Fordham Urban Law Journal

Volume 42 | Number 5 Article 1

2015

You Didn't Even Notice! Elements of Effective Online Privacy Policies

Amanda Grannis

YOU DIDN'T EVEN NOTICE! ELEMENTS OF EFFECTIVE ONLINE PRIVACY POLICIES

Amanda Grannis[*]

Introduction 1110
I. The Landscape of Notice in U.S. Privacy Law.....1113
A. The Federal Trade Commission and Notice and Choice .1113
B. The FTC's Harm-Based Model 1116
C. Statutory Protections of Privacy 1118
D. Common Law Notice Standards Applied to the Digital Age.....1120
II. Exploring the Elements of Effective Legal Notice 1123
A. Arbitration Clauses Viewed as Contracts: Actual and Constructive Notice 1123
1. Contract Remedies for Insufficient Notice of Arbitration Clauses.....1128
2. Arbitration Clauses Viewed as Waivers: The "Voluntary and Knowing" Standard.....1131
B. FDA Labeling Rules.....1134
1. Standardized Content in FDA Labeling Rules 1135
2. User-friendly Formatting 1136
3. Symbolic Visual Cues 1139
C. FTC Enforcement Actions.....1140
1. Unauthorized Disclosure of Personal Information.....1141
2. Surreptitious Collection of Personal Information.....1142
3. Failure to Secure Personal Information 1145
4. Unlawful Retention of Personal Information.....1146

---

[*] J.D., Fordham University School of Law, 2016; B.A., Binghamton University, 2012. I would like to thank my wonderful professor Joel Reidenberg, who advised me throughout the note writing process. I could not have written this article without his remarkable guidance and insights. I would also like to thank Professor Cameron Russell of the Fordham Center on Law and Information Policy (CLIP), who helped inspire me to write this note. I would also like to thank my eternally supportive parents Mark and Sandra Grannis, who have helped me every step of the way throughout law school. Finally, I would like to thank Josh Lampert, who has been a constant source of love and encouragement.

D. Notice Problems in the Online World 1146
1. The Cost of Reading Privacy Policies 1147
2. Ambiguity and Consumer Misunderstanding 1149
a. Ambiguity of Privacy Policy Language 1149
b. Misunderstanding of Privacy Policy Text 1151
c. False Assumptions and Lack of Awareness 1152
III. Elements of Effective Online Notice 1154
A. The Format of Effective Notice 1155
1. Readable Text 1155
2. Conspicuous Disclosures 1158
B. The Content of Effective Notice 1160
1. Accurate Disclosures 1160
2. Precise Language 1161
3. Affirmative Consent to Modified Material Terms 1163
4. "Knowing and Voluntary" Assent 1164
Conclusion 1166

INTRODUCTION

On February 5, 2015, electronic retailer RadioShack filed for Chapter 11 bankruptcy protection.[1] RadioShack previously announced that it planned to sell the personally identifiable information of 117 million consumers in asset auctions across several states.[2] The following month, RadioShack sought to sell its "transaction data," along with 8.5 million customer email addresses and 67 million customer names and address files.[3] This trove of personal data would be a valuable asset to third party marketers,[4] as it would reveal what items customers purchased, where they purchased it, and how much they paid.[5]

Ultimately, a bankruptcy judge approved the sale of RadioShack's customer data for $26 million, which after negotiations sold the names

---

1. Katy Stech, *Privacy Concerns Raised as RadioShack Prepares to Sell Customer Data*, WALL STREET J. (Apr. 28, 2015), http://www.wsj.com/articles/privacy-concerns-raised-as-radioshack-prepares-to-sell-customer-data-1430252834 [https://perma.cc/2FCF-G3MJ].

2. Randall Chase, *RadioShack Agrees To Mediation With Attorneys General Over Bankruptcy Sale Of Customer Data*, U.S. NEWS (Apr. 28, 2015), http://www.usnews.com/news/business/articles/2015/04/28/radioshack-agrees-to-mediation-over-sale-of-customer-data [https://perma.cc/V5UJ-WRMQ].

3. Chase, *supra* note 2.

4. *See* Stech, *supra* note 1.

5. Chase, *supra* note 2.

and addresses of 67 million former customers.[6] This controversial sale not only alarmed the public and state regulators, but arguably directly breached RadioShack's privacy policy.[7] Indeed, RadioShack's privacy policy provided that it would not "sell or rent" customers' "personally identifiable information to anyone at any time."[8] RadioShack's privacy policy also claimed that it "respect[ed]" customer's privacy, and would abstain from selling its mailing lists.[9] How could RadioShack break its own privacy promises and operate against former assurances to customers?

The RadioShack case typifies systematic problems of privacy policies and online notice. Sometimes, companies like RadioShack will break their own promises to customers, and appropriate consumer data in ways that the average consumers would not anticipate.[10] More often, however, privacy policies are vague or silent about core data practices.[11] Commercial websites often collect, share, and retain consumer information without mentioning these practices or disclosing their specific details in privacy policies.[12] Furthermore, the verbose and legalistic character of policy language often makes it difficult for consumers to understand privacy terms,[13] and the format of privacy policies deters consumers from reading them. Research shows that the majority of consumers do not read privacy policies[14] and this may be because they are often displayed in dense paragraphs of crowded text.

---

6. *See* Nick Brown, *U.S. Judge Rules RadioShack IP Auction Was Fair*, REUTERS (May 20, 2015), http://www.reuters.com/article/us-radioshack-bankruptcy-idUSKBN0O52I120150520 [https://perma.cc/SYC9-7GML].

7. *See* State Of Texas's Limited Objection To Sale Of Personally Identifiable Information Of One Hundred Seventeen Million Consumers, *In re* RadioShack Corporation, et al., 2015 WL 641870, No. 15-10197-KJC, 3 (Bankr. Del. Mar. 20, 2015) (No. 1393).

8. *Id.*

9. *Id.* at 3-4.

10. *See, e.g.,* Complaint, at 2, *In re* Upromise, Inc., FTC File No. 102 3116, No. C-4351 (F.T.C. Mar. 27, 2012) [hereinafter Upromise Complaint].

11. *See* J. R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 87 (2015).

12. *See Fact Sheet 18: Online Privacy: Using the Internet Safely*, PRIVACY RTS. CLEARING HOUSE (Jan. 2016), https://www.privacyrights.org/online-privacy-using-internet-safely [https://perma.cc/8KHF-JV2M].

13. *See* Irene Pollach, *What's Wrong with Online Privacy Policies?*, 50 COMM'N OF THE ACM 103, 104 (2007).

14. *See* Sarah Gordon, *Privacy: A Study of Attitudes and Behaviors in US, UK and EU Information Security Professionals*, SYSTEMATIC SECURITY RESPONSE 12 (2003).

In response to these prevalent issues, this Note explores how companies alter their privacy policies so that they will become usable notice mechanisms of online data collection and dissemination practices. Part I analyzes common law and statutory sources of notice regulation in the United States. Part I also addresses the Federal Trade Commission's (FTC) privacy jurisprudence as well as notice and choice, the dominant model for displaying and attaining users consent to the terms of online privacy policies.

Part II examines and extracts the most salient principles of effective notice from established relevant legal models. Each legal model represents a different aspect of commercial practice, and their notice standards thus provides valuable insights for conveying effective notice in the context of commercial websites and online consumer transactions. To illustrate greater standards of notice in the domain of commercial contracts, this section first studies notice requirements of enforceable arbitration agreements. The second legal model discussed is the Food and Drug Administration's (FDA) over-the-counter (OTC) drug labeling rule. This section examines FDA labeling practices to highlight what constitutes sufficient notice and warnings in highly regulated industries. Part II then describes different FTC enforcement actions that relate to consumer privacy harms as a reflection of greater notice and privacy standards of general commercial entities. Part II concludes with an overview of some of the most prominent issues pertaining to online notice today.

Part III extrapolates core principles from the three legal models to articulate the elements of effective online notice. This Note does not purport to outline an exhaustive list of essential elements. Rather, these elements are intended to inform expectations of what effective notice should be in the online world. These elements pertain to both the format and content of effective notice, as each of these aspects has a vital impact on consumer understanding of privacy terms. Part III also discusses what tactics commercial websites should implement to sufficiently communicate the nature and scope of their data collection practices to consumers. Moreover, this Part offers a greater analytical framework for addressing online notice problems.

I. THE LANDSCAPE OF NOTICE IN U.S. PRIVACY LAW

A. The Federal Trade Commission and Notice and Choice

Privacy law in the United States is often described as "sectoral"[15] because there is no one dominant source of privacy legislation.[16] Privacy laws operate like a patchwork quilt of various state law privacy torts, federal statutes, and administrative rules.[17] In terms of government regulation, the Federal Trade Commission (FTC) is the main federal agency that regulates the privacy space.[18] Congress created the FTC in 1914 after it enacted the Federal Trade Commission Act (FTCA) to protect consumers and promote competition.[19] In 1995, the FTC began to shift its focus to online consumer privacy issues,[20] as the Internet was becoming more ubiquitous and the online marketplace was burgeoning.[21] During this time, the FTC endorsed a policy of privacy self-regulation, in which it entrusted consumers to make their own decisions and judgments about their privacy.[22] The FTC began to clarify and define this model of privacy self-regulation in a 2000 report.[23] In the report, the FTC determined that commercial entities that collected consumers' personally identifiable data must comply with the "fair information practice principles" of "Notice" and "Choice."[24] The FTC explained

---

15. Sectoral refers to the various sources of privacy law.

16. *See* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 910 (2009).

17. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014) (referring to U.S. privacy law as a "hodgepodge" of different "constitutional protections, federal and state statutes, torts, regulatory rules, and treaties"); *see also* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 887–89 (2003).

18. *See* Solove & Hartzog, *supra* note 17, at 587.

19. *See Our History*, THE FEDERAL TRADE COMMISSION, https://www.ftc.gov/about-ftc/our-history [https://perma.cc/HD2D-5JZK].

20. FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 2 (1998)

21. *Id.* at 40. ("The World Wide Web provides a host of opportunities for businesses to gather a vast array of personal information from and about consumers, including children. The online environment and the advent of the computer age also provide unprecedented opportunities for the compilation, analysis, and dissemination of such information.").

22. *See* Gina Stevens, *The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority*, CONG. RES. SERVS. 3 (Sept. 11, 2014).

23. *See* Federal Trade Commission, *Privacy Online: Fair Information Practices In The Electronic Marketplace A Report To Congress* (May 2000) [hereinafter *Privacy Online*]. The Commission named four information practice requirements in total: Notice, Choice, Access, and Security.

24. *See id.* at 12.

that "Notice" required entities to give consumers "clear and conspicuous notice" of their information practices "before any personal information is collected."[25] The FTC stated that "Notice" was the "most fundamental" principle because it was a "prerequisite to implementing other fair information practice principles, such as Choice."[26] According to the principle of "Choice," entities must give consumers options pertaining to how "any personal information collected . . . may be used for purposes beyond those necessary to complete a contemplated transaction."[27] Such "purposes" may include sharing consumer information with third parties or using it for marketing products.[28]

The FTC premised the notice and choice model on the belief that companies would disclose their data collection practices to consumers, and consumers would self-manage their privacy by offering or denying their consent.[29] The FTC asserted that privacy notices should be seen as a way to help consumers understand what information is collected about them and what is done with that information.[30] In response to the FTC's endorsement of a policy of privacy self-regulation, companies began to draft and post privacy policies on their commercial websites.[31] Not only could these policies promote companies' privacy practices, but could also help to "stave off" formal privacy regulations from Congress.[32] Eventually, privacy policies became fairly ubiquitous in online commercial practice.[33] In 1998, only two percent of websites displayed privacy policies—by 2000, nearly all websites featured them.[34]

---

25. *Id.* at 14.

26. *Id.* at 14.

27. *Id.* at 15.

28. *Id.* at 15-16.

29. *See* Lorrie Faith Cranor, *Necessary But Not Sufficient: Standardized Mechanisms For Privacy Notice And Choice*, 10 J. ON TELECOMM. & HIGH TECH. L. 273, 277-79 (2012).

30. *See* Howard Beales, Dir., Bureau of Consumer Prot., *Privacy Notices and the Federal Trade Commission 2002 Privacy Agenda*, 2002 WL 1713227 (Jan. 24, 2002), https://www.ftc.gov/public-statements/2002/01/privacy-notices-and-federal-trade-commissions-2002-privacy-agenda [https://perma.cc/6ZGG-VYLA].

31. *See* Solove & Hartzog, *supra* note 17, at 592-95 (explaining that as a general matter, privacy policies describe websites' terms of use and the nature of their data collection practices and privacy policies have the same binding force as any other legal contract and are usually featured on a separate webpage of a website).

32. *See* Solove & Hartzog, *supra* note 17, at 594.

33. *See* Solove & Hartzog, *supra* note 17, at 594.

34. Solove & Hartzog, *supra* note 17, at 594.

The self-regulatory regime of notice and choice remains in place today.[35] Companies display disclosure statements pertaining to their data collection practices on their websites, and consumers can choose to read those disclosures and decide to consent to privacy terms.[36] Nevertheless, in 2000, the FTC reported that only about twenty percent of privacy policies that were studied implemented, at least in part, the criteria for the "Fair Information Practice Principles."[37] The FTC determined that privacy legislation, in addition to self-regulation, would allow the "electronic marketplace to reach its full potential" and increase consumer confidence.[38] Congress did not enact the recommended legislation, and the FTC began to increasingly rely on its statutory authority in order to protect consumers' privacy.[39]

The FTC's statutory grant of power enables it to enforce the promises that companies make in their privacy policies.[40] The FTC's statutory authority arises from Section 5 of the FTCA.[41] Section 5 states that "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are . . . unlawful."[42] Pursuant to Section 5, the FTC files complaints against companies that engage in "unfair" or "deceptive" online practices.[43] Though the FTC provides no enumerated examples of "unfair" and "deceptive" commercial practices,[44] the FTC interprets this language to include unfair and deceptive uses of consumers' personal information.[45] The FTC defines a deceptive practice as one that is a "representation, omission or practice that is likely to mislead

---

35. *See* Cranor, *supra* note 29, at 277.

36. *See* Cranor, *supra* note 29, at 277.

37. *See Privacy Online*, *supra* note 23, at 12-13.

38. *See* FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 8 (Dec. 2010) [hereinafter PROTECTING CONSUMER PRIVACY].

39. *See id.*

40. *See* Solove & Hartzog, *supra* note 17, at 598.

41. *See* Federal Trade Commission Act, 15 U.S.C. § 45 (2012).

42. 15 U.S.C. § 45(a)(1).

43. *See* Solove & Hartzog, *supra* note 17, at 598-99.

44. *See* Fed. Trade Comm'n v. R.F. Keppel & Bro., 291 U.S. 304, 312 n.2 ("It is impossible to frame definitions which embrace all unfair practices. There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again. If Congress were to adopt the method of definition, it would undertake an endless task" (quoting H.R. Conf. Rep. No.1142, 63rd Cong., 2d Sess. 19 (1914))).

45. *Division of Privacy and Identity Protection*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity [https://perma.cc/5EE8-AXUL].

the consumer acting reasonably in the circumstances, to the consumer's detriment."[46] Generally, a misleading act or broken promise, such as when companies breach their own privacy policies, will satisfy this language.[47] The FTC maintains that an "unfair practice" is one that causes or is likely to cause "substantial injury" that is not "reasonably avoidable" or "outweighed by countervailing benefits to consumers or competition."[48] An "unfair practice" need not entail a misleading act or broken promise.[49] Rather, "unfair" practices include monetary, health or safety injuries.[50]

B. The FTC's Harm-Based Model

In the early 2000s, the FTC focused on addressing harms to online consumers as a means of confronting greater privacy issues.[51] Under its harm-based model, the FTC advanced online consumer protection claims in response to known privacy harms, which included data security breaches, identity theft, children's privacy and spyware.[52] The number of FTC privacy enforcement actions has since grown steadily since the FTC first started to address and regulate privacy harms online.[53] This growth is likely in response to companies' new business models that collect and share online consumers' personally identifiable information. For example, online social media networks capture consumer data through personalized account profiles.[54] Likewise, location-based mobile applications, which provide consumers with uses like navigation services and weather reports,

---

46. FTC Policy Statement on Deception (1983), *appended* to Final Order, Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984), http://www.ftc.gov/bcp/policystmt/ad-decept.htm [https://perma.cc/E289-HBV5];

47. *See* Joel R. Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework,* FORDHAM CTR. ON L. & INFO. POL'Y, 19 (2014), http://moritzlaw.osu.edu/students/groups/is/files/2015/01/Privacy-Harms-and-Notice-and-Choice-01-12-2015-1-4.pdf [https://perma.cc/3YRL-LLK8]. Companies that do not have privacy policies, or fail to include certain provisions in their privacy policies, will not be charged with committing "deceptive" practices. Rather, companies must make positive statements in their privacy policies that mislead consumers' expectations of privacy. *Id.*

48. 15 U.S.C. § 45(n) (2012).

