Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 27 *Volume XXVII*
Number 1

Article 5

2016

The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model

Thomas B. Norton
tnorton1@fordham.edu

The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model

Cover Page Footnote

J.D., Fordham University School of Law; Privacy Fellow, Fordham Center on Law and Information Policy at Fordham University School of Law. I thank Professors Joel Reidenberg and Cameron Russell for their continued input and support. I also thank the participants of the 43rd Research Conference on Communications, Information and Internet Policy (Sept. 2015) and the inaugural European Privacy Law Scholars Conference (Oct. 2015) for their insightful comments, as well as Professor Aditi Bagchi for her advice on an earlier version of this project. This project was supported in part by the National Science Foundation Secure and Trustworthy Computing initiative grant 1330214 for the project "TWC SBE: Option: Frontier: Collaborative: Towards Effective Web Privacy Notice and Choice: A Multi-Disciplinary Prospective" (the "Usable Privacy Project"). I thank the project's principal investigators and the research teams at Carnegie Mellon University for their efforts and support.

The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model

Thomas B. Norton*

Notice and Choice is the model for protecting privacy online in the United States. Under the model, users of online services are given notice about services information and privacy practices in the form of privacy policies. Based on this information, users can choose whether to use particular online services and whether to exercise any options for protecting their privacy that the services might offer.

In theory, Notice and Choice seems like a sound regulatory mechanism. Indeed, state and federal regulatory agencies prefer the model as a basis for privacy enforcement action. But Notice and Choice faces harsh criticism from privacy advocates. This Note adds a new critique to the list—that Notice and Choice leaves individual consumers who are affected by privacy policy breaches, legally, empty-handed. This is because website privacy policies—the principal mechanism for effectuating Notice and Choice—are generally not considered to be legally binding

* J.D., Fordham University School of Law; Privacy Fellow, Fordham Center on Law and Information Policy at Fordham University School of Law. I thank Professors Joel Reidenberg and Cameron Russell for their continued input and support. I also thank the participants of the 43rd Research Conference on Communications, Information and Internet Policy (Sept. 2015) and the inaugural European Privacy Law Scholars Conference (Oct. 2015) for their insightful comments, as well as Professor Aditi Bagchi for her advice on an earlier version of this project.

This project was supported in part by the National Science Foundation Secure and Trustworthy Computing initiative grant 1330214 for the project "TWC SBE: Option: Frontier: Collaborative: Towards Effective Web Privacy Notice and Choice: A Multi-Disciplinary Prospective" (the "Usable Privacy Project"). I thank the project's principal investigators and the research teams at Carnegie Mellon University for their efforts and support.

agreements. As a result, individuals' contract theory-based actions against companies for privacy policy breaches almost categorically fail. As a result, the users of online services are largely left without individual redress for privacy policy breaches.

Much has been written about Notice and Choice, and even more has been written about online contracting. Yet, like Notice and Choice and contract theory themselves, these two bodies of scholarship remain misaligned. This Note fills that gap by addressing Notice and Choice in the context of contracts, and offers alternative solutions to give individuals the opportunity to seek redress in the Notice and Choice scheme through contract theory.

INTRODUCTION

Imagine that you bought a plane ticket online. To complete your order, you provided the airline with your name, address, phone number, credit card number, and other sensitive personal information. Before you did this, you read the airline's privacy policy, which promised that the airline would not share any of your information with third parties. This promise gave you faith that you could safely entrust the airline with your information.

Months later, the Department of Defense hired a data analytics company to build a model for identifying individuals who might pose a threat to military facilities. At the Transportation Security Administration's urging, the airline from whom you have bought your ticket shared your information, and the information of other customers, with the data analytics company in blatant violation of the airline's privacy policy.

Based on the privacy policy you read, you expected that your personal information would not be transferred in this way. You sue the airline for breaching the policy. You believe you will win because the airline made a promise to not share your personal information, and it broke that promise. But in reality, you might not have it so easy.

The Internet has become a tool that billions of people around the world use every day to work, play, shop, socialize, and learn. Rapidly evolving technologies enable companies to track users online and collect ever-more-granular information about their Internet use habits—from details about website browsing history to records of individual keystrokes and clicks.[1] Websites and other providers of online services collect and use this information for their own commercial gain.[2]

But there is a trade-off: Websites and online services often offer free content and personalized services to individuals in exchange for sharing personal information.[3] This model of commerce poses risks, however; it can lead to discrimination (based on price or other factors) or can result in non-quantifiable harms, such as the ex-

---

1 *See generally* Tal Z. Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503.

2 *See infra* notes 16–19 and accompanying text.

3 *Id.*

posure of sensitive personal information.[4] For these reasons, significant policy-making efforts have been expended to establish boundaries for the collection and use of personal information.[5]

Despite such efforts, the United States has not adopted a comprehensive privacy law.[6] Instead, a patchwork quilt of federal and state laws narrowly targeted to specific sectors and actors establish privacy rules.[7] However, individuals' personal information collected by websites and online services is not protected by these industry-specific laws; instead, it is protected by a self-regulatory regime referred to as "Notice and Choice."[8]

Under the Notice and Choice model, websites or online services provide individuals with disclosure about their information practices, such as those pertaining to data collection, use, sharing, and security.[9] This knowledge, in turn, empowers individuals to make choices with respect to whether and how they will use the service.[10]

---

[4] *See* Alessandro Acquisti, *The Economics and Behavioral Economics of Privacy*, *in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD 76, 83 (Julia Lane et al. eds., 2014); *see also* Kim Zetter, *The Year's 11 Biggest Hacks, from Ashley Madison to OPM*, WIRED (Dec. 23, 2015, 2:00 PM), http://www.wired.com/2015/12/the-years-11-biggest-hacks-from-ashley-madison-to-opm/ [https://perma.cc/3AN6-TFP6].

[5] *See, e.g.*, Cybersecurity Information Sharing Act of 2015, 6 U.S.C. §§ 1501–1510 (Supp. 2015).

[6] *See* PAUL M. SCHWARTZ AND JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF U.S. DATA PROTECTION 7–10 (1996).

[7] *See id.*; Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights*, 44 FED. COMM. L.J. 195, 208–10 (1992). For example, the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.), protects personally identifiable health information and provides patients with a host of rights regarding that information by imposing layered privacy safeguards. Similarly, the Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012), protects information held by credit reporting agencies by giving consumers the right to access, dispute, and correct information about them. The Electronic Communications Privacy Act of 1986, Pub. L. 99–508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.), limits government access to private information that is stored and transmitted on the Internet.

[8] *See infra* Section II.A.

[9] Florencia Marotta-Wurgler, Does "Notice and Choice" Disclosure Regulation Work? An Empirical Study of Privacy Policies 2–3 (Apr. 2015) (unpublished manuscript) (on file with the Fordham Intellectual Property, Media & Entertainment Law Journal).

[10] *See id.*

Privacy policies are the primary mechanism for ensuring valid Notice and Choice.[11] Websites and online services use privacy policies to disclose their information practices.[12] As this Note explains, however, privacy policies generally lack contractually binding effect.[13] This means that in the event of a privacy policy breach, users are unable to seek redress by relying on contract theories.[14] This Note argues that this reality undermines Notice and Choice by running contrary to its objectives and rationales.[15]

The Note proceeds in three parts. Part I describes what privacy policies are, what they are meant to do, and the main critiques privacy policies face, including the fact that courts tend to interpret privacy policies as non-binding agreements. It concludes by discussing the practical effects of this state of affairs. Part II outlines the Notice and Choice regime and its history before arguing that privacy policies' non-contractual, non-binding nature is incongruent with Notice and Choice and its rationales and objectives. Part III offers potential solutions for this disconnect, including form-based and technology-based approaches.

I. NON-CONTRACTUAL PRIVACY POLICIES

This Part examines the enforceability of privacy policies as binding, contractual agreements. First, it describes privacy policies generally in terms of purpose and form. Next, it offers critiques of privacy policies. Then, the Part analyzes why contract claims founded on privacy policy breaches typically fail, and discusses the practical implications of this state of affairs.

A. Privacy Policies Generally

We live in a global economy supported by a common currency: information.[16] The companies we interact with online compile

---

11 *See* discussion *infra* Section I.A.

12 *Id.*

13 *See* discussion *infra* Section I.C.

