingly. While these disclaimers would frustrate the ability of users to contractually protect their information, they would also clarify the currently vague promises to respect users' privacy. Currently, the fine print of agreements often gives a different impression than the overall user experience. This is an unjust result.

Websites might also make greater use of merger and integration clauses in an attempt to limit all contractual agreements to the standard-form terms of use. Yet the effectiveness of the clauses might be limited because, as previously discussed, privacy and even privacy settings are often explicit and operative aspects of the terms of use.[180]

Courts should look to the specific facts of a dispute to determine what should be inferred from code and user activity. Ambiguous promises might be better informed by looking to the code in the same way that other "offline" ambiguous terms are informed by context.[181] In many instances, interactivity will have no contractual effect. Yet, courts should not ignore code-based features, such as privacy settings, used to earn a user's trust when a website has promised to respect the privacy wishes of its users.

Although the benefit from this proposal might be seen as incremental, it furthers the same interests sought to be covered by a website's privacy policies. It is not burdened with the "omnibus" dilemma whereby one agreement covers all information, regardless of a user's preference regarding specific pieces of personal information.[182] Indeed, benefits can be found even in modest solutions to privacy harms. There may not be one solution to protecting user privacy, but to echo Professor Michael Froomkin, "a smorgasbord of creative technical and legal approaches could make a meaningful stand against what otherwise seems inevitable."[183]

---

179. *See, e.g.*, Hartzog, *supra* note 73, at 891, 894.

180. *See supra* Part I.B.

181. *See, e.g.*, Taylor Energy Co. v. U.S. Dep't of Interior, 734 F. Supp. 2d 112, 122 (D.D.C. 2010) ("Plaintiff correctly argues that '[n]ot all disclosures are created equal; context matters as to whether a limited disclosure places that information in the public domain.'").

182. *See, e.g.*, McGeveran, *supra* note 103, at 1814 (arguing libertarian versus regulatory regimes for privacy protection presents a false dichotomy, supporting a multi-modal and incremental approach).

183. Froomkin, *supra* note 103, at 1466; *see also* Thomas, *supra* note 175, at 156 ("[P]rivacy reform is best approached in small increments that avoid the paralysis

B. Unconscionable Design

While some website features, such as privacy settings, help users control the flow of personal information, other website features might frustrate or confuse users or trick them into disclosing information they did not want to divulge.[184] When considering what parties to a contract "agreed" to, courts should also consider whether a user's actions were induced by a malicious interface. Gregory Conti and Edward Sobiesk, leading researchers on this form of computer deception, define malicious interfaces simply as those that "deliberately violate usable design best practices in order to manipulate, exploit, or attack the user."[185] Malicious interfaces are the inverse of code-based promises. Whereas code-based promises clarify the terms of disclosure regarding a user's information, malicious interfaces confuse them.

A significant motivation for designers to employ malicious interfaces is to gather personal information and obfuscate "legally mandated but undesirable information from the user."[186] Thus, these interfaces are likely to be involved in privacy and contract disputes. To the extent that a malicious interface distorted the agreement between a website and a user, courts should take note of the interference and refuse to give proposed terms, such as user consent, legal effect.

1. Procedural unconscionability of website design

In essence, this Article proposes that courts extend the concept of procedural unconscionability beyond consent to boilerplate terms so as to also apply it to website design features that can affect the online agreement between users and websites. The equitable doctrine of procedural unconscionability was popularized by the UCC but has been expanded in most states to non-sales contracts.[187] Unconscionability is the main tool used by courts to reject some or all terms in standard-form contracts.[188] While "substantive unconscionability" focuses on the substance of the

---

historically associated with comprehensive reform.").

184. *See, e.g.*, *In re* Easysaver Rewards Litig., 737 F. Supp. 2d 1159, 1172 (S.D. Cal. 2010) (involving claims by users of an ecommerce website for, among other things, breach of contract and fraud because the users were allegedly "deceived into authorizing separate charges to their debit cards simply by typing in their e-mail address for a complimentary gift").

185. GREGORY CONTI & EDWARD SOBIESK, MALICIOUS INTERFACE DESIGN: EXPLOITING THE USER 271 (2010), *available at* http://www.rumint.org/gregconti/publications/201004_malchi.pdf (arguing that security and human-computer interaction committees need to come together to fix deceptive designs).