49. *See* Reidenberg et al., *supra* note 47, at 19.

50. *See* Reidenberg et al., *supra* note 47, at 19.

51. *See* PROTECTING CONSUMER PRIVACY, *supra* note 38, at 9.

52. *See* PROTECTING CONSUMER PRIVACY, *supra* note 38, at 10.

53. Solove & Hartzog, *supra* note 17, at 600 (observing that the FTC brought nine privacy-related complaints in 2002, but brought twenty-four privacy-related complaints in 2012).

54. *See* PROTECTING CONSUMER PRIVACY, *supra* note 38, at 58.

gather satellite information on consumers' geographic location.[55] More so, online behavioral advertisers market personalized products and services to consumers on the web by tracking consumers' browsing habits over time.[56]

Due to technological advancements and increased computing power, many companies are now capable of collecting a variety of consumer data in vast amounts.[57] Some of this data may include personally identifiable information like consumers' Social Security numbers, names, addresses, telephone numbers, credit or debit card numbers, bank account numbers, driver's license numbers, or precise-geolocation data.[58]

Companies also profit from the consumer data that they collect and share. Companies may collect personal data and proceed to sell or rent it to third parties.[59] They may also share this information with marketing affiliates in order to profile the behavior of users that visit their websites.[60] Companies may also share this information with third party behavioral advertisers, which rely on consumer data to deliver personalized advertising.[61] Companies often fail to disclose how long they retain consumer data after collection.[62] However, some companies have retained consumer data for extended periods, and as seen with RadioShack, can even attempt to sell off their databases during bankruptcy.[63]

As companies found new ways to collect and share a greater quantity and variety of data, the FTC filed a greater number of complaints in response to incidental privacy harms.[64] Some of the alleged privacy harms cited in such complaints are linked with findings of insufficient notice. For example, the FTC has filed

---

55. *See* PROTECTING CONSUMER PRIVACY, *supra* note 38, at 21.

56. *See* PROTECTING CONSUMER PRIVACY, *supra* note 38, at 21. *See generally* Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent*, PROCEEDINGS OF THE ENGAGING DATA FORUM: THE FIRST INTERNATIONAL FORUM ON THE APPLICATION AND MANAGEMENT OF PERSONAL ELECTRONIC INFORMATION (2009).

57. *See* PROTECTING CONSUMER PRIVACY, *supra* note 38, at 21.

58. *See In re* HTC Am. Inc., FTC File No. 122 3049, No. C-4406, at 2 (F.T.C. June 25, 2013).

59. *See* JOSHUA GOMEZ ET AL., KNOW PRIVACY, U.C. BERKELEY, SCHL. OF INFO. 9 (Jun. 1, 2009).

60. *See id.*

61. *See* Barocas & Nissenbaum, *supra* note 56, at 1.

62. *See* GOMEZ ET AL., *supra* note 59, at 25.

63. *See* Stech, *supra* note 1; *see generally* Brian Carroll, *Price of Privacy: Selling Consumer Databases in Bankruptcy*, 16 J. INTERACTIVE MKTG. 47 (2002).

64. *See* Solove & Hartzog, *supra* note 17, at 600.

complaints against companies that fail to apprise consumers of their data collection practices.[65] The FTC's position is that without proper disclosure of data collection practices, consumers can not offer informed consent.[66] Similarly, the FTC has filed complaints against companies for collecting consumer data without consumers' knowledge.[67] Some complaints allege instances of privacy harm when companies offer consumers installable software that, unbeknownst to consumers, collects personally identifiable information.[68] FTC jurisprudence characterizes such covert collection as a "deceptive" under Section 5.[69]

After filing a complaint, the FTC grants the respondents the option to settle or dispute the charges in administrative court.[70] Most cases, however, are dropped or settled through the FTC's consent orders, which are similar to settlement agreements.[71] Though consent orders have the legal force of a contract between the FTC and respondent company, they sometimes, as a practical matter, have precedential value.[72] Other companies that read these orders may opt to comply with them in order to avoid similar charges for privacy harms.[73]

C. Statutory Protections of Privacy

In addition to FTC enforcement actions, some federal laws also define and protect consumers' privacy rights. These statutes tend to be directed toward a specific industry or sector, and the FTC often

---

65. *See e.g.,* Complaint, FTC v. Frostwire LLC, FTC File No. 112 3041, No. 111-cv-236443 (F.T.C. Oct. 7, 2011); Complaint, *In re* Red Zone Inv. Grp., Inc. FTC File No. 112 3151, No. C-4396 (F.T.C. Apr. 11, 2013).

66. *See* PROTECTING CONSUMER PRIVACY, *supra* note 38, at 25-26.

67. *See*, *e.g.,* Complaint, *In re* Aspen Way Enters., Inc., FTC File No. 1123151, No. C-4392 (F.T.C. Sept. 25, 2012) (collecting user data through secretly installed software on rental computers) [hereinafter *In re* Aspen Way Complaint]; Complaint, *In re* Epic Marketplace, Inc., File No. 112 3182, No. C-4389 (F.T.C. Dec. 5, 2012) (collecting browsing history data).

68. *See* Upromise Complaint, *supra* note 10, at 5.

69. *See In re* Aspen Way Complaint, *supra* note 67, at 5.

70. *See* Solove & Hartzog, *supra* note 17, at 609.

71. *See* Solove & Hartzog, *supra* note 17, at 610, 611 n.120 (noting that out of 154 FTC complaints, only six lacked an accompanying settlement agreement).

72. *See* Solove & Hartzog, *supra* note 17, at 607.

73. *See* Solove & Hartzog, *supra* note 17, at 607 ("[A]lleged violations precipitating the consent orders reflect conduct the FTC believes is a violation of Section 5 . . . and companies that engage in the same or similar conduct can expect an investigation and an allegation of illegal conduct from the FTC" (quoting Email from Chris Wolf, Dir., Privacy & Info. Mgmt. Grp., Hogan Lovells, to author (Mar. 31, 2013, 11:21 AM) (on file with the *Columbia Law Review*)).

has authority to enforce them.[74] The Gramm-Leach-Bliley Act, for example, prohibits financial institutions from disclosing consumers' non-public personal information to unaffiliated third parties.[75] Pursuant to the Act, financial institutions are obliged to provide notices of their privacy policies to consumers and to give consumers reasonable opportunity to opt-out of disclosing personal information to third parties.[76] Compliant financial institutions must supply a notice statement of their privacy policies at the time a consumer relationship is established and at least once every twelve months thereafter.[77] In addition to the Gramm-Leach-Bliley Act, the privacy rule of the Health Insurance Portability and Accountability Act (HIPAA) protects personally identifiable health information held or transmitted by health plans, insurers, and health providers.[78] HIPAA prohibits the unauthorized disclosure of information relating to patients' identities or health status.[79] Such information includes patients' medical histories, payment records, Social Security numbers, names, addresses, and email addresses.[80]

State laws also reserve special privacy rights for citizens.[81] For instance, California's Online Privacy Protection Act of 2003 requires commercial websites that collect personally identifiable information to prominently post privacy policies and identify the kinds of data they collect from consumers.[82] Under this law, websites must disclose any processes that they maintain for allowing consumers to review and change their personally identifiable information.[83] California law not only regulates how websites may disclose their privacy practices, but also how they collect consumer data.[84] California's

---

74. *See* PROTECTING CONSUMER PRIVACY, *supra* note 38, at 4.

75. The Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et. seq. (2012).

76. 15 U.S.C. § 6802.

77. 15 U.S.C. § 6803.

78. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 26 U.S.C., 28 U.S.C., and 42 U.S.C.); 45 C.F.R. §§ 164.103, 164.500 (2013).

79. 45 C.F.R. §§ 164.103, 164.502 (2013).

80. 45 C.F.R. § 164.514(2)(i) (2013). Beyond the Gramm–Leach–Bliley Act and HIPAA, other federal privacy statutes, such as the CAN-SPAM Act (which regulates how commercial entities send advertising emails to consumers), and the Telemarketing and Consumer Fraud and Abuse Prevention Act, were also enacted to protect privacy. *See* 5 U.S.C. § 7701 *et seq.* (2012); 15 U.S.C. § 6101 *et seq.* (2012).

81. *See e.g.,* California Invasion of Privacy Act, CAL. PENAL CODE § 630 *et seq.* (West 2015).

82. Online Privacy Protection Act, CAL. BUS. & PROF. CODE § 22575-22579 (West 2015).

83. CAL. BUS. & PROF. CODE § 22575(b)(2).

84. *See* CAL. BUS. & PROF. CODE § 22575-22579.

Consumer Protection Against Computer Spyware Act prohibits unauthorized users from knowingly copying software on consumers' computers to surreptitiously collect personally identifiable information that "includes all or substantially all of the Web sites visited by an authorized user."[85] This law prohibits companies from installing spyware on the computers of unknowing consumers.[86]

D. Common Law Notice Standards Applied to the Digital Age

Principles of effective notice are central to privacy-related enforcement actions as well as to some federal and state privacy statutes. Demonstrating effective notice is also critical throughout traditional legal areas, such as tort law,[87] corporate law,[88] and property law.[89] The principle of notice is of particular importance to common law contracts.[90] Contract theory is premised on the reasoning that parties have "freedom of contract."[91] The ability to enter contacts has traditionally been viewed as a "fundamental" right because it reflects parties' liberties to control the disposition of their property and alter

---

85. Consumer Protection Against Computer Spyware Act, CAL. BUS. & PROF. CODE § 22947.2 (West 2015).

86. *See* CAL. BUS. & PROF. CODE § 22947.3 (West 2015).

87. *See generally* Bremer v. W. W. Smith, Inc., 126 Pa. Super. 408 (1937) (holding that proof of an injured party's notice of hazardous conditions provided a defense in a premises liability suit). *But see* Mack v. Pittsburgh Rys. Co., 93 A. 618 (Pa. 1915) (holding defendant railroad had constructive notice of a grease spot due to the presence of footprints and was negligent because it did not apprise injured parties with a proper warning of hazardous conditions).

88. *See generally In re* Citigroup Inc. S'holder Derivative Litig., 964 A.2d 106 (Del. Ch. 2009) (demonstrating Delaware courts' reference to the "Red Flag" doctrine when imposing a duty to monitor upon directors who know or have reason to know of employees' illegal conduct).

89. *See* 3 Am. Jur. 2d Adverse Possession § 57 (2015) (providing adverse possession of land must be "open and notorious" in order to put landowners on sufficient notice of the trespass of their property).

90. *See* RESTATEMENT (SECOND) OF CONTRACTS: CONTRACTS DEFINED § 1 (AM. LAW INST. 1981) ("A contract is 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.").

91. *See Slaughter-House Cases*, 83 U.S. (16 Wall.) 36, 89 (1873) (holding that citizens have the right to contract without unreasonable government interference and that this right was protected by the due process clause of the Fourteenth Amendment). *See generally* David E. Bernstein, *Freedom of Contract*, GEO. MASON L. & ECON. RES. PAPER SERIES, No. 08-51 (2008), http://www.law.gmu.edu/assets/files/publications/working_papers/08-51%20Freedom%20of%20Contract.pdf [https://perma.cc/3LAU-FJ7Z] (discussing the notion of freedom of contact and its place in U.S. Jurisprudence).

their legal relationships.[92] By their very nature, contracts enable parties to structure an agreement on their own terms and attribute that agreement with legally binding status.[93] However, if a party does not receive sufficient notice of a contract's substantive terms at the formation stage, the agreement may be unenforceable.[94] This is because parties may not be able to meaningfully assent to terms that they are unaware of or do not understand.[95] Contracts are only enforceable if both parties mutually agree to their conditions.[96]

Models of sufficient notice in common law contracts have shaped legal precedents in the privacy space. In the landmark case *Specht v. Netscape Communications Corp.*, then-Second Circuit Judge Sotomayor relied on traditional notice principles when concluding that that plaintiffs did not manifest consent to an arbitration clause in a browsewrap licensing agreement.[97] In browsewrap agreements, websites display their terms of use at the bottom of a webpage.[98]

---

92. *See* David P. Weber, *Restricting the Freedom of Contract: A Fundamental Prohibition*, 16 YALE HUM. RTS. & DEV. L.J. 51, 56 (2013).

93. The process of contract formation entails the formal steps of offer, a bargained-for exchange (also known as consideration) and acceptance of the offer. Fiederlein v. Boutselis, 952 N.E.2d 847, 856 (Ind. Ct. App. 2011) ("The basic requirements for a contract include offer, acceptance, consideration, and a meeting of the minds of the contracting parties.").

94. *See* RESTATEMENT (SECOND) OF CONTRACTS: REQUIREMENT OF A BARGAIN § 17 (1981) ("[T]he formation of a contract requires a bargain in which there is a manifestation of mutual assent to the exchange and a consideration.").

95. *See* Douglas v. U.S. Dist. Court for Cent. Dist. Of Cal., 495 F.3d 1062 (2007) ("[A]n offeree cannot actually assent to an offer unless he knows of its existence.") (quoting 1 SAMUEL WILLISTON, A TREATISE ON THE LAW OF CONTRACTS § 4:13 (Richard A. Lord ed., 4th ed. 1990)); Trimble v. N.Y. Life Ins. Co., 234 A.D. 427, 431 (N.Y. App. Div. 1932) ("An offer may not be accepted until it is made and brought to the attention of the one accepting.").

96. *See* RESTATEMENT (SECOND) OF CONTRACTS: REQUIREMENT OF A BARGAIN § 17. *See also* Motise v. Am. Online, Inc., 346 F. Supp. 2d 563, 564-65 (S.D.N.Y. 2004) (holding that the plaintiff was not bound by AOL's forum selection clause because the agreement failed to appear "on screen," and the plaintiff was not given enough notice); Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN ST. L. REV. 587, 613 (2007) ("The most obvious challenge to the enforceability of an online privacy policy as a binding contract is that the website visitor failed to assent to the agreement. A contract is only enforceable if both parties have manifested their assent to its terms").

97. 306 F.3d 17, 32 (2d Cir. 2002).

98. *See* Nguyen v. Barnes & Noble Inc., 763 F.3d 1171, 1176 (9th Cir. 2014) (explaining in "'browsewrap' agreements . . . a website's terms and conditions of use are generally posted at the bottom of the screen," and that "'[u] nlike a clickwrap agreement, a browsewrap agreement does not require the user to manifest assent to the terms and conditions expressly . . . [a] party instead gives his assent simply by using the website.'") (quoting Hines v. Overstock.com, Inc., 668 F. Supp. 2d 362, 366–67 (E.D.N.Y. 2009)).

Online users do not have to expressly consent to browsewrap terms, as websites will typically interpret continued use of their services as acceptance of the agreement.[99]

The plaintiffs in *Specht* downloaded SmartDownload software, which Netscape owned.[100] The plaintiffs then sued Netscape after learning that the SmartDownload software surreptitiously gathered their online data and transmitted it to Netscape.[101] Netscape then argued that the plaintiffs were bound to arbitrate these claims.[102] In support of its contention, Netscape pointed to the existence of an arbitration provision in the SmartDownload browsewrap agreement, which Netscape argued plaintiffs had accepted by using the software.[103]

The court held that the plaintiffs were not bound by the arbitration provision because they did not have sufficient notice of its existence.[104] Judge Sotomayor, writing for the majority, observed that SmartDownload users would have had to scroll down to the very bottom of their computer screens in order to access the browsewrap licensing agreement.[105] Even if an Internet user did scroll down to the bottom of the page, they would have only seen a hyperlink[106] to the browsewrap agreement, rather than the licensing agreement itself.[107] Users would then have had to click on the hyperlink, located at the bottom of the screen, to be directed to a separate webpage that featured the licensing agreement and arbitration provision.[108] Judge Sotomayor concluded that a "reasonably prudent" Internet user would not have had a basis for learning of or inquiring about the existence of the arbitration provision.[109] She determined that the

---

99. *See id.* ("[I]n a pure—form browsewrap agreement, 'the website will contain a notice that—by merely using the services of, obtaining information from, or initiating applications within the website—the user is agreeing to and is bound by the site's terms of service') (quoting Fteja v. Facebook, Inc., 841 F.Supp.2d 829, 837 (S.D.N.Y.2012)).

100. *Specht*, 306 F.3d at 21.

101. *Id.* at 21.

102. *Id.* at 25.

103. *Id.* at 24.

104. *Id.* at 28, 30 (finding "[c]larity and conspicuousness of arbitration terms are important in securing informed assent").

105. *Id.* at 23.

106. A hyperlink is "a highlighted word or picture in a document or Web page that you can click on with a computer mouse to go to another place in the same or a different document or Web page." *See Hyperlink*, MERRIAM-WEBSTER (2016), http://www.merriam-webster.com/dictionary/hyperlink [https://perma.cc/52PJ-42JA].

107. *Specht*, 306 F.3d at 23.