14 *Id.*

15 *Id.*

16 *See generally* William D. Eggers et al., *Data as the New Currency*, DELOITTE REV., July 24, 2013, at 18, 20–21.

massive quantities of data about their customers.[17] When we use allegedly "free" services—for example, those provided by Google—we pay for those services by enabling the service provider to build a database of information about our searches, online activity, and personal information.[18] The service provider may then leverage this data for commercial gain.[19]

Privacy policies are meant to address how a company such as Google handles customer information. Generally, privacy policies are "comprehensive disclosure[s]" describing how websites and online services handle their users' information.[20] Though a privacy policy's precise content depends on a company's specific information practices, privacy policies typically include disclosures of how companies collect, use, disclose, retain, and manage customer information.[21]

Privacy policies are meant to increase the transparency of websites' information practices so that users are aware of those practices.[22] These policies often suggest that users refrain from using the website or service if they disagree with the policy terms.[23] Put another way, privacy policies provide users with *notice* of a website's information practices. With this notice, users can make a

---

[17] *Id.*

[18] *Id.*

[19] Companies perform large-scale analytics on their databases to convert data into actionable knowledge. *See* Thomas H. Davenport et al., *Data to Knowledge to Results: Building an Analytic Capability*, 43 CAL. MGMT. REV., no. 2, Winter 2001, at 117, 128. For example, companies use consumer data to deliver advertisements to individual consumers based on their online behavior. One recent estimate suggests that online advertising is a $23 billion per year industry. *See* INTERACTIVE ADVERT. BUREAU, INTERNET ADVERTISING REVENUE REPORT 3 (2009), http://www.iab.net/media/file/IAB_PwC_2008_full_year.pdf [https://perma.cc/ZY2H-9TFV]; *see also* Darrell Etherington, *Google Stops Mining Education Gmail and Google Apps Accounts for Ad Targeting*, TECHCRUNCH, (Apr. 30, 2014), http://techcrunch.com/2014/04/30/google-stops-mining-education-gmail-and-google-apps-accounts-for-ad-targeting/ [https://perma.cc/3ARK-3RNE].

[20] Richard Raysman & Peter Brown, *Contractual Nature of Online Policies Remains Unsettled*, N.Y.L.J., Aug. 10, 2010, at 2.

[21] *See, e.g.*, *Privacy Policy*, N.Y. TIMES, http://www.nytimes.com/content/help/rights/privacy/policy/privacy-policy.html [https://perma.cc/ZK9Z-DNBY] (last updated June 10, 2015).

[22] *See* Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN ST. L. REV. 587, 596 (2007).

[23] *Id.*

choice about whether to use the website or service, depending on how its information practices comport with their personal privacy preferences. This model is referred to as "Notice and Choice," and it is the preferred method for protecting privacy online in the United States.[24]

Today, nearly all companies have a privacy policy.[25] Though not required by law except in certain circumstances (e.g., to comply with the Children's Online Privacy Protection Act[26] ("COPPA")), privacy policies are de facto mandatory. In 2003, California enacted the California Online Privacy Protection Act[27] ("CalOPPA"), which requires that operators of commercial websites that collect personal information from California residents post a privacy notice that fulfills certain requirements.[28] Because online businesses typically serve a national audience, despite the physical location of users, the California law effectively imposes a requirement that all entities conducting business online in the United States post a privacy policy.

B. Common Privacy Policy Critiques

Privacy policies face a number of critiques. First, people rarely read or even see online privacy policies.[29] Those that attempt to

---

[24] Notice and Choice will be more thoroughly described *infra* Section II.A.

[25] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 594 (2014). According to Professor Haynes: "In 1998, only 2% of all websites had some form of privacy notices, and in 1999, eighteen of the top 100 shopping sites did not display a privacy policy. By 2001, virtually all of the most popular commercial websites had privacy notices. . . ." Haynes, *supra* note 22, at 593–94.

[26] COPPA requires that online services which collect information from children under 13 obtain parental consent to such collection after posting "a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page or screen of its Web site or online service, and, at each area of the Web site or online service where personal information is collected from children." FTC Commercial Practices Rule, 16 C.F.R. § 312.4(d) (2016).

[27] CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2014).

[28] The statute requires that an operator of commercial websites or online services that collect personally identifiable information about individual consumers residing in California "conspicuously post its privacy policy on its Web site, or in the case of an operator of an online service, make that policy available" via "reasonably accessible means of making the privacy policy available for consumers of the online service." §§ 22575(a), 22577(b)(5).

[29] *See* Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1885 (2013). Even Chief Justice Roberts admits to not reading

read the policies are unlikely to understand them because they are long and often filled with legal jargon.[30] And, given the multitude of complex ways that companies might use and manipulate information, it is difficult—if not impossible—for companies to accurately describe their information practices in a concise privacy statement.[31] For this reason, privacy policy drafters often employ vague or ambiguous language to either generalize very complex information practices or reserve the option to alter specific information practices in the future without creating the need to revise the policy.[32] Due to privacy policies' length, complexity, and incomprehensibility, it would prove extremely costly in both time and re-

---

the fine print he encounters online. *See* Debra Cassens Weiss, *Chief Justice Roberts Admits He Doesn't Read the Computer Fine Print*, ABA J. (Oct. 20, 2010, 12:17 PM), http://www.abajournal.com/news/article/chief_justice_roberts_admits_he_doesnt_read_the_computer_fine_print/ [https://perma.cc/RDF8-YAEX].

30 *See* Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 930 (2013); Solove, *supra* note 29, at 1885; *see also* Nick Bilton, *Price of Facebook Privacy? Start Clicking*, N.Y. TIMES (May 12, 2010), http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html?_r=0 [https://perma.cc/82TX-M2QQ] (contrasting Facebook's privacy policy length with that of the U.S. Constitution). The FTC has echoed this concern. *See* Press Release, Fed. Trade Comm'n, FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers (Dec. 1, 2010), https://www.ftc.gov/news-events/press-releases/2010/12/ftc-staff-issues-privacy-report-offers-framework-consumers [https://perma.cc/TV5H-WZ36] (noting that the "notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand"); *see also* United States v. Nosal, 676 F.3d 854, 861 (9th Cir. 2012) (en banc) (dictum) ("Our access to . . . remote computers is governed by a series of private agreements and policies that most people are only dimly aware of and virtually no one reads or understands."). In an amusing anecdote exemplifying the point, a company called PC Pitstop promised in its terms of use to pay a cash prize to anyone who read the terms and wrote to the company to claim the prize; it took months before a consumer noticed the promise and wrote in. *See* Larry Magrid, *It Pays to Read License Agreements*, PC PITSTOP, http://www.pcpitstop.com/spycheck/eula.asp [https://perma.cc/5LHM-AS8H] (last visited Oct. 9, 2016).

31 *See* Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S: J. L. & POL'Y FOR INFO. SOC'Y 425, 436–37 (2011) ("Privacy policies for the first-party websites that users interact with are difficult enough for users to understand, but when third-party sites enter the mix, the notion of effective privacy notice becomes completely untenable."); Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 SUFFOLK U. J. HIGH TECH. 370, 390–98 (2014).

32 *See* Joel R. Reidenberg et al., *Ambiguity in Privacy Policies and the Impact of Regulation*, 45 J. LEGAL STUD. (forthcoming 2016) (manuscript at 4) (on file with the Fordham Intellectual Property, Media & Entertainment Law Journal).

sources for an Internet user to read the privacy policy of every website he or she visited.[33]

C. Privacy Policies as Contracts?

Occasionally, websites or online services engage in information practices that differ from those described in their privacy policies: In contractual terms, they breach the policy.[34] But plaintiffs who have been the victims of alleged breaches have experienced difficulty alleging viable contract claims.[35] This runs contrary to early views on the issue: As privacy policies began to emerge, scholarship argued that contract law should play a role in their enforcement.[36] This view made sense, especially considering that some policies contained statements assuring users that the policies would be binding upon them.[37] But, as case law on the issue has devel-

---

[33] *See* Lorrie Faith Cranor, *Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. TELECOMM. & HIGH TECH. L. 273, 274 (2012). Cranor estimates that it would take a user an average of 244 hours per year to read the privacy policy of every website he or she visited. *Id.* This translates to about 54 billion hours and $781 million worth of time. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 540, 560–61 (2008).

[34] *See* Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and in Practice*, 7 J. INTELL. PROP. L. 57, 91–92 (1999).

[35] *See id.*

[36] *Id.* ("As between the website and the user, a privacy policy bears all of the earmarks of a contract. . . ."). *See generally* Curtis Bridgeman & Karen Sandrik, *Bullshit Promises*, 76 TENN. L. REV. 379 (2009).