186. *Id.*

187. RESTATEMENT (SECOND) OF CONTRACTS § 208 (1981); Russell Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. CHI. L. REV. 1203, 1256 (2003) (citing Weaver v. Am. Oil Co., 276 N.E.2d 144, 145–48 (Ind. 1971)).

188. Korobkin, *supra* note 187, at 1256.

actual terms, procedural unconscionability focuses on deficiencies in the contract formation resulting from lack of knowledge of some or all of the terms, or lack of voluntariness.[189] Lack of knowledge of the terms can be summarized as "a lack of understanding of the contract terms arising from inconspicuous print or the use of complex, legalistic language, . . . disparity in sophistication of parties, . . . and lack of opportunity to study the contract and inquire about contract terms."[190] Similarly, involuntary assent to a contract may exist where parties have unequal bargaining power, non-negotiable terms exist, and there is a lack of viable options for the weaker party.[191]

As others have called for an empirically created "reasonable digital consumer,"[192] this Article echoes the call for empirical analysis of users and content and proposes that it be extended to the entire user experience. An analysis of the entire experience is necessary because the agreement between a user and a website involves more than boilerplate terms, and thus an examination of unconscionability cannot end at the terms of use.

With respect to privacy, this Article proposes that the significant presence of malicious interfaces should invalidate consent found in terms of use to utilize disclosed information. Additionally, personal information obtained through the use of malicious interfaces should be presumed to be confidential if a user had an expectation of privacy according to a website's terms of use or privacy policy. For example, if Classmates.com promised to respect its users' privacy settings yet made the settings intentionally difficult to use and changed them without notice, the website should be obligated to keep its promise to its users notwithstanding the consent obtained via confusing or modified privacy settings.

2. A taxonomy of malicious interfaces

Courts should consider empirical evidence of user confusion when confronted with a dispute involving a malicious interface. Common examples of malicious interfaces include "misleading links, disabled back buttons, browsers with 'sponsored' default bookmarks, unexpected and unnecessary forms, blinking advertisements, and pop-ups covering desired content."[193] These malicious interfaces often coerce users into disclosing

189. Bank of Ind., Nat'l Ass'n v. Holyfield, 476 F. Supp. 104, 109 (S.D. Miss. 1979) (discussing when a contract is unconscionable and finding the contract at issue unconscionable because it was too one-sided).

190. *Id.* at 109–10 (citations omitted).

191. *Id.*

192. Matwyshyn, *supra* note 85, at 560 (citations omitted).

193. Gregory Conti & Edward Sobiesk, *Malicious Interfaces and Personalization's Uninviting Future*, IEEE SECURITY AND PRIVACY, May–June 2009, at 73, http://www.rumint.org/gregconti/publications/j3pri.pdf (noting that many individuals are tricked or coerced into divulging information they do not intend or do not want to divulge).

private information.[194] Indeed, eleven categories of malicious design techniques have been identified by Conti and Sobiesk: coercion, confusion, distraction, exploiting errors, forced work, interruption, manipulating navigation, obfuscation, restricting functionality, shock, and trick.[195] Nearly all these categories could significantly affect the validity of an agreement between a website and a user.

Several of these malicious interface techniques could invalidate the assent necessary to form an agreement. For example, coercion, defined as "[t]hreatening or mandating the user's compliance,"[196] could require a user to agree to a contract before being allowed to close a screen or otherwise make use of a computer. Such a tactic would leave no viable alternative to agreeing to the terms; thus, no voluntary assent would be present. An interface could also be designed to manipulate navigation toward some manifestation of consent to disclosure and use of information, for example by leading the user to a dead end or on an infinite path,[197] and the placement of desired content or important information deep in a navigation hierarchy.[198] If assent to a contract or consent to collect and use personal information is obtained through manipulated navigation, to what degree is that consent voluntary?

Confusion, defined as "[a]sking the user questions or providing information that they do not understand,"[199] could similarly frustrate contract formation.[200] Confusion tactics can include use of multiple negatives,[201] such as "we promise never to refrain from ever disclosing your information."