108. *Id.*

109. *Id.* at 30.

plaintiffs never manifested their "unambiguous assent" to the arbitration provision, as it was not sufficiently visible to them upon installing SmartDownload.[110] The plaintiffs had no knowledge of the arbitration agreement, and therefore, did not have opportunity to accept or reject its terms.[111] Because the plaintiffs never assented to the arbitration clause, their continued use of the SmartDownload software could not be viewed as an objective showing of their agreement.[112]

II. EXPLORING THE ELEMENTS OF EFFECTIVE LEGAL NOTICE

As discussed in Part I, principles of effective notice are critical to FTC enforcement actions,[113] state and federal statutes,[114] and enforceable contracts.[115] Though notice is significant to many different areas of U.S. law, it is of particular importance to legal models that regulate commercial practices. This Part examines the notice requirements of arbitration contracts in Part II.A, FDA labeling rules in Part II.B, and FTC enforcement actions in Part II.C. These three models respectively show standards of notice in businesses contracts, highly regulated industries, and commercial websites. Furthermore, this Part explores how these models define effective notice, as well as the mechanisms each model has in place to ensure that consumers are fairly apprised of material terms and risks.

A. Arbitration Clauses Viewed as Contracts: Actual and Constructive Notice

As the Second Circuit demonstrated in *Specht*, a finding of effective notice and mutual assent is essential to enforcing an arbitration clause.[116] Under federal law, courts are required to

---

110. *Id.* at 23, 29. ("[A]n offeree, regardless of apparent manifestation of his consent, is not bound by inconspicuous contractual provisions of which he is unaware, contained in a document whose contractual nature is not obvious.") (quoting Windsor Mills, Inc. v. Collins & Aikman Corp., 101 Cal. Rptr. 347, 351 (Cal. Ct. App. 1972). *See also* Marin Storage & Trucking, Inc. v. Benco Contracting & Eng'g, Inc., 104 Cal. Rptr. 2d 645, 651 (Cal. Ct. App. 2001).

111. *See* Specht, 306 F.3d at 20.

112. *Id.* at 28.

113. *See, e.g.,* Upromise Complaint, *supra* note 10, at 5.

114. *See* Consumer Protection Against Computer Spyware Act, CAL. BUS. & PROF. CODE §§ 22947-22947.6 *et seq.* (West 2015); 12 C.F.R. § 573.1 (2015); 45 C.F.R. § 164.500 (2015).

115. *See* Specht, 306 F.3d at 32.

116. *See* Specht, 306 F.3d at 29.

"rigorously enforce" the terms of arbitration agreements.[117] The Federal Arbitration Act (FAA) dictates that arbitration provisions shall be "valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract."[118] This law dictates that courts are to interpret arbitration provisions according to general principles of contract doctrine.[119] If the parties mutually agreed to an arbitration clause in a contract, courts are obliged to compel arbitration when future disputes fall within the scope of that provision.[120]

Parties that arbitrate will often not be afforded procedural protections from formal discovery, the Federal Rules of Civil

---

117. Am. Express Co. v. Italian Colors Rest., 133 S. Ct. 2304, 2309 (2013) ("Th[e] text [of the Federal Arbitration Act] reflects the overarching principle that arbitration is a matter of contract. And consistent with that text, courts must 'rigorously enforce' arbitration agreements according to their terms.") (quoting Dean Witter Reynolds Inc. v. Byrd, 470 U.S. 213, 221 (1985).

118. 9 U.S.C. § 2 (2012). The FAA evinces Congress's greater aim to create a "national policy favoring arbitration." Southland Corp. v Keating, 465 U.S. 1, 10 (1984). Granting arbitration provisions the status of binding contracts meant that courts were required to enforce them upon a showing of parties' valid agreement. *See* Gilmer v. Interstate/Johnson Lane Corp., 500 U.S. 20, 33 (1991). The FAA's legislative history suggests that Congress enacted it in response to lasting judicial hostility towards arbitration. Prior to the FAA, there was a long tradition of courts refusing to enforce these provisions because it ousted them of jurisdiction. Preceding the Act's enactment, the chairman of the House Judiciary Committee commented on a lasting history, stemming from English Courts, of judicial hostility and suspicion towards arbitration. *See* Dean Witter Reynolds Inc. V. Byrd, 470 U.S. 213, 220 n.6 (1985) (citing H.R. Rep. No. 96, 68th Cong., 1st Sess., 1-2 (1924)).

119. *See* Italian Colors Rest., 133 S. Ct. at 2309. Arbitration clauses are often found in the boilerplate language of standard form contracts. For example, Judicial Arbitration and Mediation Services (JAMS), an organization that provides arbitration and mediation services for different legal disputes, suggests this standard language for an arbitration clause in domestic commercial contracts:

"Any dispute, claim or controversy arising out of or relating to this Agreement or the breach, termination, enforcement, interpretation or validity thereof, including the determination of the scope or applicability of this agreement to arbitrate, shall be determined by arbitration in [insert the desired place of arbitration] before [one/three] arbitrator(s) . . . Judgment on the Award may be entered in any court having jurisdiction. This clause shall not preclude parties from seeking provisional remedies in aid of arbitration from a court of appropriate jurisdiction."

JAMS Clause Workbook: ***A Guide to Drafting Dispute Resolution Clauses for Commercial Contracts***, JUD. ARB. & MEDIATION SERVICES **(Apr. 1, 2015), http://www.jamsadr.com/clauses/ [https://perma.cc/2T7U-LZLL].**

120. Southland Corp., 465 U.S. at 10 ("In enacting § 2 of the [F]ederal [Arbitration] Act, Congress declared a national policy favoring arbitration and withdrew the power of the states to require a judicial forum for the resolution of claims which the contracting parties agreed to resolve by arbitration.").

Procedure, or a jury.[121] This is so because certain "fundamental" rights, such as the right to a jury trial, are considered alienable.[122] Parties are free to exchange negotiate these rights away by private agreement.[123] Standardized arbitration clauses in form contracts provide a mechanism through which parties trade their right to a jury for consideration.[124] In the employment arbitration agreements, for example, courts have identified employers' promises to hire new employees as consideration to support an arbitration provision in an employee contract.[125]

Without evidence of parties' prior agreement, courts will refuse to enforce arbitration clauses.[126] This is because one party may not coerce another into arbitration.[127] Rather, parties must mutually assent to arbitrate and forgo their use of the judicial forum.[128] Application of common law contract principles reveals that notice is a critical aspect of this mutual assent.[129] Formation of a valid contract requires offer and acceptance.[130] Acceptance is inferred from context if an offeree receives notice of the offer and agrees or manifests

---

121. *See* Teresa Snider, *The Discovery Powers of Arbitrators and Federal Courts Under the Federal Arbitration Act*, 34 TORT & INS. L.J. 101, 109 (1998) ("In addition to refusing to maintain jurisdiction over an arbitrable action for purposes of discovery, courts have also refused to apply the discovery procedures in the Federal Rules of Civil Procedure to arbitrations where the parties have not contractually provided for those provisions to apply."). *See also* Stephen J. Ware, *Arbitration Clauses, Jury-Waiver Clauses, and Other Contractual Waivers of Constitutional Rights*, 67 L. & CONTEMP. PROBS. 167, 169 (2004).

122. Ware, *supra* note 121, at 169.

123. *See* Ware, *supra* note 121, at 169 ("One way to alienate the jury-trial right is to consent to a contract containing an arbitration clause . . . .).

124. *See* Martindale v. Sandvik, 173 N.J. 76, 89 (2002).

125. *See, e.g.,* Koveleskie v. SBC Capital Mkts., Inc., 167 F.3d 361, 368 (7th Cir. 1999). Courts have also held that the continued employment of at-will employees also constitutes sufficient consideration for an agreement to arbitrate. *See* Durkin v. CIGNA Prop. & Cas. Corp., 942 F. Supp. 481, 488 (D. Kan. 1996).

126. *See* Granite Rock Co. v. Int'l Bhd. of Teamsters, 561 U.S. 287, 297 (2010) ("A court may order arbitration of a particular dispute only where the court is satisfied that the parties agreed to arbitrate *that dispute*.") (emphasis in original). *See also* Gateway Coal Co. v. United Mine Workers of Am., 414 U.S. 368, 374 (1974).

127. *See* Volt Info. Scis., Inc. v. Bd. of Trs. of Leland Stanford Junior Univ., 489 U.S. 468, 479 (1989)
("Arbitration under the [Federal Arbitration] Act is a matter of consent, not coercion . . . .").

128. *See* Granite Rock, 561 U.S. at 297.

129. *See* RESTATEMENT (SECOND) OF CONTRACTS: CONDUCT AS MANIFESTATION OF ASSENT § 19(2) (1981).

130. Fiederlein v. Boutselis, 952 N.E.2d 847, 856 (Ind. Ct. App. 2011) ("The basic requirements for a contract include offer, acceptance, consideration, and a meeting of the minds of the contracting parties.").

agreement to the offer.[131] Common law concepts of offer and acceptance thereby inherently implicate notice, for without notice of an offer, a party cannot meaningfully assent to its terms.[132]

Though notice of an offer is necessary for assent, courts do not require that parties receive *actual* notice of an arbitration clause.[133] When a party receives "actual notice," that notice is directly or personally conveyed to them.[134] In *Doctor's Associates, Inc. v. Casarotto*, the Supreme Court struck down a Montana statute that was enacted to facilitate contacting parties' actual notice of arbitration clauses.[135] The Montana law required that on the first page of contracts subject to arbitration there be a notice statement that the contract was subject to arbitration, and that the statement be in capital and underlined letters.[136] Arbitration clauses could be considered invalid under this state law if they did not meet the notice requirements.[137] A Montana lower court upheld the special notice requirement, interpreting the law to require that "before arbitration agreements [be considered] enforceable, they be entered knowingly."[138]

Ultimately, the Supreme Court held that the FAA preempted the Montana statute due to its special notice requirements.[139] The Court held that states could not enact laws that singled out arbitration agreements by outlining unique grounds for invalidating them.[140] The FAA instructed, as the court held, that arbitration agreements must have contract status, and they therefore could be vacated solely on contract grounds such as fraud or duress.[141] The Court reasoned that creating new ways to vacate arbitration undermined Congress' intent

---

131. *See* RESTATEMENT (SECOND) OF CONTRACTS: CONDUCT AS MANIFESTATION OF ASSENT § 19(2)

132. *See* Richard A. Bales, *Contract Formation Issues in Employment Arbitration*, 44 BRANDEIS L.J. 415, 435 (2006).

133. *See id.* at 436; *see generally* Doctor's Assocs., Inc. v. Casarotto, 517 U.S. 681 (1996) (invalidating a Montana law which required notice of arbitration to be printed in "underlined capital letters on the first page of [a] contract").

134. Black's Law Dictionary defines "actual notice" as "[n]otice given directly to, or received personally by, a party." *Notice*, BLACK'S LAW DICTIONARY (10th ed. 2014).

135. *See* Doctor's Associates, 517 U.S. at 685.

136. *See id.* at 684.

137. *Id.*

138. *Id.* at 685.

139. *Id.* at 688.

140. *Id.* at 687 ("Courts may not, however, invalidate arbitration agreements under state laws applicable *only* to arbitration provisions.") (emphasis in original).

141. *Id.*

to put arbitration agreements upon the "same footing as other contracts."[142]

Because courts put arbitration agreements "on equal footing" with contracts, parties need not receive actual notice to be bound by their terms.[143] As in common law contracts, parties' constructive notice will often suffice to render arbitration agreements enforceable.[144] A party receives "constructive notice" of an agreement when, given the specific facts or circumstance, a party had reason to know that certain terms existed and had the duty to apprise themselves of those terms.[145] The requisites of constructive notice are outlined in *F.D. Import & Export Corporation v. M/V REEFER SUN*.[146] In that case, the court determined that F.D. Import, a large commercial buyer of international fruit, was compelled to arbitrate with various suppliers and carriers.[147] Though F.D. Import had no actual notice of the clause, the court held that it had received constructive notice, which was enough to compel arbitration.[148] The court found that F.D. Import had constructive notice of the arbitration clause, despite the

---

142. *Id.* (quoting Scherk v. Alberto-Culver Co., 417 U.S. 506, 511 (1974)). *But see* Keystone, Inc. v. Triad Sys. Corp., 1998 MT 326, ¶ 23 (1998) (holding that "[t]he FAA generally preempts state law which restricts the application of arbitration agreements. However, when a state law does not conflict with the FAA so as to frustrate the objectives of Congress, it is not necessarily preempted. State law may be applied in spite of the FAA's preemptive effect "*if* that law arose to govern issues concerning the validity, revocability, and enforceability of contracts generally") (quoting Perry v. Thomas, 482 U.S. 483, 492-93, n.9 (1987)). *See also* Wells v. Tenn. Homesafe Inspections, LLC, No. M200800224-COA-R3-CV, 2008 WL 5234724, at *3 (Tenn. Ct. App. 2008) (holding that an arbitration clause was unenforceable because it was not separately signed or initialed by both parties, as required by state law).

143. *See* AT&T Mobility LLC v. Concepcion, 563 U.S. 333, 339 (2011); Buckeye Check Cashing, Inc. v. Cardegna, 546 U.S. 440, 443 (2006); Doctor's Assocs., Inc. v. Casarotto, 517 U.S. 681, 686 (1996). *See also* Bales, *supra* note 132, at 424.

144. *See* Steel Warehouse Co. v. Abalone Shipping Ltd. of Nicosai, 141 F.3d 234, 237 (5th Cir. 1998) (holding that parties were bound by an arbitration clause because they had constructive notice that it was incorporated into their agreement); F.D. Imp. & Exp. Corp. v. M/V REEFER SUN, 248 F. Supp. 2d 240, 247 (S.D.N.Y. 2002) ("A party does not need actual notice to be bound by an arbitration agreement. Constructive notice is sufficient to create a binding arbitration agreement.").

145. Black's Law Dictionary defines "constructive notice" as "[n]otice arising by presumption of law from the existence of facts and circumstances that a party had a duty to take notice of, such as a registered deed or a pending lawsuit; notice presumed by law to have been acquired by a person and thus imputed to that person." *Notice*, Black's Law Dictionary (10th ed. 2014). *See also* Steel Warehouse, 141 F.3d at 237. ("Constructive notice can be defined, crudely, as a rule in which 'if you should have known something, you'll be held responsible for what you should have known.'").

146. 248 F. Supp. 2d at 247.

147. *Id.* at 251.

148. *Id.* at 248.

fact that F.D. Import was never a signatory of the contract in which the arbitration clause appeared.[149] Though only the ship owner and charterer signed the agreement, it was later incorporated into subsequent bills of lading.[150] The reverse side of the bills of lading stated that it incorporated all terms of the previous contract, including the arbitration clause.[151] The court held that the bill of lading was sufficient to place F.D. Import on constructive notice and to compel arbitration.[152]

1. Contract Remedies for Insufficient Notice of Arbitration Clauses

Though parties are not entitled to actual notice of arbitration, common law contract remedies may provide redress when notice of an arbitration clause is insufficient.[153] Courts should not presume that parties agreed to arbitrate a dispute "unless there is 'clea[r] and unmistakabl[e]' evidence that they did so."[154] A court's determination of whether a dispute should be moved to arbitration depends on whether the parties actually agreed to arbitrate and whether the dispute falls within the scope of that agreement.[155] Nevertheless, parties may prevail in vacating an arbitration clause through a showing of insufficient notice.[156] Parties may argue that without being offered fair notice of an arbitration clause, they could not manifest requisite consent to this contract term.[157]

---

149. *Id.* at 247-48.

150. *Id.* A "bill of lading" is defined as a "document acknowledging the receipt of goods by a carrier or by the shipper's agent and the contract for the transportation of those goods; a document that indicates the receipt of goods for shipment and that is issued by a person engaged in the business of transporting or forwarding goods." *Bill of Lading*, Black's Law Dictionary (10th ed. 2014).

151. F.D. Imp. & Exp. Corp., 248 F. Supp. 2d at 248.

152. *Id.*

153. *See* First Options of Chi., Inc. v. Kaplan, 514 U.S. 938, 943 (1995) (holding that when an arbitration clause is valid, an arbitrator, rather than a court, has the deciding power over parties' disputes). *But see* Mobil Oil Corp. v. Local 8-766, Oil, Chem. & Atomic Workers Int'l Union, 600 F.2d 322, 324-25 (1st Cir. 1979) (providing that a court must hear questions of arbitrability, or the threshold issue of whether or not an arbitration clause is enforceable).

154. *See* First Options, 514 U.S. at 944 (citing AT&T Tech., Inc. v. Comm'ns. Workers of Am., 475 U.S. 643, 649 (1986)) (alteration in original).

155. *See* First Options of Chi., Inc., 514 U.S. at 944-45.