[37] *See* Haynes, *supra* note 22, at 596 (describing how some websites presented their privacy policy terms as binding on the user); Raysman & Brown, *supra* note 20 (noting that "users implicitly acknowledge that they have read and understood the policy and agree to be legally bound by it"). Privacy policy enforcement cases follow a track that is slightly different from the typical case seeking enforcement of online terms. In many of the cases that establish the principles of online contracting, websites or providers of online services typically fight to enforce elements of their online terms against consumers. *See* Ian Rambarran & Robert Hunt, *Are Browse-Wrap Agreements All They Are Wrapped Up to Be?*, 9 TUL. J. TECH. & INTELL. PROP. 173, 179–83 (2007). For example, a user of an online service will bring an action against the service in court, and the service will move to compel arbitration per the service's terms of use. *See id.* at 181–83. Privacy policy enforcement cases, on the other hand, typically follow a different trajectory. In those cases, a user of a website or online service alleges that the website or service breached its privacy policy and that it should be held accountable for breaching a policy term. *See* Haynes, *supra* note 22, at 606–09. In the first line of cases, users try to escape enforceability of a policy term; in the latter, users fight to have policy terms enforced. And often, in the first line of cases, users try to claim that no binding agreement exists, whereas in the latter, they allege that the privacy policy is indeed a binding agreement.

oped, it has become clear that contract law is not as useful a tool for addressing privacy policy enforceability as early scholars thought it would be.[38]

Indeed, courts have eschewed contract theory when analyzing privacy policy enforceability.[39] Instead of finding that a privacy policy is binding on one party or the other, courts determine that no privacy agreement exists between the parties in the first place.[40] In these cases, courts take the view that privacy policies are general statements of policy rather than enforceable contracts.[41]

Privacy policy form contributes to this result. In the online space, two basic types of agreements dominate: clickwrap and browsewrap.[42] Clickwrap agreements are designed to secure a us-

---

[38] *See, e.g.*, Jurin v. Google Inc., 768 F. Supp. 2d 1064, 1073 (E.D. Cal. 2011) (dismissing breach of contract claims arising out of the alleged breach by Google of its AdWords policy terms and conditions on the ground that a "broadly stated promise to abide by its own policy does not hold Defendant to a contract"); Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004) (holding that plaintiffs could not maintain suit against Northwest Airlines for breach of its privacy statement because it was not a contract); *In re* Nw. Airlines Privacy Litig., No. Civ. 04-126 (PAM/JSM), 2004 WL 1278459, at *6 (D. Minn. June 6, 2004) ("The usual rule in contract cases is that general statements of policy are not contractual."); *see also* Meyer v. Christie, No. 07-2230-JWL, 2007 WL 3120695, at *4–5 (D. Kan. Oct. 24, 2007) (noting that unilateral corporate policies generally do not support breach of contract claims).

[39] *See Jurin*, 768 F. Supp. 2d at 1073.

[40] *See Dyer*, 334 F. Supp. 2d at 1200.

[41] *See In re Nw. Airlines Privacy Litig.*, 2004 WL 1278459, at *6.

[42] The distinction this Note draws between the clickwrap model and the browsewrap model is a simplified one, as the line between the two is sometimes blurred. For over a decade, courts have had difficulty drawing this distinction and applying it in their cases. *See, e.g.*, Hotels.com, L.P. v. Canales, 195 S.W.3d 147, 155 (Tex. Ct. App. 2006) (resolving that the agreement on the Hotels.com website "cannot be neatly characterized as either a 'click-wrap' or 'browse-wrap'"); *see also* Venkat Balasubramani, *The "Browsewrap"/"Clickwrap" Distinction Is Falling Apart*, TECH. & MARKETING L. BLOG (Feb. 24, 2015), http://blog.ericgoldman.org/archives/2015/02/the-browsewrap clickwrap-distinction-is-falling-apart.htm [https://perma.cc/Z67B-GACD] (summarizing recent decisions imprecisely drawing the browsewrap/clickwrap distinction). This is because, sometimes, online agreements do not fit neatly into one of these forms. To account for this, some authorities have proposed a third online contracting category—"modified clickwrap"—which include elements of both clickwraps and browsewraps. *See, e.g.*, Swift v. Zynga Game Network, Inc., 805 F. Supp. 2d 904, 910–11 (N.D. Cal. 2011); Deborah Davis Boykin, *Survey of E-Contracting Cases: Browsewrap, Clickwrap, and Modified Clickwrap Agreements*, 68 BUS. LAW. 257, 257, 259–262 (2012). At least one court has abandoned the clickwrap/browsewrap distinction in its decision-making. *See* Hoffman v. Supplements Togo Mgmt., LLC, 419 N.J. Super. 596, 612 (N.J. Super. Ct. App. Div.

er's express assent to an agreement.[43] Under the clickwrap model, a website presents a user with the website's terms and requires that the user assent to those terms by clicking an icon—usually reading "I Accept" or "I Agree"—to signal her assent before using the website.[44] Courts find clickwrap agreements enforceable when users have knowledge of the presented terms,[45] including unread terms.[46] Courts enforce clickwrap agreements because it is easy to identify whether and when a user consents to the agreement terms.[47]

Privacy policies, however, often take the browsewrap form. Browsewrap agreements are visible on a separate webpage accessible via a hyperlink on the main webpage; a website user may click that link to visit, view, and read the site's terms.[48] Users are not required to visit and view these agreements before using the website or service,[49] but the terms are nonetheless purportedly binding on the user.[50] Browsewrap agreements do not require that a user affirmatively consent to the terms, so in the browsewrap context it is difficult to pinpoint the precise moment of assent that the tradi-

---

2011) (recognizing a division in case law about the extent to which clickwrap features are needed to make contractual provisions enforceable, and instead deciding an online contract assent issue on notice grounds). But for my purposes here, the simplified distinction suffices.

43 *See* Rambarran & Hunt, *supra* note 37, at 174, 177.

44 *See id.*

45 *See, e.g.*, Hancock v. Am. Tel. & Tel. Co., 701 F.3d 1248, 1257–58 (10th Cir. 2012) (enforcing clickwrap terms against plaintiffs after determining that they had expressed assent to the terms on two different occasions by clicking "I Acknowledge" and "I Agree").

46 *See, e.g.*, Davis v. HSBC Bank Nevada, N.A., 691 F.3d 1152, 1163–64 (9th Cir. 2012) (enforcing unread clickwrap terms where a plaintiff checked a box acknowledging that he had, in fact, read them).

47 *See id.*

48 *See* Rambarran & Hunt, *supra* note 37, at 174. Links to browsewrap agreements can usually be found at the bottom of a website's homepage, and often appear in language such as "Legal" or "Terms of Use." *Id.* at 176; *see also* Solove & Hartzog, *supra* note 25, at 592.

49 *See* Be In, Inc. v. Google Inc., No. 12-CV-03373-LHK, 2013 WL 5568706, at *6 (N.D. Cal. Oct. 9, 2013) ("The defining feature of browsewrap agreements is that the user can continue to use the website or its services without visiting the page hosting the browsewrap agreement or even knowing that such a webpage exists.").

50 *See* Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 429 (2d Cir. 2004); Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 28–30 (2d Cir. 2002); Pollstar v. Gigmania, Ltd., 170 F. Supp. 2d 974, 981–82 (E.D. Cal. 2000).

tional principles of contract formation require.[51] Because clear manifestation of assent is often lacking in the browsewrap context, courts' analysis of whether such agreements are binding between the parties "turns on whether a website user has actual or constructive knowledge of a [web]site's terms and conditions prior to using the [web]site."[52] A few exceptions notwithstanding, browsewrap agreements are usually held not enforceable.[53] When a priva-

---

[51] *See* Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 465–66 (2006).

[52] Sw. Airlines Co. v. BoardFirst, L.L.C., No. 3:06-CV-0891-B., 2007 WL 4823761, at *5 (N.D. Tex. Sept. 12, 2007).