Restricted functionality, defined as "[l]imiting or omitting controls that the user needs to accomplish a task,"[202] could also serve to invalidate assent to an agreement.[203] For example, while not allowing a user to proceed

---

194. *Id.*

195. CONTI & SOBIESK, *supra* note 185, at 272. A full explication of this taxonomy's application to contract law is outside the scope of this Article, but will be addressed in future research.

196. *Id.* at 273.

197. *See id.* (listing as a representative instance "[a]sking a (near infinite) number of questions to get a 'free' iPod").

198. See *id.* (listing as a representative instance "[m]aking the free version of an application far more difficult to find than the commercial version on a consumer firewall vendor's website").

199. *Id.*

200. *Id.*

201. *Id.*

202. *Id.*

203. *Id.* (separating "Restricting Functionality" into two smaller categories—"Omit necessary controls" and "Hide desired interface elements"). Conti and Sobiesk provide as representative instances "[r]emoval of 30 second skip button on TiVo remote control, lack of video download option at a video sharing site, pre-checked mailing list selections (but no 'unselect all' option)," and placing the print button at an obscure location on a webpage to increase ad viewing times. *Id.*

using a website without agreeing to the proposed terms would not be malicious—and under current doctrine would serve to form a valid agreement—certain features such as forcing a user to accept an agreement or lose certain pieces of information could invalidate consent.[204]

Interfaces that obscure information or manipulate navigation have already been considered significant, or even dispositive, by some courts in analyzing electronic agreements.[205] In one of the most prominent browsewrap cases, *Specht v. Netscape Communications Corp.*,[206] the Second Circuit refused to enforce terms of use where "[t]he sole reference to [the terms] was located in text that would have become visible to plaintiffs only if they had scrolled down to the next screen."[207] Thus, if links to terms of use are buried at the bottom of a website or anywhere where they are unlikely to be seen, courts have refused to find notice of terms sufficient to form a contract.[208] The *Specht* decision was an excellent example of judicial recognition of a malicious interface, but it should be seen as only the beginning of the exploration regarding how website design can affect contract formation.

Yet these are not the only types of malicious interfaces that can invalidate notice of terms. Interfaces employing distraction and interruption techniques could also serve to invalidate the notice required for contract formation. Distracting video, animation, blinking, color, and motion could attract the user's attention away from inconspicuously presented terms by exploiting perception, particularly pre-attentive processing.[209] Overly large "hot" regions for ads and other rollover design

---

204. *Id.*

205. *See In re* Easysaver Rewards Litig., 737 F. Supp. 2d 1159, 1172 (S.D. Cal. 2010) (accepting at the pleading stage of litigation as plausible that the plaintiffs "were deceived into authorizing separate charges to their debit cards simply by typing in their e-mail address for a complimentary gift"); Nordberg v. Trilegiant Corp., 445 F. Supp. 2d 1082, 1088, 1098 (N.D. Cal. 2006) (finding that the plaintiffs adequately pled claims against a rewards program where consumers claimed they had been automatically enrolled in a membership program through a pop-up advertisement, without their consent, that charged fees unless the consumer affirmatively canceled the program).

206. 306 F.3d 17 (2d Cir. 2002).

207. *Id.* at 23.

208. *See, e.g.*, Hines v. Overstock.com, Inc., 668 F. Supp. 2d 362, 367 (E.D.N.Y. 2009) (holding that the plaintiff lacked knowledge of the terms of service because the website did not prompt her to scroll down to read them), *aff'd*, 380 F. App'x 22 (2d Cir. 2010); Druyan v. Jagger, 508 F. Supp. 2d 228, 237 (S.D.N.Y. 2007) (enforcing terms of service when such terms were clearly conspicuous); Recursion Software, Inc. v. Interactive Intelligence, Inc., 425 F. Supp. 2d 756, 787 (N.D. Tex. 2006) (taking into account the license agreements were neither long nor buried).

209. CONTI & SOBIESK, *supra* note 185, at 273; *see also* Complaint at 15, FTC v. Pereira (E.D. Va. June 20, 2007), *available at* http://www.ftc.gov/os/caselist/9923264/990922comp9923264.shtm (alleging an unfair and deceptive trade practice by the defendant, which allegedly "uses technical tricks and thievery to drive consumers to defendant WTFRC's sexually-explicit, adult-oriented Web sites," which the consumer then has difficulty leaving because WFTRC manipulated functions of Internet browsers).

elements could interrupt the contract formation process or obstruct the presented terms.