156. *See* Campbell v. General Dynamics Gov't Sys. Corp., 321 F. Supp. 2d 142, 147 n.3 (D. Mass. 2004) ("[A]n employee's knowledge of the [employer's] offer is obviously a necessity for the inference of acceptance to hold."); *see* Bales, *supra* note 132, at 436-37.

157. *See* Campbell v. General Dynamics Gov't Sys. Corp., 407 F.3d 546, 555 (1st Cir. 2005).

Contract defenses of unconscionability encompass underlying claims of insufficient notice and defective consent.[158] In contract law, the doctrine of unconscionability consists of two branches: procedural unconscionability and substantive unconscionability.[159] Though both procedural and substantive unconscionability must be present to invalidate an agreement, and the more one is shown, the less the other is needed.[160] Contracts that are substantively unconscionable tend to have unduly harsh or unreasonable terms.[161] Agreements that are procedurally unconscionable, on the other hand, tend to be formed under unjust conditions, such as when one party has disproportionate bargaining power or fails to apprise an offeree of the contract's terms.[162] A showing of lack of notice and "surprise" is sometimes inherent to a procedural unconscionability analysis.[163] "Surprise" may occur when "supposedly agreed-upon terms of the bargain are hidden in a prolix printed form drafted by the party seeking to enforce the disputed terms."[164]

A court may refuse to enforce a "surprise" arbitration clause if it was either buried in an agreement, or not sufficiently called to a party's attention during the formation of a contract.[165] For example, in *Zaborowski v. MHN Gov't Servs., Inc.*, the court held that an arbitration clause was one of surprise because it was inconspicuously included in the twentieth paragraph of the twenty-three paragraph long agreement.[166] The court noted that there was no separate signature in the contract for the arbitration clause, and the signature line was on an entirely separate page.[167] Moreover, the arbitration

---

158. *See* Zaborowski v. MHN Gov't Servs., Inc., 936 F. Supp. 2d 1145 (N.D. Cal. 2013).

159. *See* Discover Bank v. Superior Court of L.A., 36 Cal. 4th 148, 160 (2005); *Unconscionability*, Black's Law Dictionary (10th ed. 2014).

160. *See* Gatton v. T-Mobile USA, Inc., 152 Cal. App. 4th 571, 579 (2007).

161. *Unconscionability*, Black's Law Dictionary (10th ed. 2014).

162. *Id.*

163. *See* Ingle v. Circuit City Stores, Inc., 328 F.3d 1165, 1171 (9th Cir. 2003) ("To determine whether the arbitration agreement is procedurally unconscionable the court must examine 'the manner in which the contract was negotiated and the circumstances of the parties at that time.' An inquiry into whether [an] arbitration agreement involves oppression or surprise is central to that analysis.") (quoting Kinney v. United Healthcare Servs., Inc., 70 Cal. App. 4th 1322, 1329 (1999)).

164. A & M Produce Co. v. FMC Corp., 135 Cal. App. 3d 473, 486 (Ct. App. 1982).

165. *See* Lau v. Mercedes-Benz USA, LLC, No. CV 11-1940 MEJ, 2012 WL 370557, at *8 (N.D. Cal. Jan. 31, 2012) (finding surprise because an arbitration clause was not separated from the rest of the page and was not on the page that required agreeing parties' signatures).

166. 936 F. Supp. 2d 1145, 1152 (N.D. Cal. 2013).

167. *Id.*

clause was neither highlighted nor outlined on the page in order to stand out to the reader.[168] Thus, the court held that the arbitration agreement was unenforceable on the grounds of unfair surprise.[169]

Arbitration clauses may also be unconscionable when a drafting party reserves the right to change the terms of arbitration without notice.[170] In *Hooters of America, Inc. v. Phillips*, the Fourth Circuit held that an arbitration clause in an employment contract was unconscionable because it reserved the right of employer, Hooters of America Inc. ("Hooters"), to unilaterally modify the arbitration terms in the post-agreement stage.[171] According to its contract terms, Hooters could modify the rules of employee arbitration "in whole or in part," whenever it wished, "without notice" to the employee.[172] Further, Hooters reserved the right to expand the scope of an employee arbitration to cover matters not already listed in the initial arbitration agreement, whether or not it related to an employee's initial claim.[173] Because Hooters maintained the right to change the terms of arbitration agreements as it wished, the court held that the arbitration agreement was one-sided and unenforceable.[174] The ability to modify arbitration terms in the post-agreement stage, without apprising employees with notice, impermissibly allowed Hooters to dominate arbitration outcomes.[175]

---

168. *Id.* Note that the district court's holding in *Zaborowski* rests alongside the Supreme Court's ruling in Doctor's Assocs., Inc. v. Casarotto, 517 U.S. 681 (1996), because in *Doctor's Associates*, the Supreme Court struck down a state law that specifically demanded special notice requirements for arbitration clauses. The FAA made no such demands, and federal law therefore preempted the state law. In *Zaborowski*, however, the district court found that an agreement was procedurally unconscionable under common law contract grounds, as its terms were visibly inconspicuous to the agreeing party.

169. *See* Zaborowski, 936 F. Supp. 2d at 1152.

170. *See* Hooters of Am., Inc. v. Phillips, 173 F.3d 933, 939, 941 (4th Cir. 1999). A contract has also been found to be invalid due to lack of acceptance when one party unilaterally modifies a contract. *See* Douglas v. U.S. Dist. Court for Cent. Dist. of Cal., 495 F.3d 1062, 1066 (9th Cir. 2007) ("Indeed, a party can't unilaterally change the terms of a contract; it must obtain the other party's consent before doing so. This is because a revised contract is merely an offer and does not bind the parties until it is accepted.").

171. 173 F.3d at 939, 941.

172. *Id.* at 939.

173. *Id.*

174. *Id.* at 941.

175. *Id.* ("By promulgating this system of warped rules, Hooters so skewed the process in its favor that [plaintiff] has been denied arbitration in any meaningful sense of the word. To uphold the promulgation of this aberrational scheme under the heading of arbitration would undermine, not advance, the federal policy favoring alternative dispute resolution. This we refuse to do.").

2. Arbitration Clauses Viewed as Waivers: The "Voluntary and Knowing" Standard

Some federal courts equate arbitration provisions with waivers of legal rights.[176] When parties agree to arbitrate, these courts argue, they waive certain legal rights by default.[177] The agreeing parties lose access to the traditional judicial forum for their dispute.[178] Instead of a judge and jury, one or more arbitrators determine the outcome of a case.[179] Arbitrators are not bound by the same rules and procedures as judges, and they do not have to comply with the Rules of Civil Procedure or Rules of Evidence during the arbitration.[180] Moreover, fact-finding in arbitration proceedings is less thorough and more limited than that in the judicial setting.[181] Fact-finding in arbitration need not include sworn testimony, cross-examination, or discovery.[182]

In addition to waiving the right to a jury trial, parties to an arbitration agreement relinquish other procedural and substantive protections. For example, in *Mitsubishi Motors Corp. v. Soler Chrysler-Plymouth, Inc.*, the Supreme Court determined that arbitration procedures are capable of vindicating parties' federal statutory rights.[183] It held that parties are free to stipulate that an arbitrator will have deciding power over federal statutory claims, and

---

176. *See* Bales, *supra* note 132, at 449; Christine M. Reilly, Comment, *Achieving Knowing and Voluntary Consent in Pre-Dispute Mandatory Arbitration Agreements at the Contracting Stage of Employment*, 90 CAL. L. REV. 1203, 1210 (2002).

177. Among these rights is the Seventh Amendment right to a jury trial. U.S. CONST. amend VII. *See* RDO Fin. Servs. Co. v. Powell, 191 F. Supp. 2d 811, 813 (N.D. Tex. 2002). The right to a jury trial also depends on the type of legal proceeding involved. In administrative hearings, for example, there is no right to a jury trial. *See* Ware, *supra* note 121, at 169.

178. *See* Reilly, *supra* note 176, at 1211.

179. *See* Reilly, *supra* note 176, at 1210.

180. *See* Reilly, *supra* note 176, at 1210.

181. *See* Alexander v. Gardner-Denver Co., 415 U.S. 36, 57-58 (1974) ("[T]he factfinding process in arbitration usually is not equivalent to judicial factfinding. The record of the arbitration proceedings is not as complete; the usual rules of evidence do not apply; and rights and procedures common to civil trials, such as discovery, compulsory process, cross-examination, and testimony under oath, are often severely limited or unavailable.").

182. *Id.* at 57-58.

183. Mitsubishi Motors Corp. v. Soler Chrysler-Plymouth, Inc., 473 U.S. 614, 638, (1985). Since *Mitsubishi,*

the Supreme Court has held that claims arising under federal statutes such as anti-trust laws, securities law, and the Age Discrimination in Employment Act (ADEA) are appropriate for arbitration. *See generally* Richard E. Speidel, *Consumer Arbitration of Statutory Claims: Has Pre-Dispute (Mandatory) Arbitration Outlived Its Welcome?*, 40 ARIZ. L. REV. 1069 (1998).

are free to stipulate if that arbitrator should apply federal law.[184] The Court noted that parties have the freedom to determine the scope and procedure of their own arbitration agreements.[185] It concluded that "so long as the prospective litigant effectively may vindicate its statutory cause of action in the arbitral forum," a federal statute may "continue to serve both its remedial and deterrent function."[186]

The Supreme Court held that arbitration provisions do not prevent individuals from asserting statutory rights.[187] Nonetheless, some circuit courts require proof of parties' "knowing" waiver of their legal rights before enforcing arbitration agreements.[188] The Ninth[189] and Sixth Circuits,[190] for instance, have expressly adopted the "knowing" agreement waiver standard, while courts in the Seventh Circuit have endorsed it.[191] Courts in these Circuits require proof of parties' informed consent to waiving constitutional or statutory rights prior to compelling arbitration.[192] Under this standard, parties cannot agree to arbitrate and lose access to a judicial forum without receiving explicit notice of the constitutional or statutory rights that they may be signing away.[193]

---

184. Mitsubishi Motors, 473 U.S. at 628 ("Nothing . . . prevents a party from excluding statutory claims from the scope of an agreement to arbitrate.").

185. *Id.* at 628.

186. *Id. See also* Gilmer v. Interstate/Johnson Lane Corp., 500 U.S. 20, 26-28 (1991) (holding that an employee's Age Discrimination in Employment Act (ADEA) are appropriate for arbitration because Congress did not intend to exclude arbitration as a form of dispute resolution under the statute).

187. Mitsubishi Motors, 473 U.S. at 628.

188. *See* Walker v. Ryan's Family Steak Houses, Inc., 400 F.3d 370, 381 (6th Cir. 2005); Prudential Ins. Co. of Am. v. Lai, 42 F.3d 1299, 1305 (9th Cir. 2005). In the context of criminal law, defendants must "knowingly and intelligently" relinquish their Fifth Amendment due process rights in order for waiver to be valid. *See* Miranda v. Arizona, 384 U.S. 436, 444 (1966).

189. *See* Lindgren v. Pub. Storage, 290 Fed. Appx. 971, 972 (9th Cir. 2008) (citing Nelson v. Cyprus Bagdad Copper Corp., 119 F.3d 756, 761 (9th Cir. 1997)).

190. The Sixth Circuit has articulated a test for assessing the validity of parties' waivers. The court evaluates whether parties knowingly and voluntarily waived their rights according to "(1) plaintiff's experience, background, and education; (2) the amount of time the plaintiff had to consider whether to sign the waiver, including whether the employee had an opportunity to consult with a lawyer; (3) the clarity of the waiver; (4) consideration for the waiver; as well as (5) the totality of the circumstances." *See* Morrison v. Circuit City Stores, Inc., 317 F.3d 646, 668 (2003) (quoting Adams v. Philip Morris, Inc., 67 F.3d 580, 583)6th Cir. 1995)).

191. *See* Gibson v. Neighborhood Health Clinics, Inc., 121 F.3d 1126, 1130 (7th Cir. 1997); *see also* Bales, *supra* note 132, at 449-50.

192. *See* Walker., 400 F.3d at 380.

193. *See* Tanya J. Axenson, *Mandatory Arbitration Clauses and Statutory Rights: The Legal Landscape After Nelson v. Cyprus Bagdad Copper Corporation, 119 F.3d 756 (1997)*, 3 HARV. NEGOT. L. REV. 271, 281-82 (1998).

The Ninth Circuit described the core requirements of the "knowing" agreement standard in *Nelson v. Cyprus Bagdad Copper Corp.*[194] In *Nelson*, the court applied the "knowing" agreement standard and held that an employee could not be compelled to arbitrate his Americans with Disabilities Act (ADA) claim.[195] The appellant's employer in *Nelson* gave him an employee handbook that contained an arbitration provision.[196] After receiving the handbook, the appellant returned a form to his employer that stated that he agreed to "read and understand" the handbook.[197] A year after the appellant received the employee handbook, he was terminated from his position, and filed a claim alleging discrimination under the ADA against his former employer in federal court.[198] The district court granted summary judgment for the defendant employer, upholding the arbitration agreement in the Employee Handbook.[199]

The Ninth Circuit determined that the arbitration clause was not enforceable because the appellant did not knowingly agree to waive his statutory rights.[200] Examining the history and language of the ADA, the court determined that Congress intended that employees knowingly consent prior to waiving their ADA rights, protections, and remedies.[201] Furthermore, the court held that though the appellant agreed to "read and understand" the handbook, he did not agree to be bound by its terms.[202] Neither the appellant's employer nor the handbook informed the appellant that his agreement to "read and understand" his employer's terms would translate to a waiver of his statutory civil rights.[203]

Finally, the *Nelson* court held that continued employment was not enough to put the appellant on notice that he had waived his statutory rights.[204] Rather, the Ninth Circuit concluded that when employees

---

194. 119 F.3d 756, 761 (9th Cir. 1997).

195. *Id.* 762.

196. *Id.* at 758.

197. *Id.* at 761.

198. *Id.* at 759.

199. *Id.*

200. *Id.* at 762. The *Nelson* court aligned with a prior Ninth Circuit's holding in *Prudential Ins. Co. of Am. v. Lai*, 42 F.3d 1299, 1303 (9th Cir. 1994), which held that employees did not consent to arbitrate their Title VII sexual harassment claims because they did not do so "knowingly." The *Lai* court determined that the plaintiffs' employee registration forms failed to notify them that future sexual discrimination claims in particular would be subject to arbitration. *Id.*

201. Nelson, 119 F.3d at 761 n.9.

202. *Id.* at 761.

203. *Id.*

204. *Id.* at 762.

bargain to waive their rights to a judicial forum, they must waive those rights in an express and explicit manner.[205] The "unilateral promulgation by an employer of arbitration provisions" in the employee handbook failed to meet the standard of a "knowing" waiver of ADA protections.[206] The court determined that to arbitrate statutory claims, employers must inform employees of the existence of arbitration clauses and specifically refer to the rights that employees will waive if they agree to them.[207] Otherwise, arbitration agreements would be unenforceable, as employees would unknowingly surrender their guaranteed statutory privileges and remedies.[208]

B. FDA Labeling Rules

Notice is critical in the domain of arbitration clauses and commercial contracts. Proof that parties were on actual or constructive notice of an arbitration agreement may evince their consent to arbitrate future disputes and waive their access to a judicial forum. Similarly, notice is critical to ensuring consumer safety in highly regulated industries.[209] The FDA regulates how OTC drug manufacturers convey notice to consumers.[210] Through its OTC drug-labeling rule, the FDA uses product packaging as a mechanism for effective notice.[211] The FDA regulates the content and format of OTC drug labels with standardized requirements so that labels are readable and rapidly inform consumers of pertinent drug information.[212] This Note ultimately argues that if some features of OTC drug labels were to be extrapolated and applied to online privacy policies, then online privacy polices might become more legible and digestible to the average consumer.

---

205. *Id.* at 762 ("Any bargain to waive the right to a judicial forum for civil rights claims, including those covered by the ADA, in exchange for employment or continued employment must at the least be express: the choice must be explicitly presented to the employee and the employee must explicitly agree to waive the specific right in question. That did not occur in the case before us.").

206. *Id.*

207. *Id.* at 762.

208. *See* Axenson, *supra* note 193, at 282.

209. *See* Lars Noah, *The Imperative to Warn: Disentangling the "Right to Know" from the "Need to Know' About Consumer Product Hazards*, 11 YALE J. ON REG. 293, 321 (1994) (discussing required warnings on FDA regulated drug products).

210. *See* 21 C.F.R. § 201.66 (2014).

211. *See* Noah, *supra* note 209, at 320-21.