[53] *See, e.g.*, Nguyen v. Barnes & Noble Inc., 763 F.3d 1171, 1178–79 (9th Cir. 2014) ("[W]here a website makes its terms of use available via a conspicuous hyperlink on every page of the website but otherwise provides no notice to users nor prompts them to take any affirmative action to demonstrate assent, even close proximity of the hyperlink to relevant buttons users must click on—without more—is insufficient to give rise to constructive notice."); *Specht*, 306 F.3d at 35 (holding that hidden, linked-to license agreement terms were not binding on plaintiffs, who lacked notice of and did not assent to the terms); *Be In*, 2013 WL 5568706, at *9 (declining to enforce Terms of Service against defendants because, except for the existence of a "Terms of Service" hyperlink, no allegations showed that the defendants had notice that mere use of the plaintiff's website amounted to assent to the Terms); Defontes v. Dell Computs. Corp., No. C.A. PC 03-2636, 2004 WL 253560, at *6 (R.I. Super. Jan. 29, 2004), *aff'd*, 984 A.2d 1061 (R.I. 2009) (no manifestation of assent to online terms and conditions that were only accessible via an inconspicuous hyperlink at the bottom of Dell's webpage). The cases in which courts enforce browsewrap agreements typically present unique facts in that the parties are businesses or are otherwise sophisticated. For example, courts have enforced browsewraps in instances where one party continually violates the other's terms after receiving explicit notice of the terms and instructions to cease the violation. *See, e.g.*, *Sw. Airlines Co.*, 2007 WL 4823761, at *7–8 (finding terms binding on defendant after it continued to use the plaintiff's website after receiving a letter ordering it to cease and desist the activity that violated the terms); Ticketmaster Corp. v. Tickets.com, Inc., No. CV997654HLHVBKX, 2003 WL 21406289, at *2 (C.D. Cal. Mar. 7, 2003) (enforcing terms when defendant continued to breach terms of use even after receiving a letter from plaintiff citing the terms and replying that it did not accept those terms). Other cases enforce browsewrap terms where the party against whom the terms are to be enforced admitted to having knowledge of the terms. *See, e.g.*, *Register.com*, 356 F.3d at 429–30; Cairo, Inc. v. Crossmedia Servs., Inc., No. C 04-04825 JW, 2005 WL 756610, at *5 (N.D. Cal. Apr. 1, 2005). Browsewrap agreements have also been enforced when factual allegations beyond a browsewrap's terms or presentation support the notion that a user had actual or constructive knowledge of the terms. *See, e.g.*, AvePoint, Inc. v. Power Tools, Inc., 981 F. Supp. 2d 496, 510–11 (W.D. Va. 2013) (declining to declare a browsewrap agreement unenforceable at the motion to dismiss stage when facts alleged that the defendant corporation used a fictitious email to download plaintiff's software, which, by its terms, was not to be used for commercial purposes).

cy policy takes browsewrap form, it then becomes difficult to find that the policy amounts to a binding agreement.[54]

In fact, it has been industry practice to draft privacy policies in this way so that they do *not* constitute enforceable agreements.[55] Since privacy policies enforcement is typically sought *by users* and *against* websites or online services, and because the services can include in their terms of use any provisions they would like to be binding on the user, websites typically "opt not to provide users with another reason to sue them" and assure users that the privacy policy is a mere policy statement not intended to be a contract.[56]

Another reason that courts reject contract claims for privacy policy breaches is because plaintiffs fail to allege cognizable damages resulting from the breach—an essential element of a breach of contract claim.[57] Proving damages resulting from privacy policy breaches is extremely difficult. For example, a claim for mere emotional harm stemming from a loss of privacy is not sufficient as an

---

[54] *See Sw. Airlines Co.*, 2007 WL 4823761, at *5.

[55] IAN C. BALLON, 2 E-COMMERCE AND INTERNET LAW: A LEGAL TREATISE WITH FORMS § 26.14[2] (2d ed. 2014).

[56] *Id.*

[57] *See, e.g.*, Smith v. Trusted Universal Standards in Elec. Transactions, Inc., No. 09-4567 (RBK/KMW), 2010 WL 1799456, at *10 (D.N.J. May 4, 2010) (holding that the plaintiff could, in principle, assert a breach of contract claim based on privacy policy breach, but nevertheless granting defendants' motion to dismiss because the plaintiff did not allege any damages resulting from the alleged breach); Cherny v. Emigrant Bank, 604 F. Supp. 2d 605, 609 (S.D.N.Y. 2009) (ruling that the plaintiff's receipt of spam email after defendant disclosed her email address in contravention of its privacy policy failed to give rise to recoverable damages); *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 325–27 (E.D.N.Y. 2005) (granting defendants' motion to dismiss because the plaintiff did not allege any damages resulting from the alleged breach); *In re* Am. Airlines, Inc., Privacy Litig., 370 F. Supp. 2d 552, 567 (N.D. Tex. 2005) (dismissing plaintiffs' breach of contract claim on the ground of failure to allege damages); *In re* Nw. Airlines Privacy Litig., No. 04-126 (PAM/JSM), 2004 WL 1278459, at *6 (D. Minn. June 6, 2004). *But see In re* EasySaver Rewards Litig., 737 F. Supp. 2d 1159, 1172–74 (S.D. Cal. 2010) (denying a motion to dismiss a breach of contract claim where plaintiffs alleged that they purchased flowers from a website subject to the Terms of Use, Privacy Policy, and Rewards Policies posted on the website and were, as a result, unknowingly enrolled in a rewards program that automatically charged them an activation fee). EasySaver eventually settled, so it remains unclear whether the court would have enforced the privacy policy at issue as a contract later in litigation. *See* Megan Leonhardt, *ProFlowers Parent Co. Arranges $38M Deal over Data Policies*, LAW360 (June 14, 2012, 2:19 PM), http://www.law360.com/articles/350092/proflowers-parent-co-arranges-38m-deal-over-data-policies [https://perma.cc/VZF4-RCH6].

allegation of damages.[58] Neither is a claim for mere loss of privacy.[59] Courts have also held that personally identifiable information is not considered property and thus has no compensable value, despite concrete evidence to the contrary.[60]

As an alternative to alleging damages, some plaintiffs have attempted to lean on promissory estoppel to have their contract claims considered.[61] Promissory estoppel is a doctrine providing that if a party relies on a promise, the promise can be enforced even though the essential elements of a contract (e.g., damages) are not met.[62] But like plaintiffs alleging pure contract claims, plaintiffs alleging promissory estoppel have seen little success, as they are

---

[58] *See, e.g.*, Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1028 (N.D. Cal. 2012) (rejecting embarrassment and property-based theories of harm as insufficient to state claim for breach of contract); Trikas v. Universal Card Servs. Corp., 351 F. Supp. 2d 37, 45–46 (E.D.N.Y. 2005).

[59] *See* Rudgayzer v. Yahoo! Inc., No. 5:12-CV-01399 EJD, 2012 WL 5471149, at *6 (N.D. Cal. Nov. 9, 2012) (finding that "[m]ere disclosure of such information in and of itself, without a showing of actual harm, is insufficient" to support a claim of breach of contract); *Smith*, 2010 WL 1799456, at *10 ("[E]ven assuming that a contract did exist between Comcast and Plaintiff that incorporated the above terms, and even assuming that Comcast violated those terms, Plaintiff must still plead loss flowing from the breach to sustain a claim. . . . He has not done so."); *Cherny*, 604 F. Supp. 2d at 609 ("This Court finds that the release of an e-mail address, by itself, does not constitute an injury sufficient to state a claim under any of the legal theories Cherny asserts.").

[60] *See In re* Facebook Privacy Litig., 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011) ("[P]ersonal information does not constitute property. . . ."); Stayart v. Google Inc., 783 F. Supp. 2d 1055, 1057 (E.D. Wis. 2011) ("[P]laintiff alleges no facts which suggest that her name has any commercial value. . . ."); In re *JetBlue*, 379 F. Supp. 2d at 327 ("[T]here is absolutely no support for the proposition that the personal information of an individual JetBlue passenger had any value for which that passenger could have expected to be compensated."). These conclusions seem to skirt the reality that personal information is a highly valued commodity. *See, e.g.*, John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, 12–15 (2009) (summarizing the multiple ways that personal information is valuable to companies that possess it); Julie Brill, Comm'r, Fed. Trade Comm'n, Keynote Address at Proskauer on Privacy 4 (Oct. 19, 2010), http://www.ftc.gov/speeches/brill/101019proskauerspeech.pdf [https://perma.cc/79X-8E3E] ("[T]he collection and use of consumer information . . . underwrites so much of the free content available to consumers online."); *see also supra* notes 16–19 and accompanying text.

[61] *See* Hoffman v. Red Owl Stores, Inc., 26 Wis. 2d 683, 694 (1965).

[62] *See id.* at 698; RESTATEMENT (SECOND) CONTRACTS § 90(1) (AM. LAW INST. 1981).

typically unable to show detrimental reliance on the privacy policy allegedly breached.[63]

The effect of this is that as privacy policies have grown in prominence, fewer and fewer cases alleging privacy policy breach have been grounded on contract theories. The inutility of contract law for enforcing privacy policy promises calls into question the effectiveness and legitimacy of the Notice and Choice model for privacy protection.