Malicious interfaces must be considered in context to determine their significance. Much like the factors to be considered in a fair-use analysis, the existence of a malicious interface should not automatically invalidate a contract. Rather, it should be balanced with other evidence of contract formation. Clear, non-malicious interfaces should be entitled to a rebuttable presumption of valid consent in light of an otherwise clear manifestation. However, the presence of a number of malicious interfaces (or a single significantly malicious interface) should receive a strong presumption of invalidity with regard to the disputed or operative element enabled through the interface.

C. Design as Evidence of Subsequent Agreement

When online agreements are offered as evidence in non-contractual privacy disputes, courts should avoid treating the text of terms of use as dispositive.[210] Instead courts should consider the terms in conjunction with other evidence, such as whether the contract was enforceable and whether other representations were made to the user explicitly, implicitly, or by virtue of their relationship.[211] These additional considerations could provide a better picture of what one court has dubbed the "operational reality" of the relationship between the user and the website.[212]

In *Quon v. Arch Wireless Operating Co.*,[213] city police department employees brought a number of claims, including a Fourth Amendment violation, against the city in connection with the department's review of employees' text messages.[214] Although the employees signed a general "Computer Usage, Internet and E-mail Policy," which provided that "[u]sers should have no expectation of privacy or confidentiality when using these resources," the Ninth Circuit found that the "operational

---

210. *Cf.* United States v. Hart, No. 08-109-C, 2009 WL 2552347, at *25 (W.D. Ky. Aug. 17, 2009) (finding that because the defendant consented to the terms of use, "it is difficult to conclude that [the defendant] had an actual expectation of privacy in the contents of any communications sent or received with his Yahoo! accounts").

211. James Grimmelmann has asserted that "when users make privacy choices using Facebook's technical controls, they're expressing expectations about who will and won't see their information, and society should treat those expectations as reasonable for Fourth Amendment purposes." James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1197 (2009).

212. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 907 (9th Cir. 2008) (holding that the operational realities of a police department's privacy policy gave police officers a reasonable expectation of privacy even though the written department policy specifically negated any expectation of privacy), *rev'd on other grounds sub nom.* City of Ontario v. Quon, 130 S. Ct. 2619 (2010).

213. 529 F.3d 892 (9th Cir. 2008), *rev'd sub nom.* City of Ontario v. Quon, 130 S. Ct. 2619 (2010).

214. *Id.* at 898.

reality" at the department regarding privacy in electronic messages reflected a different intent on the part of the police department.[215] The employees' superiors made it clear they would not audit messages so long as any additional costs for overage were paid for by the employees.[216] The court found the employees' reliance on this "informal policy" was reasonable, and as a result, the employees "had a reasonable expectation of privacy in the text messages archived in Arch Wireless' server."[217]

Courts should adopt the strategy employed by the Ninth Circuit in *Quon* when analyzing evidence of contracts in privacy disputes. By considering contextual factors such as informal policies or other representations made by websites, courts avoid an unjust application of contract law in situations where individuals reasonably relied on representations outside of the terms of use. Although the Supreme Court reversed the Ninth Circuit's decision in *Quon*,[218] the justices did not significantly address the "operational reality" approach taken by the Ninth Circuit. Professor Solove has suggested guidelines for courts when confronted with an agreement that could govern privacy expectations:

> (1) If the official policy clearly covers the practice at issue, and is specific in referencing it, then there should be a strong presumption it should govern. This presumption can be overridden only when there is a consistent policy to the contrary demonstrated by clear and convincing evidence based on the employer's statements and practices. (2) If the official policy is general in nature, and doesn't specifically reference the practice at issue, then there should be a weak presumption it should govern. This presumption can be overridden when there is a preponderance of evidence demonstrating a different policy with regard to the practice at issue.[219]

These guidelines could inform courts when determining the evidentiary value of online agreements in privacy-related disputes. If, in the course of an ongoing relationship with a website, representations regarding confidentiality and a user's control over the flow of information are made clear to the user, a user should be able to reasonably rely on them. [220]