212. *See* 21 C.F.R. § 201.66

1. Standardized Content in FDA Labeling Rules

Though different courts have unique standards of notice, the FDA's notice requirements for OTC drug labels are highly uniform and regulated.[213] In 1999, the FDA published a final regulation that established standardized labeling requirements for OTC drugs.[214] The regulation detailed both the content and format of OTC drug labels, and set forth a general product-labeling outline for presenting drug information to consumers.[215] Prior to the rule, the FDA found that variations between OTC drug products in areas of label content (i.e., differences in wording of drug warnings and directions for use) and label format (i.e., differences in headings and typeface) increased consumer confusion over similar OTC drugs on the market.[216] Because manufacturers presented product information differently, consumers had difficulty comparing drugs and deciding which were most appropriate for their needs.[217]

The 1999 rule aimed to improve OTC labeling by dictating requirements for drug label format.[218] The rule requires warnings to be conveyed in the form of short, directive statements.[219] For example, when an OTC drug might be dangerous to children, the FDA provides that a manufacturer display in bold type "[k]eep out of reach of children" and "'[a]sk a doctor before use if the child has' . . . all warnings for persons with certain preexisting conditions . . . and all warnings for persons experiencing certain symptoms."[220] The FDA determined that drug warnings in the form of curt and action-oriented commands would be more readable, direct, and understandable to consumers.[221] The FDA asserted that these brief directives would enhance warning clarity by conveying to consumers the precise course of action they should take for safe product use.[222] The FDA found that, unlike densely worded text, shorter sentences with simple terminology reduced consumers'

---

213. *See id.*
214. *See id.*
215. *See* 21 C.F.R. § 201.66(d).
216. *See* Over-The-Counter Human Drugs; Proposed Labeling Requirements, 62 Fed. Reg. 9024, 9027 (Feb. 27, 1997).
217. *See id.* at 9028.
218. *See id.* at 9027-28.
219. *See* 21 C.F.R. § 201.66.
220. 21 C.F.R. § 201.66(c)(5)(iv), (x).
221. *See* Over-The-Counter Human Drugs; Labeling Requirements, 64 Fed. Reg. 13254, 13254 (Mar. 17, 1999).
222. *See id.* at 13254-55.

processing time.[223] With less text on a label, consumers would not be overwhelmed with information and would be able to read and understand labels at faster rates.[224]

This rule prescribed the content of OTC drug labels and the sequence in which that content must be conveyed.[225] It required that an OTC drug label display information under the headings in the exact sequence of "active ingredients," "uses," "warnings," "directions," and "inactive ingredients."[226] The FDA determined that by requiring manufacturers to present content in this uniform order, consumers would become familiar with this routine sequence and know where to find a specific drug fact on any given OTC label.[227] By organizing drug facts in a formulaic and uniform scheme, drug labels could shape consumer expectations for what information they could find on a label and where on the label they could locate it.[228] The FDA concluded that standardizing the sequence of drug label content would enable consumers to accurately compare different brands of OTC drug products.[229] A uniform order of label content enabled consumers to perform side-by-side comparisons, identify differences between products, and readily determine which products were safest for use.[230]

2. User-friendly Formatting

Prior to the 1999 rule, the FDA discovered that some common formatting practices diminished the legibility of OTC drug labels.[231] The FDA observed that labels with compressed text and small type letters contributed to consumer comprehension problems.[232] The FDA concluded that such labels required consumers to possess a greater than normal visual acuity in order to read and understand displayed product information.[233] Additionally, the FDA determined that even if consumers could see the information on drug labels,

---

223. *Id.* at 13255.
224. *Id.*
225. *See* 21 C.F.R. § 201.66(c) (2014).
226. *Id.*
227. *See* Over-The-Counter Human Drugs; Labeling Requirements, 64 Fed. Reg. at 13255.
228. *Id.*
229. *Id.*
230. *See id.* at 13277.
231. *See* Over-The-Counter Human Drugs; Proposed Labeling Requirements, 62 Fed. Reg. 9024, 9027-28 (Feb. 27, 1997).
232. *Id.*
233. *Id.*

compressed paragraphs of text caused consumers to lose interest in the information presented.[234]

The 1999 rule required OTC drug label content to be displayed in a tabular outline.[235] Within this outline, the FDA requires drug manufacturers to describe drug information in shorter phrases under standardized, bold-type title headings.[236] As opposed to displaying paragraphs of text, the rule requires drug manufactures to "chunk" similar groups of information together on the label.[237] This "chunked" format entailed separating discrete units of related label information (i.e., drug warnings, drug directions, active ingredients) in list form.[238] The FDA determined that organizing label information in a chunked structure improved consumers' reading and processing abilities.[239] Using simpler terminology, shorter sentences, and conspicuous headings tended to reduce consumers' "cognitive load" by creating less demand on consumers' memories.[240] Finally, the FDA concluded that in comparison to paragraphs, the chunked format had greater eye appeal and was more likely to draw consumers' attention to the information presented.[241]

User-friendly titles, headings, and subheadings are a central aspect of the 1999 FDA rule.[242] These formatting elements advance the FDA's overarching aim to make information easier to locate and

---

234. *Id.* at 9028.

235. *See* Over-The-Counter Human Drugs; Labeling Requirements, 64 Fed. Reg. at 13265-66.

236. *Id.* at 13265.

237. *Id.* at 13255.

238. *Id.* at 13265-66.

239. *Id.* at 13255. *See generally* Michael S. Wogalter & Mica P. Post, *Printed Tutorial Instructions: Effects Of Text Format And Screen Pictographs On Human-Computer Task Performance*, 89 PROCEED. INTERFACE 133 (1989) (finding that when shown information in the form of paragraph and lists with screen pictographs, participants in a study made fewer errors and help requests, and completed tasks in shorter time when shown lists); Lawrence T. Frase & Bary J. Schwartz, *Typographical Cues That Facilitate Comprehension*, 71 J. EDUC. PSYCHOLOGY 197, 204-05 (1979) (finding that grouping information facilitates readers' search for information as well as their acquisition of knowledge); William J. Vigilante, Jr. & Michael S. Wogalter, *Over-The-Counter (OTC) Drug Labeling: Format Preferences*, PROCEED. HUM. FACTORS & ERGONOMICS SOC'Y 43RD ANN. MEETING 104 (1999), http://www.safetyhumanfactors.org/wp-content/uploads/2011/12/163Vigilante_Wogalter1999.pd [https://perma.cc/6YF2-CT5T] (stating that chunking information into groups can foster improved reading comprehension).

240. Over-The-Counter Human Drugs; Labeling Requirements, 64 Fed. Reg. at 13255.

241. *Id.*

242. *Id.* at 13254.

read.[243] Titles and headings provide consumers with "visual cues" that could draw their eyes to important categories of information on a drug label.[244] To enhance uniform compliance with its headings regulations, the FDA provides specific and detailed requirements in the rule.[245] For example, the rule requires that headings be displayed in bold italic type and subheadings displayed in bold type.[246]

The 1999 rule also regulates the size of typeface on OTC drug labels.[247] Prior to the rule, the FDA found that labels were cramped and difficult for many consumers to read.[248] It concluded that small type, text-heavy labels demanded a greater than normal visual acuity from consumers.[249] Moreover, the FDA found that only forty-eight percent of the population could see the typical type size of label text.[250] To improve the legibility of OTC labels, the FDA prescribes that the letter height or type size for subheadings and all other information should be no smaller than 6-point type.[251] According to the FDA, this larger type size improves much of the general population's ability to physically see the text on product labels.[252] Increased visibility also improves consumers' reading and

---

243. *See id.*

244. *Id.*

245. *See* 21 C.F.R. § 201.66(d)(5)-(6) (2014).

246. 21 C.F.R. § 201.66(d)(3).

247. *See* 21 C.F.R. §§ 201.66(d)(2), (4), (10)(ii).

248. *See* Over-The-Counter Human Drugs; Proposed Labeling Requirements, 62 Fed. Reg. 9024, 9024 (Feb. 27, 1997).

249. *See id.* at 9028. To support its proposal, the Administration cited a study that explored "the effects of type size (vertical letter height) and horizontal letter compression" on the legibility of OTC drug labels among the geriatric population and found that "a significant number of the elderly population could not adequately see the print on certain OTC product labels due in part to the small type sizes and high degree of horizontal compression. *Id.* (citing Richard K. Watanabe, *The Ability of the Geriatric Population to Read Labels on Over-the-Counter Medication Containers*, J. THE AM. OPTOMETRIC ASS'N., 65:32-37 (1994)). The Administration also cited another study, which "evaluated the visual acuity needed to read 25 marketed OTC drug product labels" and found that the majority of labels demanded a much higher than normal visual acuity. *Id.* (citing Greg A. Holt et al., *OTC Labels: Can Consumers Read and Understand Them*?, AM. PHARMACY, NS30:51-54 (1989)).

250. Over-The-Counter Human Drugs; Labeling Requirements, 64 Fed. Reg. at 13265 (explaining that prior to the rule, the National Drug Manufactures Association recommended a minimum type size of 4.5, which the FDA found that only 48% of the public could actually read). *See also* Vigilante & Wogalter, *supra* note 239, at 104 (asserting that people are less likely to expend the mental energy on reading information on densely printed labels).

251. 21 C.F.R. § 201.66(d)(2).

252. Over-The-Counter Human Drugs; Labeling Requirements, 64 Fed. Reg. at 13264.

comprehension of product labels.[253] The FDA determined that when consumers are more confident about their ability to read a product label, they are more capable of processing and understanding that label's information.[254]

3. Symbolic Visual Cues

The FDA endorses the use of symbolic cues on OTC labels as a means of conveying information.[255] For example, the FDA affirms that bullet points could be used to introduce "chunks" of information without distracting or confusing consumers.[256] By separating drug facts into discrete chunks, bullets on OTC drug labels convey key information without overwhelming consumers.[257] An FDA guidance document explains how bullets may be used on drug labels.[258] The guidance document states that drug labels should list separate statements under bullets, rather than consolidating the statements into longer paragraphs.[259] For example, instead of presenting user directions in a large block of text, the guidance document states that phrases such as "shake well" and "children under 2 years: ask a doctor" may be positioned under bullets in an easier to read format.[260]

The FDA permits, but does not require, OTC drug manufacturers to communicate drug information through pictograms.[261] The FDA defines a "pictogram" as "a pictorial representation of some object used to symbolize information."[262] The FDA also provides for the use of pictograms outside of the OTC drug context.[263] For instance, the Administration requires that powdered infant formula manufacturers display pictures to represent the three-step process involved in safely preparing and using the product.[264] It determined that pictures, rather than words, would enhance the clarity of the preparation

253. *See id.* at 13254.

254. *See id.* at 13257.

255. *See* 21 C.F.R. § 201.66(d)(4).

256. Over-The-Counter Human Drugs; Labeling Requirements, 64 Fed. Reg. at 13266. The FDA defines "bullet" as a "geometric symbol," either a solid square or circle, "that precedes each statement in a list of statements." 21 C.F.R. § 201.66(d)(4).

257. *See* Over-The-Counter Human Drugs; Labeling Requirements, 64 Fed. Reg. at 13266.

258. *See Guidance For Industry Labeling OTC Human Drug Products (Small Entity Compliance Guide)*, FOOD & DRUG ADMIN. 2009 WL 1887337 (May 2009).

259. *Id.* at *5.

260. *Id.* at *9.

261. *Id.* at *11.

262. *Id.*

263. *See* 21 C.F.R. § 107.20 (2014).

264. *Id.*

instructions.[265] The FDA further recognized that many caregivers and health professionals might not be able to speak or read English.[266] Showing the product directions via images would reach a wider audience and help ensure that consumers could properly dilute the formula regardless of reading level.[267]

C. FTC Enforcement Actions

Like the FDA, the FTC exercises its administrative authority to regulate notice in the commercial domain.[268] FTC enforcement actions have shaped the contours of U.S. privacy law, and inform legal standards of notice in the present digital age.[269] While identifying the different categories of FTC Section 5 privacy actions, this Note relies on the typology of underlying privacy harms developed by the Fordham Law Center for Law and Information Policy (CLIP).[270] CLIP has categorized FTC actions according to the most frequently asserted privacy harms in FTC complaints[271] and classified FTC actions as relating to four distinct privacy harms: (1) unauthorized disclosure of personal information, discussed in Part II.C.1;[272] (2) surreptitious collection of personal information, discussed in Part II.C.2;[273] (3) failure to secure personal information, discussed in Part II.C.3;[274] and (4) unlawful retention of personal information, discussed in Part II.C.4.[275]

---

265. *See Infant Formula; Labeling Requirements*, 48 Fed. Reg. 31880-01, 31883 (July 12, 1983).

266. *See id.*

267. *See id.*

268. *See* Solove & Hartzog, *supra* note 17, at 585-86 (asserting that FTC privacy actions provide a basis for modern U.S. privacy jurisprudence).

269. *See* Solove & Hartzog, *supra* note 17, at 606 ("The FTC has essentially been inching itself into the role of a de facto federal data protection authority).

270. *See* Reidenberg, et al., *supra* note 47, at 20.

271. *See* Reidenberg, et al., *supra* note 47, at 20. Due to the fact that the FTC can only act pursuant to its statutory authority, enforcement actions must "fit" within the scope of Section 5's statutory language of an "unfair" or "deceptive" practice. In its study, CLIP looked beyond FTC's characterizations of certain practices as "unfair" or "deceptive" and studied the underlying privacy harms asserted in the Commission's complaints. CLIP explained that "[t]his approach looked to the true substance of the wrongful event rather than the way a claim was formulated to fit within the existing constraints of the legal landscape." Reidenberg, et al., *supra* note 47, at 20.

272. *See* Reidenberg, et al., *supra* note 47, at 21.

273. *See* Reidenberg, et al., *supra* note 47, at 22.

274. *See* Reidenberg, et al., *supra* note 47, at 23.

275. *See* Reidenberg, et al., *supra* note 47, at 24.

1. Unauthorized Disclosure of Personal Information

Under the "unauthorized disclosure" class of FTC actions, websites disclose users' personal information to third parties without first notifying users or obtaining their consent.[276] An unauthorized disclosure occurs either when a consumer is not notified that his or her data is shared with a third party, or when a consumer is misled about how or for what purposes his or her data is collected.[277] The FTC Complaint for *In re GeoCities*, demonstrates the privacy harms that may result from unauthorized disclosures.[278] In this action, the FTC determined that GeoCities committed a "deceptive practice" because it misrepresented its data collection and sharing practices to consumers.[279]

GeoCities hosted different web pages that provided its members with personal home pages, email addresses, and online children's clubs.[280] The GeoCities membership form collected "mandatory" information, including first and last name, zip code, e-mail address, gender, date of birth, and "optional" information, such as education level, income, marital status, occupation, and interests.[281] Geocities users could also opt to receive "special offers" from other companies.[282] Though the Geocities privacy statement claimed, "[w]e assure you . . . we will NEVER give your personal information to anyone without your permission," the company actually disclosed, rented, and sold users' personally identifiable information to third party advertisers for the purposes of targeted advertising.[283] The shared information also included data that GeoCities collected from children.[284] The FTC determined that by failing to notify members regarding how it collected and shared personal data with advertisers, GeoCities committed a Section 5 deceptive practice.[285] Beyond its failure to disclose the nature of its data collection and sharing, GeoCites actively misled consumers with its privacy statements,

---

276. *See e.g.*, Frostwire Complaint, *supra* note 65; HTC America Complaint, *supra* note 65; Red Zone Complaint, *supra* note 65.

277. *See* Reidenberg et al., *supra* note 47, at 21-22.

278. *See generally* Complaint, *In re* GeoCities, FTC File No. 9823015, No. C-3850 (F.T.C. Feb. 5, 1999).

279. *Id.* at 2-5.

280. *Id.* at 1.

281. *Id.* at 2.

282. *Id.*

283. *Id.* at 3.

284. *Id.*

285. *Id.* at 4-5.

which stated that personal data would not be transmitted to third parties without users' consent. [286]

The FTC has also filed complaints against companies that failed to apprise consumers of how personal data was appropriated.[287] In *In re Facebook, Inc.*, the FTC filed a complaint against Facebook for failing to disclose how it used its members' personal profile information.[288] According to the FTC complaint, Facebook claimed that it never shared users' personal data with advertisers without their consent,[289] but stated that it only shared "aggregate and anonymous data" with advertisers so that Facebook's advertisers could generate more effective advertisements.[290]

The FTC also found that Facebook failed to notify consumers of material privacy policy changes that increased the visibility of users' personal information to third parties.[291] Under its new privacy policy, Facebook retroactively applied changes to members' accounts without their consent and disclosed parts of Facebook profiles that were formerly under privacy settings.[292] As with GeoCities, the FTC determined that this lack of disclosure constituted a Section 5 deceptive practice.[293] By failing to disclose its practices, Facebook promoted false expectations of privacy among its members.[294]

2. Surreptitious Collection of Personal Information

The FTC has also filed complaints against companies for failing to inform consumers when and how they collect personal data.[295] Sometimes, websites that surreptitiously collect personal data partially disclose their collection practices to users.[296] However, such disclosures may be inadequate when websites fail to notify users of the true scope of the information they collect, or how they acquire

---

286. *See id.* at 3.

287. *See* Reidenberg et al., *supra* note 47, at 21-22.

288. *See generally* Complaint, *In re* Facebook, Inc., FTC File No. 0923184, No. C-4365 (F.T.C. July 27, 2012).