II. CONTRACT LAW'S INEFFECTIVENESS FOR ADDRESSING PRIVACY POLICY BREACHES IS INCONGRUENT WITH NOTICE AND CHOICE

Contract law's ineffectiveness for addressing privacy policy breaches exposes a gap in the Notice and Choice approach. This Part addresses that gap. First, the Part describes Notice and Choice in terms of what it is, what is intended to do, and why it is considered important. Then the Part argues that privacy policies' non-contractual, non-binding nature is incongruent with the Notice and Choice model.

A. Notice and Choice: The U.S. Approach to Online Privacy

1. Notice and Choice Generally

Notice and Choice is the preferred model for protecting individuals' privacy online.[64] The general thrust of the scheme is that

---

[63] *See, e.g.*, Azeltine v. Bank of America, No. CV 10-218-TUC-RCC (HCE), 2010 WL 6511710, at *10 (D. Ariz. Dec. 14, 2010) (dismissing the plaintiff's breach of contract claim after determining that plaintiff alleged no reliance on Bank of America's privacy policy); Smith v. Trusted Universal Standards in Elec. Transactions, Inc., No. 09-4567(RBK/KMW), 2011 WL 900096, at *10 n.10 (D.N.J. Mar. 15, 2011) ("[T]here is no evidence . . . that Plaintiff relied on a promise . . . . Therefore, no reasonable jury could conclude that a contract existed between the parties based upon a doctrine of promissory estoppel."); *see also* Solove & Hartzog, *supra* note 25, at 595. *But see* Meyer v. Christie, No. 07-2230-JWL, 2007 WL 3120695, at *4–6 (D. Kan. Oct. 24, 2007) (allowing plaintiff to sue for breach of a bank's privacy policy where the plaintiff had a long-term relationship with the bank that led him to rely on the bank to preserve his confidential information in accordance with the policy).

[64] Notice and Choice is also sometimes referred to as Notice and Consent. *See, e.g.*, Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent*, *in*

an entity that collects or uses individuals' personal information must disclose the ways it collects and uses that information and must afford individuals an opportunity to choose whether and how to transact with the entity.[65] Privacy policies are the primary means for effectuating Notice and Choice.[66]

Valid notice requires that an entity disclose to individuals its data practices before collecting or using their personal information.[67] Adequate disclosure requires providing specific details about data collection, use, sharing, security, and other similar elements.[68] Choice is a consent-based theory centered on the notion that consumers should have options with respect to how their collected personal information will be used and that they should be able to make informed privacy choices based on their personal privacy preferences.[69]

The principles behind Notice and Choice have been evolving since the early 1970s, at which time concerns about the potentially

---

PROCEEDINGS OF THE ENGAGING DATA FORUM: THE FIRST INTERNATIONAL FORUM ON THE APPLICATION AND MANAGEMENT OF PERSONAL ELECTRONIC INFORMATION 4 (2009), https://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf [https://perma.cc/72BD-KY3D] (defining "notice and consent"); Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 342, 351 (Jane Winn ed., 2006) (addressing notice and consent principles for data collection).

65 *See* Barocas & Nissenbaum, *supra* note 64.

66 FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 8 (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [https://perma.cc/U4RS-RF7A] ("In the Internet context, notice can be accomplished easily by the posting of an information practice disclosure describing an entity's information practices on a company's site on the Web.").

67 *Id.*

68 Some of which might include:

> identification of the entity collecting the data; identification of the uses to which the data will be put; identification of any potential recipients of the data; the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information); whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and the steps taken by the data collector to ensure the confidentiality, integrity, and quality of the data.

See id. at 7–8.

69 *Id.* at 8.

harmful consequences of computer-based technologies incubated.[70] The concept of what is now referred to as Notice and Choice was articulated for the first time in a 1977 Privacy Protection Study Commission report on mailing lists maintained for commercial purposes.[71]

In the 1990s, as Internet use became prevalent, issues of online privacy and notice began to take center stage. By the mid-1990s, both the White House and the Federal Trade Commission ("FTC") began to implement key theories of the Notice and Choice approach in policymaking efforts.[72] Later in the decade,

---

[70] In 1973, an Advisory Committee on Automated Personal Data Systems produced a report which advised that private and public sector organizations implementing programs for maintaining information about individuals should provide annual public notice of the "existence and character" of their programs, and which also offered a list specific elements the notice should contain. *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS 57–58 (1973). A year later, Congress passed the Privacy Act of 1974, 5 U.S.C. § 552a (2012), which was designed to regulate the federal government's collection and protection of citizens' personal information. The Privacy Act also called for the creation of the Privacy Protection Study Commission ("PPSC"), which was charged with analyzing various privacy and record-keeping practices arising in both the public and commercial sectors. Pub. L. No. 93-579, § 5, 88 Stat. 1896, 1905 (1974) (current version at § 552a).

[71] The PPSC investigated whether parties maintaining mailing lists for commercial purposes should be required to de-identify individuals appearing on the list. PRIVACY PROT. STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 125–54 (July 1977). The PPSC's report on the matter recommended that private sector organizations that share their mailing lists with third parties should provide notice of the practice to list members and to give them the opportunity to opt out of the sharing. *Id.* at 151.

[72] In 1993, the administration of President Bill Clinton established the Information Infrastructure Task Force ("IITF") to develop policies and programs for promoting the development of a new "National Information Infrastructure." Fred H. Cate, *The National Information Infrastructure: Policymaking and Policymakers*, 6 STAN. L & POL'Y REV. 43, 44, 47 (1994). The IITF contained a Privacy Working Group, which included in its 1995 report a notice principle requiring that individuals be provided with information sufficient to make informed decisions about their privacy. PRIVACY WORKING GRP., PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION II.B (1995), http://aspe.hhs.gov/datacncl/niiprivp.htm [https://perma.cc/T329-39C8]. The White House reinforced this principle in its 1997 framework. *See* WHITE HOUSE, THE FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (1997), https://clinton4.nara.gov/WH/New/Commerce/read.html [https://perma.cc/R26K-PZS6] ("Data-gatherers should inform consumer what information they are collecting and how they intend to use such data. . . ."). In 1996, the FTC undertook a consumer privacy initiative to explore online privacy issues and reported that participants in an online privacy workshop agreed that notice of information practices is a principle essential to protecting privacy online. *See* FED. TRADE COMM'N

Notice and Choice became the primary online privacy protection mechanism. Indeed, in its 1998 report to Congress, the FTC asserted that notice is "the most fundamental principle" for protecting privacy online.[73]

Notice and Choice remains regulators' preferred approach: Both the White House and the FTC again advocated for Notice and Choice when they issued major privacy reports in 2012.[74] Why do regulators so staunchly support the model? The next Section addresses the benefits of and rationales for Notice and Choice.

2. Why Notice and Choice?

Since it was first articulated, the principles of Notice and Choice have evolved to benefit individuals, businesses, and regulators alike. A primary benefit of Notice and Choice is that it is a self-regulatory scheme.[75] Though guidelines exist for how companies should draft their privacy policies and for what those policies should include so that valid Notice and Choice is offered,[76] compa-

---

BUREAU OF CONSUMER PROT., STAFF REPORT: PUBLIC WORKSHOP ON CONSUMER PRIVACY ON THE GLOBAL INFORMATION INFRASTRUCTURE ch. 2 (1996), http://www.ftc.gov/reports/staff-report-public-workshop-consumer-privacy-global-information-infrastructure [https://perma.cc/U2X5-XRLW]. The initiative also concluded that there was general agreement among participants that, in addition to providing notice, organizations should offer choice and establish safeguards for information they hold. *See id.*

[73] FED. TRADE COMM'N, *supra* note 66, at 7.

[74] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 35–36, 61–64 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/K4DY-23R8]; WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 11–18 (2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf [https://perma.cc/3U29-BHY7] (highlighting notice's role, illustrating the challenges organizations face in providing in light of emerging technology, and explaining the significance of the consumer-company relationship in determining how notice is provided).

[75] *See* Joel R. Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S: J.L. & POL'Y FOR INFO. SOC'Y 485, 489–90 (2015).