---

215. *Id.* at 896.
216. *Id.* at 907.
217. *Id.*
218. City of Ontario v. Quon, 130 S. Ct. 2619, 2624 (2010); *see also* CX Digital Media, Inc. v. Smoking Everywhere, Inc., No. 09-62020-CIV, 2011 WL 1102782, at *11–12 (S.D. Fla. Mar. 23, 2011) (finding that an instant message exchange effectively modified a written agreement which contained a "no-oral modification clause").
219. Daniel Solove, *Thoughts on* City of Ontario v. Quon*: The Fourth Amendment and Privacy of Electronic Communications in the Workplace*, CONCURRING OPINIONS (Apr. 15, 2010, 12:04 PM), http://www.concurringopinions.com/archives/2010/04/thoughts-on-city-of-ontario-v-quon-the-fourth-amendment-and-privacy-of-electronic-communications.html.
220. This reliance justification is similar to a promissory estoppel argument and is related to the code-based promises proposal above. Users might only disclose information if websites promise to respect a user's privacy preferences. *See* Hartzog, *supra* note 73, at

Some courts weighing the evidentiary value of online agreements have looked to user attempts to indicate privacy preferences. Although the court in *United States v. Hart* found the terms of use dispositive regarding a reasonable expectation of privacy, it noted that "the evidence in the record does not show that the defendant sought to preserve as private that which the plaintiff now seeks to introduce into evidence."[221] By considering text, design, and action together, courts will be able to gain a better understanding of whether expectations of privacy are "reasonable" and alleviate some of the potentially unjust results from application of the ill-fitting standard-form contract theory to privacy disputes.

CONCLUSION

Privacy has become central to the user experience on many websites. Users regularly adjust privacy settings, un-tag photos, and delete information on their profile page. Privacy is also a significant aspect of the terms of use and privacy policies present on nearly every website. These consistently vague terms often reference the website's interactive features allowing users to protect their privacy. Yet courts customarily look only to the fine print to determine the scope of the agreement between users and websites regarding privacy. The contractual relationship formed when users interact with a website is far more complicated. Website design and features are capable of conveying a promise of privacy and inducing user reliance. The fine print in terms of use agreements and privacy policies often incorporates user privacy and website design. When website design is part of, or consistent with, the terms of use and central to the user experience, courts should look beyond boilerplate terms to find additional promises, acceptances of offers, and even elements that can interfere with contract formation.

Often, websites give the impression that website features, like the ability to increase privacy settings, are offers to protect information. Websites often promise to respect a user's privacy choices and in the same paragraph reference their privacy settings. In those contexts, courts should consider user preferences for privacy as acceptances of offers of confidentiality.

Courts should also more thoroughly scrutinize the ways in which website design can frustrate true agreement between the parties. Specifically, courts should refuse to enforce agreements where websites have egregiously employed malicious interfaces in the contract formation process. Courts should extend the concept of procedural unconscionability

---

924.

221. United States v. Hart, No. 08-109-C, 2009 WL 2552347, at *2 (W.D. Ky. Aug. 17, 2009) (citation omitted).

beyond the terms of use and consider the presence of malicious interfaces in website features on the agreement regarding user privacy. Features such as misleading links, disabled back buttons, unnecessary and confusing forms, and pop-ups covering desired content could all frustrate contract formation.

Finally, in non-contractual disputes where terms are merely evidence of consent, courts should look beyond the fine print to discover the operational reality between the parties. Here, courts should consider the relationship between the parties, other representations made by the website, and the context in which information was disclosed. For example, courts could consider whether information was deleted before a privacy harm occurred, whether privacy settings were utilized, or whether there were any other operational realities outside of the terms of use that induced reliance on a promise of confidentiality.

Online agreements are a promising solution to protect the flow of personal information only if courts look beyond the language included in standard-form contracts. Greater recognition of website design as a contract would advance both contract and privacy doctrine by better reflecting perceived promises of privacy and what information individuals desire to keep confidential. Empowering users with simple and precise ways to contractually protect their personal information could make the overwhelming number of online agreements part of a trusted system of Internet communication.