289. *Id.* at 12.

290. *Id.*

291. *Id.* at 9.

292. *Id.*

293. *Id.* at 19.

294. *See id.* at 14.

295. *See, e.g., In* re Aspen Way Complaint, *supra* note 67 (collecting user data by remotely operating website users' webcams on their personal computers); *In re* Epic Marketplace, Inc. Complaint, *supra* note 67 (collecting users data by tracking their browsing histories).

296. *See, e.g.,* Complaint at 5, United States v. In re Path, Inc., F.T.C. File No. 1223158 (N.D. Cal. 2013).

that information.[297] For example, in *In re Upromise, Inc.*, Upromise, an online service that offered college savings to members, clandestinely collected users' data through its downloadable "Turbosaver Toolbar."[298] Upromise stated to users that the Toolbar collected information about websites that they visited in order to present savings opportunities tailored to their interests.[299]

The FTC determined that the Toolbar's data collection practices went beyond the scope of what Upromise disclosed to users.[300] The FTC found that the Toolbar collected users' passwords and usernames, information about every website they visited, and the links that they clicked.[301] The Toolbar also collected information from users' interactions on secured webpages such as banks and online retailers.[302] As a result, the Toolbar gathered users' financial account numbers, credit card numbers, social security numbers, and security codes.[303] The FTC found that without special software, or technical expertise, consumers had no means of discovering Upromise's true data collection practices.[304] The FTC concluded that Upromise's data collection constituted an unfair practice.[305] The true nature of Upromise's collection practices, which included gathering sensitive financial data, actually put users at risk for identity theft and other consumer harms.[306]

In a later enforcement action, *In re ScanScout*, the FTC articulated concrete standards for enhancing consumer notice of data collection practices.[307] The FTC initially filed the complaint against the video advertising network ScanScout due to its use of HTTP cookies.[308] ScanScout stated that consumers could "opt-out" of receiving cookies

---

297. *Id.* at 9.

298. Upromise Complaint, *supra* note 10, at 2. A "toolbar" is "a row of buttons on a display screen that are clicked on to select various functions in a software application or web browser." *Toolbar*, DICTIONARY.COM (2016), http://www.dictionary.com/browse/toolbar [https://perma.cc/UX3N-Y33N].

299. Upromise Complaint, *supra* note 10, at 2.

300. Upromise Complaint, *supra* note 10, at 5.

301. Upromise Complaint, *supra* note 10, at 2.

302. Upromise Complaint, *supra* note 10, at 2-3.

303. Upromise Complaint, *supra* note 10, at 3.

304. Upromise Complaint, *supra* note 10, at 2.

305. Upromise Complaint, *supra* note 10, at 6.

306. Upromise Complaint, *supra* note 10, at 3.

307. *See* Complaint at 2, *In re* ScanScout, Inc., File No. 102-3185, No. C-4344 (F.T.C. Dec. 14, 2011).

308. *See id.* (providing "HTTP cookies . . . are small text files that can be used to collect and store information about a user's online activities").

by changing their browser settings.[309] Nonetheless, flash cookies, which were stored in a unique location on consumers' computers, could not be deleted in this way.[310] The FTC determined that ScanScout violated Section 5 for making false and misleading statements to consumers.[311]

In the *ScanScout* decision and order, the FTC described how consumers should be apprised of the choice to opt-out of data collection practices.[312] The FTC ordered ScanScout to place a "clear and prominent notice" on its homepage that disclosed that it collected consumer data through targeted advertising.[313] Next to the disclosure, the FTC required ScanScout to include a link that consumers could click on to opt-out of the data collection.[314] The order provided that the link should lead consumers directly to a "clearly and prominently disclosed mechanism" that consumers could use to prevent future data collection.[315]

In the order, the FTC included a definition of "clearly and prominently."[316] It determined that "clear and prominent" disclosures are in a "type, size, and location sufficiently noticeable for an ordinary consumer to comprehend and read."[317] According to the FTC, the statements should also be in a print that "contrasts highly with the background on which they appear."[318] Additionally, the FTC stated that "in all instances," required disclosures must be presented in an "understandable language and syntax," not contradicted by any other statements.[319] By requiring ScanScout to be direct about its targeted advertising practices, the FTC sought to prevent future privacy harms caused by covert collections of consumer data.

---

309. *Id.*
310. *See id.*
311. *See id.* at 3.
312. Decision and Order at 4, *In re* ScanScout, Inc., File No. 102-3185, No. C-4344 (F.T.C. Dec. 14, 2011).
313. *Id.* at 3.
314. *Id.* at 4.
315. *Id.*
316. *See id.* at 2.
317. *Id.*
318. *Id.*
319. *Id.*

3. Failure to Secure Personal Information

A website's failure to secure users' personal data may be better characterized as a "broken promise" than as a failure to notify.[320] With regard to data security harms, the FTC does not focus on whether or not websites provided users with sufficient notice, but whether they breached their vows to keep user data secure.[321] For example, the FTC complaint in *In re Eli Lily & Co.*, is silent on the issue of notice.[322] Instead, the FTC was concerned with how the pharmaceutical company, Eli Lily & Co. ("Eli Lily"), breached its promise to keep consumers' personal information confidential,[323] and the company's failure to provide training, checks, and controls over consumers' sensitive information.[324]

Similarly, in *United States v. ChoicePoint Inc.*, the FTC did not characterize ChoicePoint Inc.'s ("ChoicePoint") failure to secure consumers' personal data in terms of notice.[325] ChoicePoint was a company that furnished personal data, like Social Security numbers, dates of birth, and credit card histories, to governments and businesses.[326] In its complaint, the FTC found that ChoicePoint violated Section 5 because it failed to employ "reasonable and appropriate security measures" to protect consumers' personal information.[327] Though the FTC found that ChoicePoint violated Section 5, concerns for proper notice were not part of the FTC's inquiry.[328] Rather, the FTC's concerns focused on ChoicePoint's

---

320. *See* Solove & Hartzog, *supra* note 17, at 643; Reidenberg et al., *supra* note 47, at 27 ("While the notice and choice framework may be effective to protect against privacy harms in some areas, the framework will inherently be unable to protect against some of the articulated harms. Breaches of commitments made in notices will violate the terms of user consent and create unauthorized disclosures, the inadequacy of data security cannot be cured by notice, and mismatches for data retention preclude the capability for notice to avoid the privacy harms.").

321. *See* Reidenberg et al., *supra* note 47, at 28.

322. *See generally* Complaint, *In re* Eli Lily & Co., FTC File No. 012 3214, No. C-4047 (F.T.C. May 8, 2002).

323. *Id.* at 2. Despite its promise, Eli Lily disclosed the email addresses of 669 of its customers after sending a mass email and leaving customers' emails visible in the "to:" line of the message. *Id.*

324. *Id.* at 3.

325. *See generally* Complaint, United States v. ChoicePoint Inc., FTC File No. 0523069 (N.D. Ga. 2006).

326. *Id.* at 3.

327. *Id.* at 9.

328. *See id.*

failures to sustain reasonable security measures, as well as the company's breached privacy promises to consumers.[329]

4. Unlawful Retention of Personal Information

FTC enforcement actions also cover instances in which companies unnecessarily retain personal data.[330] Still, the FTC does not address unlawful retention as a problem of insufficient notice, but as a security risk.[331] For example, in its complaint against CardSystems Solutions, Inc. ("CardSystems"), the FTC held that CardSystems failed to reasonably secure personal information that was stored on its computer network.[332] The FTC found that, in addition to failing to take reasonable measures to secure consumer data from hackers, CardSystems generated unnecessary risks by storing information for up to 30 days in an insecure state.[333] Like other FTC complaints, the company's retention practices were not challenged because consumers were not notified of how long their data was retained, rather, the retention practice was considered a Section 5 violation in that it caused the security and confidentiality of consumer data to be compromised.[334]

D. Notice Problems in the Online World

This Part examines various barriers to sufficient notice in the online space. This Part also analyzes different obstacles that consumers encounter when they are confronted with websites' privacy agreements, and how they prevent consumers from gaining awareness of websites' data handling practices. Specifically, this Part explores notice problems such as the high cost of reading privacy policies, the vague and misleading language that privacy polices

---

329. *Id.* at 9, 11; *see also* Solove & Hartzog, *supra* note 17, at 628; Reidenberg et al., *supra* note 47, at 28.

330. *See, e.g.,* Complaint at 2, *In re* BJ's Wholesale Club, Inc., File No. 0423160, No. C-4148 (F.T.C. June 16, 2005) (finding the store "created unnecessary risks to . . . information by storing it for up to 30 days when it no longer had a business need to keep the information"); Complaint, *In re* Ceridian Corp., FTC File No. 102 3160, No. C-4325 (F.T.C. June 8, 2011) (finding the business "created unnecessary risks to personal information by storing it indefinitely on its network without a business need").

331. *See* Solove & Hartzog, *supra* note 17, at 651, 653.

332. *See* Complaint at 2, *In re* CardSystems Solutions, Inc., FTC File No. 052 3148, No. C-4168 (F.T.C. Sept. 5, 2006).

333. *Id.*

334. *See id.*

commonly use, and consumers' general lack of awareness of how companies appropriate their personal data.

1. The Cost of Reading Privacy Policies

In the domains of arbitration provisions, FDA drug labeling and FTC enforcement actions, effective notice is critical to consumers' informed consent and awareness of risk. While settled principles of sufficient notice govern these areas of law, there is presently much discourse on how notice should be dispensed in the online world.[335] Under the notice and choice model, it is expected that online consumers self-manage their privacy by reading websites' privacy policies, and, upon notice of these terms, choose whether or not to consent to them.[336] However, some scholars contend that privacy policies fail to provide consumers with meaningful notice of websites' data practices.[337] Research shows that a majority of consumers fail to pay substantial attention to online notice statements.[338] For example, in a study only 4.5% reported that they "always read" privacy policies and only 14.1% reported to "frequently" read them.[339] Subjects of this study reported that privacy statements were too long and verbose to read.[340]

---

335. *See e.g.*, *Usable Privacy Project*, NAT'L SCI. FOUND. (2016), http://www.usableprivacy.org/ [https://perma.cc/63FM-LZUS] (exploring how natural language processing technology can be used to enhance notice of privacy policy conditions and terms).

336. *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1883 (2013).

337. FTC Chairman Jon Leibowitz has stated: "Initially, privacy policies seemed like a good idea. But in practice, they often leave a lot to be desired. In many cases, consumers don't notice, read, or understand the privacy policies." *Id.* at 1884-85, (citing Jon Leibowitz, Comm'r Fed. Trade Comm'n, *So Private, So Public: Individuals, the Internet & the Paradox of Behavioral Marketing, Remarks at the FTC Town Hall Meeting on Behavioral Advertising: Tracking, Targeting, & Technology* (Nov. 1, 2007)).

338. A 2002 study showed that only about .3% of Yahoo users read the websites privacy policy. Even after Yahoo began to send users' advertisements to their email accounts and mail, this figure rose to only 1%. *See id.* Another study reported that despite the fact that 63 out of 63 respondents reported to valuing privacy, only three reported to always reading online privacy. *See* Gordon, *supra* note 14, at 13.

339. Solove, *supra* note 336, at 1884 n.14 (citing George R. Milne & Mary J. Culnan, *Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices*, 18 J. INTERACTIVE MARKETING 15, 20-21 (2004)).

340. *See* Milne & Culnan, *supra* note 339, at 23 (finding one respondent of this study complained that "[p]rivacy notices are deliberately made too long and verbose. How about the 'Privacy Notice for Dummies' version?"). Other research has shown that consumers generally face considerable difficulty when trying to decipher policy privacy terms. *See* Aleecia M. McDonald, et al., *A Comparative Study of Online*

Consumers may refrain from reading privacy policies because they are too time-consuming and costly to read.[341] Aleecia M. McDonald and Lorrie Faith Cranor investigated this proposition and studied the true costs of reading privacy policies.[342] They calculated how much time and money the U.S. population would expend by reading every single privacy policy that it was exposed to over the course of a year.[343] The study took into account variables like opportunity costs of reading privacy policies,[344] the total amount of time it would take to read the privacy policies, and the financial value of that time.[345] McDonald and Cranor calculated that Americans, on average, visit 1462 unique websites annually.[346] The participants of their study spent a median of 23 to 24 minutes reading a typical 2500-word policy.[347] McDonald and Cranor determined that if Americans were to read every single privacy policy in a year, it would take them approximately 201 hours and cost them about $3534 annually.[348] They further calculated that if all Americans were to read privacy policies

---

Privacy Policies and Formats, *in* PRIVACY ENHANCING TECHNOLOGIES 37 (Ian Goldberg & Mikhail J. Atallah eds., 2009) (finding that "[m]ost privacy policies require a college reading level and an ability to decode legalistic, confusing, or jargon-laden phrases").

341. *See* Solove, *supra* note 336, at 1885.

342. *See generally* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 J.L. & POL'Y INFO. SOC'Y 540 (2008).

343. *Id.* at 548.

344. This included the loss of a potential financial gain when time is spent reading a privacy policy rather than an alternative, and potentially profitable, activity. *Id.* at 558-59.

345. *Id.* at 559-62.

346. *Id.* at 558. Some scholars assert that the multitude of privacy policies that consumers are exposed to on an annual basis alone may deter consumers from reading them. Daniel Solve has described this as the "overload effect," stating that the problem is similar to that of a student whose professors aggregately assign an excess of reading each night. In Solve's analogy, each professor believes their assigned reading is reasonable, but every professor assigns their own reading each night, the collective amount is too high. Thus, Solve concludes "even if all companies provided notice and adequate choices, this data management problem would persist; the average person just does not have enough time or resources to manage all the entities that hold her data." *See* Reidenberg et al., *supra* note 47, at 4 (citing Solve, *supra* note 336, at 1889).

347. *See* McDonald & Cranor, *supra* note 342, at 552-53. *See also* PROTECTING CONSUMER PRIVACY, *supra* note 38, at 70 ("A particularly strong illustration of where privacy notices have been ineffective is in the mobile context where, because of the small size of the device, a privacy notice can be spread out over 100 separate screens. Indeed, it is difficult to imagine consumers scrolling through each screen or making informed decisions based on the information contained in them.").

348. McDonald & Cranor, *supra* note 342, at 562.

word for word, the value of time lost would total about $781 billion annually.[349]

McDonald and Cranor concluded that typical consumers' failure to read privacy policies may not evince a lack of concern for privacy.[350] Rather, the great expense of reading privacy policies may simply outweigh Internet users' perceived costs of privacy harms.[351] McDonald and Cranor proposed that websites should reduce the cost of reading privacy policies.[352] They concluded that decreasing the amount of time it takes to read a privacy policy, which could entail reducing the amount of text displayed, would enhance privacy policies' practical benefits and utility to consumers.[353]

2. Ambiguity and Consumer Misunderstanding

a. Ambiguity of Privacy Policy Language

Research suggests that privacy policies are verbose, legalistic, and generally hard to read,[354] and that the language of privacy policies is ambiguous and misleading.[355] Thus, even if readers were able to understand the complex language of a privacy policy, there may still be confusion over what the terms of the policy actually mean.[356] A study by Professor Irene Pollach further demonstrates that the

---

349. McDonald & Cranor, *supra* note 342, at 562.

350. McDonald & Cranor, *supra* note 342, at 565. *See also* Chris Hoofnagle et al., *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies?*, 20 (April 14, 2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864 (surveying respondents of younger and older age and finding that large proportions of each group cared about their data privacy). *See also* PROTECTING CONSUMER PRIVACY, *supra* note 38, at 28-30, (citing studies that show that consumers care about their privacy and that a majority of consumers are uncomfortable with being tracked online).

351. McDonald & Cranor, *supra* note 342, at 565.

352. McDonald & Cranor, *supra* note 342, at 565.

353. McDonald & Cranor, *supra* note 342, at 565. *See also* Patrick Gage Kelly, *A "Nutrition Label" for Privacy*, *in* SYMPOSIUM ON USABLE PRIVACY AND SECURITY (2009), https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf (studying how privacy policies displayed in nutrition label-style formats can improve how consumers read and accurately interpret privacy policy terms).

354. *See* Milne & Culnan, *supra* note 339, at 23..

355. *See* Reidenberg et al., *supra* note 11, at 83.