[76] *See, e.g.*, FED. TRADE COMM'N, *supra* note 74, at 61–64; KAMALA D. HARRIS, CAL. DEP'T OF JUSTICE, MAKING YOUR PRIVACY PRACTICES PUBLIC: RECOMMENDATIONS ON DEVELOPING A MEANINGFUL PRIVACY POLICY 4–5 (2014), https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf [https://perma.cc/4WMS-93KT].

nies are largely free to construct their privacy policies as they see fit. Notice and Choice is thus seen as a regulatory alternative that is more flexible, less expensive to implement, and easier to enforce than statutory or administrative regulation.[77]

Further, Notice and Choice is designed to put individuals in charge of the collection and use of their personal information. By placing decision-making power in individuals' hands, Notice and Choice supports individual autonomy.[78] With proper notice, individuals can compare services based on their stated information practices and can choose to transact with services based on how those practices comport with the individual's privacy preferences.[79] Personal privacy preferences vary, and through Notice and Choice, individuals who place a low value on privacy are able to exchange it for goods or information that they value more highly, such as free services.[80] Individuals' consent-based relationship has the important effect of legitimizing the information practices disclosed through Notice and Choice.[81]

The individual autonomy that Notice and Choice supports influences the market for information. Individuals' ability to make decisions on how business' information practices align with their own privacy preferences makes privacy a type of "brand differentiator."[82] In this sense, disclosure through notice encourages privacy-based competition between online service providers.[83] For example, a privacy-conscious consumer might opt to transact with

---

[77] *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1049 (2012); Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 682 (2011) (noting that notice "looks cheap" and "looks easy").

[78] *See* Calo, *supra* note 77.

[79] *See* Paula J. Breuning & Mary J. Culnan, *Through a Glass Darkly: From Privacy Notices to Effective Transparency*, 17 N.C. J.L. & TECH. 515, 529 (2016).

[80] *See* Calo, *supra* note 77.

[81] MacCarthy, *supra* note 31, at 440.

[82] *See* WHITE HOUSE, *supra* note 72 ("Disclosure by data-gatherers is designed to simulate market resolution of privacy concerns by empowering individuals to obtain relevant knowledge about why information is being collected, what the information will be used for, what steps will be taken to protect that information, the consequences of providing or withholding information, and any rights of redress that they may have. Such disclosure will enable consumers to make better judgments about the levels of privacy available and their willingness to participate.").

[83] *See id.*

a business that promises to not share her information with third parties, rather than one that does not make such a promise.[84]

Because of its effect on the market, Notice and Choice serves as an appropriate basis for regulation. The FTC is the primary privacy enforcement authority in the United States, and is the agency that polices Notice and Choice.[85] Section 5 of the Federal Trade Commission Act[86] empowers the FTC to investigate and take enforcement action against companies that engage in "unfair" or "deceptive" trade practices.[87] Under this enforcement authority, the FTC investigates businesses that engage in unfair or deceptive information practices.[88] The FTC has exercised this authority and taken enforcement actions against bad actors frequently over the past fifteen years.[89] Indeed, the FTC's privacy enforcement power extends to a degree that some scholars have dubbed its privacy enforcement jurisprudence as a "common law of privacy."[90]

Additionally, Notice and Choice encourages public dialogue about information use and protection and thus promotes accountability. Privacy notices make an entity's privacy practices public. This provides a window through which individuals, businesses, and regulators can observe the evolution of information practices with-

---

84 *See id.*

85 *See* Solove & Hartzog, *supra* note 25 (providing a comprehensive discussion of the FTC's role in privacy oversight and enforcement).

86 15 U.S.C. § 45 (2012).

87 *See* § 45(a)(1).

88 *See* Haynes, *supra* note 22, at 600.

89 *See, e.g.*, FTC v. Toysmart.com, LLC, et al., No. 00-11341-RGS, 2000 WL 34016434 (D. Mass. July 21, 2000) (settling charges that ToySmart attempted to sell customers' personal information to third parties despite promises to the contrary in the privacy policy); Snapchat, Inc., No. 132 3078 (F.T.C. Dec. 23, 2014), https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf [https://perma.cc/H3LC-CDCF] (settling charges alleging that Snapchat users' photos did not automatically disappear despite a promise to the contrary); Epic Marketplace, Inc., 155 F.T.C. 406 (2013) (settling charges that Epic's failure to disclose its practice of using customers' browser histories to deliver targeted advertising violated Section 5); GeoCities, 127 F.T.C. 94 (1999) (settling charges alleging that GeoCities' privacy policy misrepresented how the company used registered visitors' marketing information); *see also* Reidenberg et al., *supra* note 75, at 507–08 (indexing recent FTC privacy enforcement actions); Solove & Hartzog, *supra* note 25, at 598–600 (summarizing the FTC's privacy enforcement history).

90 *See* Solove & Hartzog, *supra* note 25, at 627.

in the industry.[91] The resulting discourse sometimes reveals privacy practices that become targets for regulatory enforcement.[92] But despite its advantages, Notice and Choice faces critiques. The next Section addresses those, and offers a new one.

B. Privacy Policies' Non-Contractual, Non-Binding Nature Is Incongruent with the Notice and Choice Approach

Privacy advocates often criticize Notice and Choice as ineffective. Critics argue that Notice and Choice does not actually leave people informed: People rarely see, read, or understand the privacy policies they encounter,[93] so individuals make false assumptions about how websites and online services use and protect their information.[94] The model is also considered impractical, because there are simply too many privacy policies to keep track of, in light of the potentially hundreds of websites an individual might visit on any given day.[95] And what makes things even more difficult for users is that privacy policies do not apply to the often-undisclosed third parties with whom the policy owner might share user information.[96] As a result, the downstream flow of user information winds through the hands of a "potentially . . . unending chain of

---

[91] *See* Breuning & Culnan, *supra* note 79, at 17.

[92] *See, e.g.*, Facebook, Inc., No. 092 3184 (F.T.C. July 27, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf [https://perma.cc/UQZ3-8RUM] (action by privacy advocacy group Electronic Privacy Information Center resulting in comprehensive consent decree containing privacy-enhancing stipulations).

[93] *See supra* notes 29–32 and accompanying text.

[94] Two studies reveal this reality. In one, users of online services correctly answered questions about the privacy of their online transactions only 30% of the time. Joseph Turow et al., Americans Reject Tailored Advertising and Three Activities that Enable It 20–21 (2009) (unpublished manuscript), http://ssrn.com/paper=1478214 [https://perma.cc/K22M-5U97]. In another, 64% of survey respondents did not know that a supermarket may sell other information about what they buy to other companies. Joseph Turow et al., Open to Exploitation: America's Shoppers Online and Offline 3 (2005), http://repository.upenn.edu/cgi/viewcontent.cgi?article=1035&context=asc_papers [https://perma.cc/LB2H-XXEB]. The same study revealed that 75% of study respondents incorrectly believed that the mere presence of a privacy policy meant that a website would not disclose users' information to other entities. *Id.*

[95] *See* Ben-Shahar & Schneider, *supra* note 77, at 687–89 (describing the "overload effect" in online disclosure); Ohm, *supra* note 30, at 930; *see also supra* note 33 and accompanying text.

[96] *See* Barocas & Nissenbaum, *supra* note 64, at 5.

actors" in a way that is "not only difficult to grasp, but unknowable."[97] Notice and Choice, then, neither provides individuals with adequate knowledge about the consequences of information disclosure nor with mechanisms for ensuring that their information is disclosed only in the ways they desire.[98]

Further, websites and online services often unilaterally modify their privacy policies without notifying users.[99] This means that even if a user were to follow the privacy statements of the websites or services she uses, she may find that terms to which she initially agreed no longer apply. This Note adds a new critique: Because privacy policies are non-contractual in nature, Notice and Choice breaks down when websites or online services execute information practices that are different from those stated in their privacy policies, and in these instances individuals are left without the opportunity to seek redress on contractual grounds.

As this Note has shown, the development of case law addressing the issue rebuts the early notion that contract law would be the most applicable tool for responding to privacy policy breaches.[100] For one reason or another—policy form, plaintiffs' inability to allege damages, or plaintiffs' inability to prove reliance—courts are unwilling to enforce privacy policies as binding agreements between a website and a user.[101] This suggests that privacy policy breaches may be "(effectively) categorically immune" from privately brought breach of contract claims.[102] The consequence is that though individuals may vet websites or online services and opt to use those whose stated practices match their personal privacy

---

97 *Id.* at 6.

98 *See* Lorrie Faith Cranor, *Privacy Policies and Privacy Preferences*, *in* SECURITY AND USABILITY: DESIGNING SECURE SYSTEMS THAT PEOPLE CAN USE 448 (Lorrie Faith Cranor & Simson Garfinkel eds., 2005).

99 *See id.*; Solove, *supra* note 29, at 1888–89.

100 *See* Killingsworth, *supra* note 34 and accompanying text.

101 *See* discussion *supra* Section I.C.

102 Eric Goldman, *When Does a Privacy Policy Breach Support a Breach of Contract Claim?* In re JetBlue, TECH. & MARKETING L. BLOG (Dec. 16, 2005), http://blog.ericgoldman.org/archives/2005/12/when_does_a_pri.htm [https://perma.cc/83DN-GER3]. This stands in contrast with cases involving websites' terms of use, which *are* governed by contract law. *See supra* notes 42–54 and accompanying text (discussing browsewrap and clickwrap agreements). *See generally* Lemley, *supra* note 51 (tracking how contract principles have applied to online terms of use).

preferences, when a service undertakes information practices that are different from those stated, Notice and Choice fails to vindicate individuals affected by the broken promise.

This undermines several of Notice and Choice's objectives. For one, it endangers the individual autonomy that Notice and Choice fosters: If both a service's notice and an individual's choice based on that notice can essentially evaporate with no consequence, the model lacks integrity. And, to the extent that companies can deviate from their stated information practices without facing accountability, companies' privacy practices cannot effectively serve as a basis for competition in the market.[103]

The disconnect between Notice and Choice and contract law is important for other reasons as well. For one, individuals benefit from services that enable us to work, shop, socialize, and play online, and services gain from the information users provide. In turn, services leverage that gain to offer innovative products and features.[104] But such a relationship is grounded in trust. If individuals cannot trust that companies will use their information in the ways prescribed in privacy policies, then individuals may cease using the services and thus stunt innovation.[105] Non-formalized privacy agreements open the door for information misuse, and thus user mistrust, while formalized privacy contracts could help to secure the trust required for the described cycle of benefit to persist.

Additionally, there is the risk that websites or services will not abide by the various guidelines that exist for offering valid Notice and Choice.[106] Though the FTC's expanding enforcement power

---

[103] MacCarthy, *supra* note 31, at 433, and accompanying text.

[104] *See supra* notes 16–19 and accompanying text.

[105] In 2012 and 2015, modifications to Instagram's Terms of Service generated such outcry among users that the service revoked the modification. *See* Dino Grandoni, *Instagram Regulations Get Tweaked After Uproar—But The Worst Part Is Still There*, HUFFINGTON POST (Dec. 21, 2012, 9:09 AM), http://www.huffingtonpost.com/2012/12/21/instagram-regulations_n_2342509.html [https://perma.cc/V9R4-98GQ]. In 2015, negative user response changes in Spotify's privacy policy led the company to publicly apologize and clarify its terms. *See* Hayley Tsukayama, *Spotify Apologizes for Its Newest Privacy Policy*, WASH. POST (Aug. 21, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/08/21/spotify-apologizes-for-its-newest-privacy-policy/ [https://perma.cc/K8R5-V7DW].

[106] *See supra* note 76 and accompanying text.

against companies that commit unfair or deceptive privacy practices likely mitigates this risk,[107] early evidence suggested that the industry failed to adhere to FTC information principles, and that other privacy self-regulation schemes (such as privacy certifications and monitoring) were ineffective.[108] Privacy policies' nonbinding effect means that companies can depart from regulators' guidelines for valid Notice and Choice and escape liability from privately brought contract claims.

One counterargument to this point is that the FTC polices privacy to a broad extent.[109] Although the FTC plays a central role in U.S. privacy enforcement, the agency has wielded its powers more conservatively than it could, focusing mainly on the most egregious offenders' violations of the most prevalent industry norms.[110] Thus, there might be privacy policy breaches of which the FTC is unaware, or instances where the agency declines to initiate investigation or enforcement action. For example, many of the early privacy policy breach cases resulted from the vignette played out in this Note's introduction. That is, in the aftermath of the 9/11 attacks, some airlines shared passenger information with Department of Defense contractors in violation of their privacy policies.[111] Given a similar context today, it is unlikely that government regulators would investigate or penalize the airlines for such a breach. In these

---

[107] *See supra* notes 85–90 and accompanying text.

[108] *See, e.g.*, CHRIS JAY HOOFNAGLE, ELEC. PRIVACY INFO. CTR., PRIVACY REGULATION: A DECADE OF DISAPPOINTMENT 3–5 (2005), http://epic.org/reports/decadedisappoint.pdf [https://perma.cc/Z96H-BWB5]; Mary J. Culnan, *Protecting Privacy Online: Is Self-Regulation Working?*, 19 J. PUB. POL'Y & MARKETING 20, 24–25 (2000)*; see also* ROBERT GELLMAN & PAM DIXON, MANY FAILURES: A BRIEF HISTORY OF PRIVACY SELF-REGULATION IN THE UNITED STATES 27 (2011), http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf [https://perma.cc/B6JB-CP6K].

[109] *See supra* notes 85–90 and accompanying text. *See generally* Solove & Hartzog, *supra* note 25, at 588–89 (defining the FTC's privacy enforcement efforts as developing a "privacy common law").

[110] *See* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2266 (2015).

[111] *See In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 325–27 (E.D.N.Y. 2005); *In re* Am. Airlines, Inc., Privacy Litig., 370 F. Supp. 2d 552, 556 (N.D. Tex. 2005); *In re* Nw. Airlines Privacy Litig., No. 04-126 (PAM/JSM), 2004 WL 1278459, at *1 (D. Minn. June 6, 2004); Dyer v. Nw. Airlines Corp., 334 F. Supp. 2d 1196, 1199 (D.N.D. 2004).

instances in which regulators do not act, privacy policies' non-binding effect means that individuals affected by breaches are left empty-handed.

This problem with Notice and Choice affects not only individuals. To the extent that website owners include risk management provisions (e.g., disclaimers, waivers, or arbitration clauses) in their privacy policies, policy owners risk these terms being rendered as legally irrelevant (from a contracting perspective) when these statements are held to be non-binding.[112] When their online terms are held unenforceable, websites and services are left governed by less favorable default legal rules and become, essentially, "legally naked."[113]

III. ALTERNATIVE SOLUTIONS FOR ALIGNING NOTICE AND CHOICE AND CONTRACT LAW

A. Form-Based Solutions

Form-based solutions might help bridge the gap between Notice and Choice and contract law. One solution would be to require that privacy policies are drafted as clickwrap agreements. If an individual manifests affirmative assent to a privacy policy's terms at the outset, it will be easier for her to establish that the terms form a binding agreement between her and the service. Likewise, it will be more difficult for her to, at a later date, argue that she lacked notice of the service's practices.

But businesses often view the clickwrap arrangement as inefficient and impractical, as they fear that website traffic will be negatively affected as a result of users' impeded access.[114] Accordingly, regulatory or legislative action would likely be required to affect this change. Similar regulatory attempts at term standardization

---

[112] *See* Eric Goldman, *How Zappos' User Agreement Failed in Court and Left Zappos Legally Naked*, TECH. & MARKETING L. BLOG (Oct. 29, 2012), http://blog.ericgoldman.org/archives/2012/10/how_zappos_user.htm [https://perma.cc/8GKZ-65WX].

[113] *Id.*

[114] *See* BALLON, *supra* note 56, at 26–27 n.38.

have been successful,[115] and state law to the same effect could be persuasive.[116]

Another form-based solution would be to incorporate, by reference, privacy policies with other terms of use. Because terms of use often include risk management provisions such as warranty disclaimers, liability limitations, and dispute resolution terms,[117] services take steps to make these binding on users.[118] While privacy policies have traditionally been stand-alone documents, if they are incorporated with other binding terms by reference, they would have stronger binding effect.[119]

A shortcoming of either of these suggestions is that individuals would still need to prove harm for their breach of contract claims to stand. Because proving harm in the privacy context is difficult to do,[120] this could be a significant hurdle. These approaches could, however, help users to establish reliance, which would aid claims for promissory estoppel and would at least keep their contract claims from being tossed aside based on policy, not contract interpretation.[121]

B. A Technical Solution

Technological tools in development could also bridge the gap between Notice and Choice and contract law. For example, a web browser plug-in to improve privacy policy usability is presently in

---

[115] *See, e.g.*, Final Model Privacy Form Under the Gramm-Leach-Bliley Act, 74 Fed. Reg. 62,890, 62,897 (Dec. 1, 2009). The Model Privacy Form is used as a safe harbor by financial institutions for compliance with certain disclosure requirements when issuing their privacy policies. *See id.* Similarly, the FTC has issued guidance designed to encourage and improve the drafting of warranties. *See Writing Readable Warranties*, FED. TRADE COMM'N (Jan. 1983), https://www.ftc.gov/tips-advice/business-center/guidance/writing-readable-warranties [https://perma.cc/YK8G-PTJR].