356. *See* Patrick Cage Kelly, *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*, CHI 2010: PRIVACY (2010), https://pdfs.semanticscholar.org/23d6/ba79ae62fb928947c3330217d8b3ca23ff6f.pdf [https://perma.cc/SGE9-X5ZR] ("Rarely is a policy written such that consumers have a clear understanding of where and when their data is collected, how and by whom it will be used, if it will be shared outside of the entity that collected it, and for how long and in what form it will be stored.").

language of privacy policies may create more confusion than clarity.[357] Pollach analyzed the rhetorical patterns of fifty different privacy policies, finding that common trends in vocabulary, syntax, and grammar created ambiguity and confusion.[358] She determined that the choice of vocabulary in selected privacy policies "sugar-coat[ed]" companies' data handling practices by de-emphasizing their invasiveness and framing the practices in a positive light.[359]

Pollach also observed that privacy policies frequently denied that certain data practices were carried out.[360] She found that negative statements such as "except as otherwise stated we do not . . . " effectively gave companies "carte blanch . . . to engage in any practice not expressly ruled out."[361] Finally, Pollach observed that use of "modal" verbs and adverbs, such as "may," "might," and "perhaps" was a common trend among selected policies.[362] For example, a model phrase might state "[f]rom time to time [we] may also provide names, addresses or email addresses to strategic partners who have information, products or services that may be of interest to you."[363] She asserted that such modal language downplayed the frequency with which companies actually participated in data collection practices and allowed for open-ended interpretations of how companies appropriated consumer data.[364] Pollach concluded that companies likely draft privacy policies more with the aim to avoid privacy litigation than to inform consumers of their data handling practices.[365] She asserted that vague privacy policy language should

---

357. *See* Pollach, ***supra*** **note 13, at 104.**

358. *See* Pollach, *supra* note 13, at 105-06 (finding that when asking questions pertaining to key privacy concerns such as data collection, data storage, and unsolicited marketing communications of fifty different privacy policies, 39.4% of questions could not be answered because the policies lacked sufficient information).

359. Pollach, *supra* note 13, at 106.

360. Pollach, *supra* note 13, at 106 (finding that "not" was the ninth most popular word used throughout all privacy policies studied).

361. Pollach, *supra* note 13, at 106.

362. Pollach, *supra* note 13, at 106.

363. Pollach, *supra* note 13, at 107.

364. Pollach, *supra* note 13, at 106 (finding 948 instances of "may" and 123 instances of "might, perhaps, sometimes, occasional(ly), and from time to time" in the study).

365. *See* Pollach, *supra* note 13, at 107. *See also* PROTECTING CONSUMER PRIVACY, *supra* note 38, at 19 ("Too often, privacy policies appear designed more to limit companies' liability than to inform consumers about how their information will be used.").

be clarified to minimize ambiguity and accurately convey companies' true privacy terms.[366]

b. Misunderstanding of Privacy Policy Text

Other scholars' research suggests that, due to the vagueness of privacy policy language, even legal experts may have difficulty understanding their terms.[367] A study exploring privacy policy ambiguity surveyed three groups of participants: "Privacy Policy Experts," which was composed of legal and public policy scholars; "Knowledgeable Users," which consisted of law and computer science students; and "Crowd workers," which were selected as a representative sample of the general population.[368] All participants were required to read a privacy policy and then answer a question about a privacy practice (i.e., "Does the policy state that the website might collect contact information about its users?").[369] After selecting from the options "Yes," "No," "Unclear," or "Not Applicable," participants were asked to highlight the portion of policy text that supported their answer choice.[370]

Basing their judgments on privacy policies alone, study participants frequently disagreed upon the nature of companies' data-handling practices.[371] This disagreement was even apparent among the Privacy Policy Experts group, which consisted of four of the study authors who were experienced law and public policy scholars.[372] The study found that Privacy Policy Experts only reached a consensus on whether websites shared consumers' financial information 62.5% of the time, and only reached a consensus on whether websites' shared health information 50% of the time.[373] Vague policy terminology like "personal information" invited too much room for interpretation and made it difficult for privacy experts to agree on the kind of

---

366. Pollach, *supra* note 13, at 107-08. *See also* Reidenberg et al., *supra* note 47, at 26. ("Vague notices do not provide users with meaningful information about practices to which they are asked to consent. Such vague and incomplete notices deny users the ability to control their personal information . . . . By contrast, notice that is complete, accurate, and specific regarding the terms that explain how, with whom, and for what purpose a user's information will be shared enable effective consent from the user.").

367. *See* Reidenberg et al., *supra* note 11, at 40.

368. *See* Reidenberg et al., *supra* note 11, at 53-54.

369. *See* Reidenberg et al., *supra* note 11, at 56-57.

370. *See* Reidenberg et al., *supra* note 11, at 57-59.

371. *See* Reidenberg et al., *supra* note 11, at 83.

372. *See* Reidenberg et al., *supra* note 11, at 54.

373. *See* Reidenberg et al., *supra* note 11, at 65.

information that websites collected.[374] The study determined that privacy policies were often worded too ambiguously to convey effective notice, as privacy experts could not agree upon the accurate meaning of all of the privacy policy statements.[375] Due to poor drafting and confusing language, even experienced privacy scholars could not produce a uniform, professional interpretation of the privacy policies' terms.[376]

Disagreement was even more pronounced between the Knowledgeable Users and crowd worker groups. Knowledgeable User participants only agreed with each other 60% of the time when asked if a website's privacy policy indicated collection of shared location information data.[377] Similarly, crowd workers only agreed with each other 40% of the time when asked this same question.[378] The study concluded that overall lack of agreement among the three surveyed groups indicated that privacy policies lacked clarity and described data collection practices poorly.[379] The study determined that websites must candidly "spell out" their privacy practices to improve consumers' understandings of terms.[380] It asserted that lack of agreement and difficulties in interpretation evinced that consumers were being misled by website privacy policies.[381] The study contended that if privacy policies could not convey notice in a manner that a "reasonable person" could understand, then notice and choice failed as a framework.[382]

c. False Assumptions and Lack of Awareness

Research suggests that typical online consumers are unaware of the nature and scope of companies' data collection practices.[383]

---

374. *See* Reidenberg et al., *supra* note 11, at 79.

375. *See* Reidenberg et al., *supra* note 11, at 79.

376. *See* Reidenberg et al., *supra* note 11, at 79.

377. *See* Reidenberg et al., *supra* note 11, at 65.

378. *See* Reidenberg et al., *supra* note 11, at 65.

379. *See* Reidenberg et al., *supra* note 11, at 83-85.

380. *See* Reidenberg et al., *supra* note 11, at 83-84 ("To have contextual integrity, the granular aspects of a data practice, not just whether a website collects, shares or deletes personal information in general, will need to be understandable to a user. Indeed, a policy statement acknowledging general data collection and/or sharing may do very little to inform readers about the practices relevant to the user.").

381. *See* Reidenberg et al., *supra* note 11, at 83.

382. *See* Reidenberg et al., *supra* note 11, at 83.

383. *See* Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities that Enable It*, 21 (2009) (finding 54% of survey respondents wrongly stated that it was "True" that websites with privacy policies had to delete information like name and address upon their request); Solove, *supra* note 336, at 1886.

Consumers commonly harbor false assumptions about how websites collect their personal data.[384] Scholars Solon Barocas and Helen Nissenbaum contend that there are some key data collection and sharing norms that are simply unapparent to online consumers.[385] They note that when consumers access a website, they may not be aware that contracting third party advertisers may be tracking their interactions with that site.[386] Even if a website reveals how it collects consumer data through its privacy policy, this disclosure may still be incomplete because consumers are uninformed of how potential third party affiliates use their information.[387] Privacy policies cannot describe the tracking and data handling practices of third party advertisers, as websites are practically limited to disclosures about their own privacy practices.[388] Thus, the disclosures of privacy policies are inherently incomplete because policies fail to describe the full extent of what happens to consumer data.[389] Unbeknownst to consumers, third party advertisers may use personal data in a manner that contravenes the privacy promises of the main website.[390]

The "fickle" nature of privacy policies might also undermine consumers' expectations of privacy.[391] Many consumers may be unaware that the terms of privacy policies are often updated and changed.[392] As a result, consumers do not possess one absolute set of privacy rights under any given privacy policy. Describing the "fickleness" of privacy policies, Solon and Nissenbaum reference the New York Times website, which at one point, reserved the right to change the terms of the privacy policy upon thirty days' notice.[393] As a result, consumers that wished to stay informed of any potential changes bore the onus of checking the website's privacy statement every month.[394] Solon and Nissenbaum concluded that the "short

---

384. *See* Reidenberg, et al., *supra* note 11 at 78-80.

385. *See generally* Barocas & Nissenbaum, *supra* note 56 at 5.

386. *See generally* Barocas & Nissenbaum, *supra* note 56 at 5.

387. *See* Barocas & Nissenbaum, *supra* note 56 at 5.

388. *See* Barocas & Nissenbaum, *supra* note 56 at 6.

389. *See* Barocas & Nissenbaum, *supra* note 56 at 6.

390. *See* Barocas & Nissenbaum, *supra* note 56 at 6; *see also* GOMEZ ET AL., *supra* note 59, at 4. ("While most policies stated that information would not be shared with third parties, many of these sites allowed third party tracking through web bugs . . . . It makes little sense to disclaim formal information sharing, but allow functionally equivalent tracking with third parties . . . . Users do not know and cannot learn the full range of affiliates with which websites may share information.").

391. *See* Barocas & Nissenbaum, *supra* note 56, at 5.

392. *See* Barocas & Nissenbaum, *supra* note 56, at 5-6.

393. *See* Barocas & Nissenbaum, *supra* note 56, at 5.

394. *See* Barocas & Nissenbaum, *supra* note 56, at 5.

shelf-life" of online privacy policies undercut consumers' abilities to form accurate expectations of websites' privacy terms.[395] When subjected to changing terms, consumers may find that their former privacy expectations are no longer valid.[396]

III. ELEMENTS OF EFFECTIVE ONLINE NOTICE

As explored in Part C, the current format and content of typical online privacy policies routinely fail to notify consumers of companies' data collecting and sharing practices. Privacy policies are poorly drafted with vague and misleading language. Beyond this, privacy policies are too costly to read, and companies can freely modify core privacy terms without affirmatively notifying consumers. The chronic ineffectiveness of online privacy policies is highly problematic, as sufficient notice is central to an individual's ability to offer informed consent when sharing information online. Examining elements of effective legal notice from different legal models is an important preliminary step in resolving pervasive notice problems online. In the domain of arbitration clauses, for example, a showing of effective notice may evince individuals' knowing and voluntary waiver of guaranteed legal rights. In the context of FDA drug labeling rules, effective notice may ensure that consumers are properly apprised of warnings and directions for safe use. Finally, effective notice is inherent to FTC enforcement actions against unauthorized disclosures and surreptitious data collection.

Part III extracts the most salient elements of effective online notice from the aforementioned legal models. Using core common law principles of notice, and with reference to well-settled concepts of constructive notice and mutual assent, this Part evaluates the sufficiency of notice and "contract formation in cyberspace."[397] Part III also extracts principles from established legal paradigms to determine what constitutes effective online notice. By borrowing standards from judicial and administrative law, this Part outlines the most crucial elements of effective online notice. This Part also suggests how commercial websites can incorporate these elements into their regular data collection practices, which if implemented, may mitigate or prevent the notice problems discussed in Part C. These elements are also summarized in tables, which are featured in the Appendix to this Note.

---

395. *See* Barocas & Nissenbaum, *supra* note 56, at 6.
396. *See* Barocas & Nissenbaum, *supra* note 56, at 5-6.
397. *See* Specht v. Netscape Commc'n Corp., 306 F.3d 17, 20 (2d Cir. 2002).

A. The Format of Effective Notice

1. Readable Text

Effective notice demands that the text of privacy policies be legible and relatively easy to comprehend. Consumers commonly encounter difficulty with densely worded paragraphs of privacy policy text.[398] Though consumers tend to care about their online privacy, the majority of consumers do not read websites' privacy policies, with some complaining that the language of privacy policies is too legalistic and verbose.[399] The difficulty of reading privacy policies is thus a barrier to effective notice, as it discourages consumers from apprising themselves of privacy terms.[400] To achieve effective notice, the format of privacy policies should enhance their eye appeal and legibility. Incorporating the FDA's rule for "chunked" text may help to attain this goal.[401]

On average, a privacy policy consists of 2500 words.[402] As the FDA determined, dense paragraphs of fine print lack eye appeal and tend to overload consumers with information.[403] The same issues likely pertain to privacy policies, which often explain terms in paragraph form or in the context of one long statement. Chunking privacy policy information into lists would make privacy policies more usable for consumers. Adopting this formatting style would reduce the "cognitive load" many consumers may experience when reading dense blocks of privacy policy text.[404] Readers would not have to parse through an entire policy to find dispersed pieces of text that pertain to a specific data collection practice. For example, listing all terms that describe data sharing under a centralized heading would enable consumers to easily locate information related to this topic.[405] To accelerate readers' comprehension, companies could also organize core privacy terms under bullets,[406] which would visually stand out on

---

398. *See* PROTECTING CONSUMER PRIVACY, *supra* note 38, at 70 ("[P]rivacy notices are often opaque, lack uniformity, and are too long and difficult to navigate. Too frequently they bury disclosures of important information.").

399. *See* Milne & Culnan, *supra* note 339, at 23.

400. *See* PROTECTING CONSUMER PRIVACY, *supra* note 38, at 70.

401. *See* Vigilante & Wogalter, *supra* note 239, at 105.

402. *See* McDonald & Cranor, *surpa* note 342, at 552.

403. *See* Over-the-Counter Human Drugs; Labeling Requirements, 64 Fed. Reg. 13254, 13255 (Mar. 17, 1999).

404. *See id.*

405. *See* Vigilante & Wogalter, *supra* note 239, at 104.

406. *See* Over-the-Counter Human Drugs; Labeling Requirements, 64 Fed. Reg. at 13265-66.

a page and would naturally lead consumers' eyes to listed statements.[407] This formatting device may therefore be of particular use when alerting consumers to practices like sharing of financial data, which may expose consumers to special risks. Dividing privacy policy statements into discrete segments and lists could also reduce the frequency of consumer reading errors.[408]

If all privacy policies displayed key privacy terms in a standardized order, consumers could become familiar with this format and learn where to find specific terms in any privacy statement.[409] FDA labeling practices suggest that standardizing the sequence of privacy policy statements could reduce consumer confusion over policy terms.[410] Information across different OTC drug labels is displayed under the same headings and in a uniform order, and labels are organized according to core drug facts such as directions, warnings, and ingredients.[411] Similarly, a uniform privacy policy sequence could be organized with respect to key privacy terms. Such key terms would reference data collection practices that present the greatest risk to consumers for privacy harms. These terms would relate to practices such as data collection, sharing, and retention.

Presenting privacy terms in a uniform order would also reduce the burden of reading privacy policies.[412] This format would enable consumers to quickly identify a website's key privacy conditions.[413] Standardization would have the additional benefit of enabling consumers to compare privacy terms across different privacy statements.[414] If all privacy policies presented information in the same format and order, consumers could read two policies side by side and discern how data collection practices differ. This ability to compare

---

407. *See* ScanScout Decision and Order, *supra* note 312, at 2.

408. *See* Over-the-Counter Human Drugs; Labeling Requirements, 64 Fed. Reg. at 13266; Vigilante & Wogalter, *supra* note 239, at 104 ("Results indicated that list format instructions that included screen pictographs yielded fewer errors and help requests and decreased task completion times. The authors suggested that the list format allowed participants, particularly those familiar with the computer system, to scan the instructions for keywords. Other research has indicated that information grouping can facilitate the search and acquisition of information.").

409. *See* Over-the-Counter Human Drugs; Labeling Requirements, 64 Fed. Reg. at 13258.

410. *See id.* at 13264, 13266, 13271.

411. *See generally* 21 C.F.R. § 201.66 (2014).

412. *See* Kelley et al., *supra* note 353, at 11.

413. *See* Kelley et al., *supra* note 353, at 11.

414. *See* Kelley et al., *supra* note 353, at 11; Over-the-Counter Human Drugs; Labeling Requirements, 64 Fed. Reg. at 13258.

different privacy policies would encourage consumers to actively manage their privacy.[415]

Further, distilling paragraphs of privacy policy text into short and direct phrases could also enhance the effectiveness of privacy notices. As the FDA determined, statements that contain shorter sentences with simple terminology tend to reduce consumers' cognitive processing demands.[416] Reducing the text of privacy policies could free up consumers' memory and enable them to understand policies at a faster rate.[417]

Some privacy statements may be too detailed to reduce to shorter statements. Therefore, it may be helpful to feature a full privacy policy on a website that is juxtaposed with a summarized privacy statements as a companion. This would operate similarly to how OTC medications feature uniform product labels, but sometimes have package inserts that contain more extensive drug facts.[418] Just as consumers read OTC drugs labels to learn of potential health risks prior to their purchase, online users could refer to shortened statements of core privacy terms, such as data collection, sharing, and retention, prior to interacting with a website or transmitting personal data. Since consumers are not likely to read long privacy policies, a brief, summarized companion statement could, at the very least, offer a general landscape of a website's terms.