[116] *See supra* note 28 and accompanying text (describing how CalOPPA's privacy policy mandate imposes a de facto national privacy policy requirement).

[117] *See* Haynes, *supra* note 22, at 595–96.

[118] *See supra* notes 43–47.

[119] *See* Crowley v. CyberSource Corp., 166 F. Supp. 2d 1263, 1267–68 (N.D. Cal. 2001) (finding that because the privacy policy was not incorporated by reference, it did not apply in the actual contractual dispute).

[120] *See supra* notes 57–60 and accompanying text.

[121] *See supra* note 42 and accompanying text.

development.[122] The plug-in's goal is to provide users with clear, complete, and easily digestible information about the privacy policies of websites they visit.

The plug-in will take the form of a browser add-on that individuals can download, install, and use.[123] Once activated, the plug-in will employ natural language and machine learning techniques to automatically "read" and interpret the privacy policy of each website a user visits. The plug-in will then present the user with a just-in-time notice about the website's privacy practices, as articulated in the privacy policy.[124] The plug-in will present the user with a summary of information about the website's information practices

---

[122] The plug-in project is part of the Usable Privacy Project, a collaboration between Carnegie Mellon University and Fordham Law's Center on Law and Information Policy. *See* USABLE PRIVACY POL'Y PROJECT, https://www.usableprivacy.org/ [https://perma.cc/4A8Z-UDF9]. Because the plug-in is currently in the design and testing phase, there is no scholarly literature addressing it yet, but a project member has featured the plug-in on her blog. *See* Margaret Hagan, *Designing a Usable Online Privacy Tool*, OPEN L. LAB (July 22, 2015), http://www.openlawlab.com/2015/07/22/designing-a-usable-online-privacy-tool/ [https://perma.cc/VV7T-D6PJ].

[123] An example of a similar plug-in is Ghostery's browser extension, which enables users to view which third-party services track them when they visit a particular website and block those trackers, if desired. *See generally How Ghostery Can Help You,* GHOSTERY, https://www.ghostery.com/why-ghostery/for-individuals/ [https://perma.cc/X8M5-NMJE] (last visited Oct. 9, 2016).

[124] A just-in-time privacy notice serves snippets of privacy information as a service's practices call for (e.g., collection of a particular type of data), and are sometimes accompanied by a consent request (think of how some mobile apps notify you that they would like to use your geolocation data and ask you to authorize such use). The FTC has advocated for such just-in-time disclosures and has required them as part of enforcement agreements. *See, e.g.*, Decision and Order, Goldenshores Techs., LLC, No. 132 3087 (F.T.C. Mar. 31, 2014), https://www.ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf [https://perma.cc/M3YV-Q7QJ] (requiring flashlight app creator Goldenshores to provide just-in-time notice of how it collects and uses geolocation information, and also requiring Goldenshores to obtain "affirmative express consent" to the collection and use within the just-in-time notice); *see* FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 15–16, (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf [https://perma.cc/7Q5E-TK4J] (suggesting that mobile app platforms provide just-in-time notices to inform users about the collection of certain strains of sensitive information such as photos, contacts, and calendar entries). California's influential Attorney General has also advocated for just-in-time notices. *See* KAMALA D. HARRIS, CAL. DEP'T OF JUSTICE, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM 5 (2013), http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf [https://perma.cc/MWM2-RR3Z].

regarding sharing, collection, use, and other elements. Essentially, the plug-in will provide a shorthand version of the privacy policy so that users need not read the entire policy itself. The plug-in will also highlight options that the policy offers to users (e.g., the opportunity to opt out of certain data sharing or collection) and direct them on how to exercise those options. Through these features, the plug-in will allow users to make informed choices about whether to use the website or take action to protect their personal information while using it.

Installation and use of the plug-in could provide evidence of notice of privacy policy terms. This could help privacy policy breach plaintiffs establish that they relied on the policy terms, thus aiding claims based on a theory of promissory estoppel. The notice provided by a plug-in could also make it possible for courts to hold that the policy terms are binding even if the original policy takes browsewrap form, because, in interpreting browsewraps, courts "focus on whether the plaintiff had reasonable notice" of the browsewrap terms.[125] Courts have held that whether such agreements are binding depends on the website user's "actual or constructive knowledge" of the terms prior to using the website or service.[126] Thus, to be bound, the parties need not have an actual "meeting of the minds"[127]—rather, a reasonable communication of the agreement terms suffices to render the terms a binding agreement between the website and users.[128] The "reasonable communication" requirement is fulfilled through a combination of reasonable notice of and the opportunity to review terms, which serves as a "proxy for the offeree's clear manifestation of assent."[129] In the browsewrap context, "reasonable communication" can be manifested through a

---

[125] Burcham v. Expedia, Inc., No. 4:07CV1963 CDP, 2009 WL 586513, at *2 (E.D. Mo. Mar. 6, 2009) (citing Feldman v. Google, Inc., 513 F. Supp. 2d 229, 236 (E.D. Pa. 2007)).

[126] *Id.* at *3 n.5.

[127] *See* RESTATEMENT (SECOND) OF CONTRACTS § 17 cmt. c (AM. LAW INST. 1981) (explaining that though an agreement in a contract can be understood as a 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").

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

[129] *See* Juliet M. Moringiello, *Signals, Assent and Internet Contracting*, 57 RUTGERS L. REV. 1307, 1314 (2005).

conspicuous display of the terms.[130] A browser plug-in that automatically conveys to users the privacy terms of every website they visit could provide sufficient reasonable communication to render those terms binding. This would have the effect of making a website or service's privacy policy statements binding between the service and the user, and would make any privacy policy violation a breach of the privacy contract.

Nevertheless, legal and practical issues surround the use of this sort of technical tool. For example, courts may not consider the plug-in's notice a valid "reasonable communication" of a website's privacy terms because the plug-in is an independent technology not offered by any website itself. A court might be reluctant to give a policy binding effect when its drafter lacked the intent to make it binding.[131]

Even if courts were to accept the plug-in as a valid "reasonable communication," an issue remains regarding uniform use and application. For example, if an individual uses the plug-in to receive notice of and establish reliance on the policy, the policy should be binding as between the individual and the website or service. But the same policy would *not* be binding as to the website or service and an individual who did not download and use the plug-in.

Another issue relates to plug-in design. Whether due to purposefully open-ended drafting or the use of intentionally vague terms, privacy policies are often ambiguous.[132] Accordingly, there is the risk that the natural language processing and machine learning tools upon which the plug-in is built may inaccurately interpret privacy policy statements, and thus provide users with a less-than-accurate notice of what the policy means to convey. It would be difficult, and possibly unfair, for a court to enforce terms for which inaccurate notice was given.

---

130 *See* Rambarran & Hunt, *supra* note 37, at 176.

131 *See* Sulzbach v. Town of Jefferson, 155 N.W.2d 921, 923 (S.D. 1968) ("It is not necessary that the parties are conscious of the legal relationship which their words or acts give rise to, but it is essential that the acts manifesting assent shall be done intentionally."); RESTATEMENT (SECOND) OF CONTRACTS § 21 (AM. LAW INST. 1981) ("Neither real nor apparent intention that a promise be legally binding is essential to the formation of a contract, but a manifestation of intention that a promise shall not affect legal relations may prevent the formation of a contract.").

132 *See* Reidenberg et al., *supra* note 32.

And finally, the issue of harm remains. Even if all the issues discussed above resolve in such a way that a user can cite to her use of the plug-in to establish notice and reliance, she must still allege harm resulting from any breach. But like the form-based solution described above, technological tools might at least help users establish reliance and thus ground their claims in contract theory.

CONCLUSION

Privacy policies are the primary mechanism for effectuating the Notice and Choice model for protecting privacy online. Though they may seem to be contractual, jurisprudence dictates that privacy policies typically lack binding effect between individuals and websites or online services. This means that in some circumstances where websites or online services engage in information practices that differ from those stated in their privacy policies, individual users lack the opportunity to seek redress on contractual grounds. This result is at odds with the objectives of and rationales for Notice and Choice. Though form- and technology-based solutions might bridge the gap between Notice and Choice and contract law, these solutions may not be immediately practicable and questions remain as to whether and how they would work, even if they were available.

Overall, this Note shines a light on Notice and Choice and presents a new critique of the model. This critique raises questions about the model's efficiency, and more generally, it raises normative issues about the best means of protecting individual privacy in the online context.