Symbolic representations of privacy warnings could also enhance the effectiveness of online notice. As previously discussed, the FDA endorses the use of pictograms to depict proper product use and minimize safety risks for non-English speaking consumers of OTC drugs and other products.[419] Websites could also graphically convey privacy warnings through visual illustrations. For example, a symbol signifying the collection of location information may depict a globe or map and could offer consumers enhanced notice of this practice. Interpreting such a symbol would not require command of any

---

415. *See* Kelley et al., *supra* note 353, at 11; *see also* PROTECTING CONSUMER PRIVACY, *supra* note 38, at 69 (noting that improving consumers' abilities to compare data practices across companies would encourage competition on privacy issues and in providing consumers with access to their data).

416. *See* Over-the-Counter Human Drugs; Labeling Requirements, 64 Fed. Reg. 13254, 13255 (Mar. 17, 1999).

417. *Id.*

418. *See* U.S. DEP'T OF HEALTH AND HUM. SERVS., GUIDANCE: DRUG SAFETY INFORMATION-FDA'S COMMUNICATION TO THE PUBLIC 7 (Mar. 2007), http://www.fda.gov/downloads/drugs/guidancecomplianceregulatoryinformation/guidances/ucm072281.pdf [https://perma.cc/83UT-6PS9].

419. *See Infant Formula; Labeling Requirements*, 48 Fed. Reg. 31880-01, 31883 (July 12, 1983).

particular language, so consumers of all backgrounds could comprehend its message.[420] The universal meaning of privacy symbols could provide consumers with identifiable warnings regardless of their primary language. Furthermore, symbols would apprise consumers with more instantly recognizable warnings, as opposed to typical blocks of privacy policy text, which must be read and interpreted.

2. Conspicuous Disclosures

Online privacy statements should conspicuously stand out to consumers on a webpage.[421] This visibility is necessary for consumers to notice and manifest consent to companies' privacy terms.[422] In the contract domain, constructive notice is premised on the idea that a party would have discovered a disputed provision had they been diligent.[423] Yet even diligent readers of privacy policies might be unlikely to notice important terms, as disclosures of key data practices are often buried in text or articulated in ambiguous language. Presenting privacy terms in small print and dispersing them throughout dense paragraphs is akin to the contract notion of unfair surprise.[424] Scattering critical disclosures throughout copious text effectively conceals these statements in plain sight.

If online consumers cannot learn of a website's privacy practices after reading its privacy statement, then they cannot be placed on constructive notice of a website's data collection practices.[425] Rather, it can only be said that online consumers have constructive notice of these practices if they would have had a fair opportunity to learn of

---

420. *See id.*

421. *See* Specht v. Netscape Commc'n Corp., 306 F.3d 17, 35 (2d Cir. 2002) ("Reasonably conspicuous notice of the existence of contract terms and unambiguous manifestation of assent to those terms by consumers are essential if electronic bargaining is to have integrity and credibility.").

422. *Id.* at 31.

423. Steel Warehouse Co. Inc. v. Abalone Shipping Ltd., 141 F.3d 234, 237 (5th Cir. 1998) ("Constructive notice can be defined, crudely, as a rule in which 'if you should have known something, you'll be held responsible for what you should have known.'").

424. *See* Zaborowski v, MHN Gov't Servs., Inc., 936 F. Supp. 2d 1145, 1152 (N.D. Cal. 2013) ("Surprise involves the extent to which supposedly agreed-upon terms of the bargain are hidden in the prolix printed form drafted by the party seeking to enforce them."); A & M Produce Co. v. FMC Corp., 135 Cal. App. 3d 473, 486 (Ct. App, 1982) (same).

425. *See* RESTATEMENT (SECOND) OF CONTRACTS: CONDUCT AS MANIFESTATION OF ASSENT § 19(2) (1981).

them after reading a website's privacy statement.[426] Applying this contract standard, privacy policies should, at the very least, put consumers on constructive notice of a website's data practices. In other words, privacy policies should be formatted so that "reasonably prudent" consumers will be capable of understanding their terms after reviewing them.[427]

Critical privacy terms (like those pertaining to the collection or sharing of personally identifiable data) should be conspicuously pronounced in the body of policy text so that they are easily noticed.[428] "User-friendly" formatting devices such as bold type, italics, capital letters, headings, and subheadings can also be used to highlight these terms and guide consumers' eyes to important disclosures.[429] These formatting devices may be implemented for visual contrast and to ensure that vital conditions are not buried in fine print.

Consumers cannot learn of privacy policy terms that they physically cannot see. Therefore, imposing minimum type size requirements, as the FDA implemented in its labeling rule, could also improve online notice.[430] A mandatory baseline type size could ensure that statements are clearer to see and more easily stand out on a webpage. Moreover, this minimum standard would ensure that a wider audience of consumers could read privacy policies, especially those with imperfect vision.[431]

FTC privacy jurisprudence suggests how websites can enhance actual and constructive notice of the choice to opt-out of their data collection practices. As the FTC demonstrated in *ScanScout*, effective notice requires websites to conspicuously disclose how consumers can opt-out of data collection practices.[432] In *ScanScout*, the FTC described how opt-out mechanisms should be "clearly and

---

426. *See* RESTATEMENT (SECOND) OF CONTRACTS: WHEN A MISREPRESENTATION PREVENTS FORMATION OF A CONTRACT § 163 (1981).

427. *See* Specht v. Netscape Commc'n Corp., 306 F.3d 17, 30 (2d Cir. 2002).

428. *See* PROTECTING CONSUMER PRIVACY, *supra* note 38, at vii ("[A]lthough privacy policies may not be a good tool for communicating with most consumers, they still could play an important role in promoting transparency, accountability, and competition among companies on privacy issues – but only if the policies are clear, concise, and easy-to-read.").

429. *See* Over-the-Counter Human Drugs; Labeling Requirements, 64 Fed. Reg. 13254, 13254 (Mar. 17, 1999).

430. *See generally id.*

431. *See generally*, Watanabe, *supra* note 249 (studying the geriatric population's ability to comprehend fine print amid visual impairment).

432. *See In re* ScanScout, Inc., File No. 102-3185, No. C-4344, 2-3 (F.T.C. Dec. 14, 2011).

prominently" displayed to consumers.[433] The FTC prescribed that the "type, size, and location" of this mechanism be "sufficiently noticeable" for consumers to read.[434] The FTC also required that the disclosure statement contrast highly with a webpage's background.[435]

Visible opt-out mechanisms are also critical to consumers' awareness and abstention from the clandestine tracking and collection practices of online advertisers.[436] The majority of consumers are not aware that third party advertisers track their data to display ads and likely would not search for an opt-out mechanism on a website. Thus, opt-out mechanisms should be visible enough to alert consumers of, and assist them in, revoking their participation in discreet marketing practices.[437] Ideally, opt-out mechanisms should be prominently displayed on a webpage to ensure that when companies do share personal information for marketing purposes, consumers are offering informed consent.

B. The Content of Effective Notice

1. Accurate Disclosures

As an initial matter, websites should accurately disclose how and when they collect sensitive, personally identifiable consumer data as well as the types of personally identifiable data that they collect. Consumers cannot offer informed consent to privacy terms if they do not know what practices they are assenting to, and sharing sensitive or personally identifiable data places consumers at a greater risk of

---

433. *Id.*

434. *Id.* at 2.

435. *Id.*

436. *See* Barocas & Nissenbaum, *supra* note 56, at 6.

437. *See* Joseph Turow, Lauren Feldman & Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline*, UNIV. OF PA., ANNENBERG PUB. POL'Y CTR. 5 (2005), http://repository.upenn.edu/cgi/viewcontent.cgi?article=1035&context=asc_papers ("[T]he government should require retailers to disclose specifically what data they have collected about individual customers as well as when and how they use those data to influence interactions with them."); PROTECTING CONSUMER PRIVACY, *supra* note 38, at 60 ("Different mechanisms for obtaining opt-in and opt-out consent can vary in their effectiveness. Indeed, a clear, simple, and prominent opt-out mechanism may be more privacy protective than a confusing, opaque opt-in. Staff has already stated that, regardless of how they are described, choices buried within long privacy policies and pre-checked boxes are not effective means of obtaining meaningful, informed consent. Further, the time and effort required for consumers to understand and exercise their options may be more relevant to the issue of informed consent than whether the choice is technically opt-in or opt out.").

privacy harms.[438] Without accurately describing the true nature and scope of their data collection practices, websites impose risks onto consumers, which they were never given a choice to assume.

Furthermore, websites' actual data collection practices of personally identifiable data should not contradict the disclosures of their privacy statements. For example, in *GeoCities*, the FTC found that GeoCities breached its own privacy policy by collecting users' names, birthdates, zip codes, and "optional" information, such as education level, income, and occupation.[439] The Geocities privacy policy stated that it would "NEVER" share this data with anyone without user permission.[440] In practice, however, Geocities rented and sold users' personally identifiable information to third party advertisers without users' informed consent.[441]

Accurate disclosures in privacy policies are even more critical in instances where consumers do not expect to be subject to data collection or sharing. Consumers often do not suspect that websites gather their personal data.[442] Websites should thus present clear and specific disclosures that describe the actual mechanisms they employ if they collect or share consumer data. In other words, if certain features of a website, like that of a downloadable toolbar, gather data in a manner that consumers would not ordinarily expect, that website should disclose this data collection practice so consumers do not develop erroneous assumptions about the purposes of those features. This would help ensure that companies' commercial websites do not actively or inadvertently mislead consumers' expectations of privacy.

2. Precise Language

Privacy policies should provide consumers with accurate and concrete descriptions of websites' data collection practices. Presently, many privacy statements are too ambiguous to provide consumers with clear impressions of websites' data collection practices.[443] For example, rather than stating that a website collects users "personal

---

438. *See* Upromise Complaint, *supra* note 10, at 3 (explaining sharing consumers' credit card numbers or banking information, for example, exposes consumers to a greater threat of identity theft).

439. *See* GeoCities Complaint, *supra* note 278, at 2-4.

440. *Id.* at 3.

441. *Id.*

442. *See* Turow, Feldman & Meltzer, *supra* note 437, at 3 (finding that 75% of those surveyed did not "know the correct response—false—to the statement, 'When a website has a privacy policy, it means the site will not share my information with other websites and companies.'"); Solove, *supra* note 336, at 1886.

443. *See* Reidenberg et al., *supra* note 11, at 64.

information"—an indefinite term—a privacy statement should list the actual kinds of information that a website collects. Additionally, articulating privacy policy statements in direct, action-oriented phrases could improve consumer notice. Similar to how the FDA requires OTC drug labels to feature statements such as, "see your doctor if . . . ," privacy statements could be formulated to give consumers clear ideas of what steps they should take to secure their data.[444] For example, if a privacy policy states that a website uses cookies to collect user data, it could follow this disclosure with a directive phrase such as, "to change your privacy settings . . . " to help consumers limit such collection. These instructive statements would offer clarity as to what specific steps consumers could take to proactively manage their privacy.

Changing the grammar and syntax of some online disclosure statements could also make notice more effective. Permissive phrases such as "may collect," "may share," and "from time to time" contribute to consumer confusion.[445] Instead, effective notice statements should be expressed in definite language to inform consumers if a website does indeed engage in a particular practice. Replacing terms like "may collect" or "from time to time" with "we *will* collect your data *when* . . . ," and "we *will* share your data *with* . . . " would clarify the nature and extent of websites' actual data collection methods. More so, articulating disclosures in straightforward terms would deter consumers from developing false expectations of websites' privacy conditions.[446] This is because conditional terminology can conjure doubt as to the extent of a website's participation in data collection.[447]

Finally, changing the structure of some privacy statements from the passive voice to the active voice could increase the clarity of privacy disclosures.[448] Modifying vague, typical policy phrases such as, "your information may be shared" to "*we* share your information *with X, Y,*

---

444. *See* 21 C.F.R. § 201.66(c)(5)(vii) (2014) ("Stop use an ask a doctor if . . . ").

445. *See* Pollach, *supra* note 13, at 106-07.

446. *See* Upromise Complaint, *supra* note 10, at 3. In its complaint, the FTC states that the Upromise TurboSaver Privacy Statement declared that the Toolbar may "infrequently" collect some personal information and "every commercially viable effort" would be made "to purge their databases of any personally identifiable information." Upromise Complaint, *supra* note 10, at 3. Nevertheless, the FTC found that the Toolbar transmitted the personally identifiable information that it gathered. This information included credit card and financial account numbers and Social Security numbers entered into secure web pages. Upromise Complaint, *supra* note 10, at 3.

447. *See* Pollach, ***supra* note 13, at** 106-07.

448. *See* Pollach, *supra* note 13, at 106.

Z. . . " would give consumers better insight into what actors are handling their data.[449] Passive sentence structures enable websites to downplay their participation in data collection, and conceal what other parties may be involved in such practices.[450] Adopting the active voice in disclosure statements would make which parties are accountable for data collection and sharing more apparent.

3. Affirmative Consent to Modified Material Terms

Some courts have held that revised contracts merely have the status of a new offer, and are not binding on a party until its terms are accepted.[451] A party must therefore be notified of new terms to manifest assent; "an offeree cannot actually assent to an offer unless he knows of its existence."[452] Applying this contract principle to online privacy agreements, websites too should require consumers to affirmatively agree to privacy policy changes prior to appropriating consumer data in a materially different manner.[453] At minimum, effective notice requires websites to apprise consumers of material changes to privacy policy terms and to obtain consumers' consent.

The contract principle of unconscionability may also be applicable in cases in which websites unilaterally change their terms without notice. In *Hooters v. Phillips*, the Fourth Circuit refused to enforce an arbitration provision in an employee contract because the employer reserved the right to change arbitration terms at any point post-agreement.[454] In this same way, privacy policies could be considered voidable if companies make material modifications without attaining consumer notice and consent. Companies' abilities to alter consumers' privacy rights at will and without notice reflect a disparity in bargaining power between companies and consumers. This lack of mutuality has been held to be a defining characteristic of an unconscionable and voidable agreement.[455]

---

449. *See* Pollach, *supra* note 13, at 106.

450. *See* Pollach, *supra* note 13, at 106.

451. *See* Douglas v. U.S. District Court for Cent. Dist. of Cal., 495 F.3d 1062, 1066 (N.D. Cal. 2007)

452. *See* 1 SAMUEL WILLISTON, A TREATISE ON THE LAW OF CONTRACTS § 4:16 (Richard A. Lord, 4th ed. 1990).

453. *See* Douglas v. Dist. Court for Cent. Dist. of Cal., 495 F.3d 1062, 1066 (9th Cir. 2007) ("A revised contract is merely an offer and does not bind the parties until it is accepted.") (citing Matanuska Valley Farmers Cooperating Ass'n v. Monaghan, 188 F.2d 906, 909 (9th Cir. 1951)).

454. *See* Hooters of Am., Inc. v. Phillips, 1173 F.3d 933, 941 (4th Cir. 1999).

455. *See id.* at 936.

FTC jurisprudence also suggests that websites' material modifications to privacy policies without consumers' consent may qualify as an "unfair . . . practice."[456] In *Facebook*, for example, the FTC determined that Facebook committed a deceptive practice because it changed its privacy policy to increase the visibility of users' accounts to third parties.[457] As *Facebook* demonstrates, routine notice of material policy changes is critical in the context of social media websites, as these websites especially gather vast quantities of personally identifiable information. Social media websites in particular should routinely request consumers' express consent prior to executing changes that could alter the privacy of personal data; such websites should not commence new data collection or sharing practices prior to receiving this express consent.[458]

On the whole, requiring routine agreement to policy changes could ultimately create more realistic expectations of online privacy.[459] Acquiring consumers' express consent to modifications would endow them with a more meaningful say in how their data is appropriated. Finally, alerting consumers to material changes would relieve them of the onus of having to regularly check for modifications in privacy terms. Consumers would be able to rely on the fact that the websites would apprise them of updates as soon as "fickle" privacy policies were modified.[460]

4. "Knowing and Voluntary" Assent

Some data collection practices prompt consumers to waive privacy rights that are protected by state and federal statutes. For example, some websites have been known to collect personally identifiable health and financial data from consumers.[461] These collection practices contravene the statutory purposes of HIPAA, which guards the privacy of medical records,[462] and the Gramm–Leach–Bliley Act,

---

456. *See* Facebook, Complaint, *supra* note 288, at 9.

457. *See id.*

458. *See* PROTECTING CONSUMER PRIVACY, *supra* note 38, at 76-77.

459. *See* PROTECTING CONSUMER PRIVACY, *supra* note 38, at 76-77.

460. *See* Barocas & Nissenbaum, *supra* note 56, at 5-6.

461. *See* Reidenberg et al., *supra* note 11, at 63 (evaluating study participants' awareness of companies collection practices of health and financial data.).

462. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 26 U.S.C., 28 U.S.C., and 42 U.S.C.).

which prevents financial institutions from disclosing consumers' financial data to third parties.[463]

If institutions such as hospitals, insurance companies, and banks are forbidden from surreptitiously sharing personally identifiable data, then commercial websites too should be held to similar standards. Though constructive notice may suffice in many contexts, when data collection practices implicate legally protected privacy rights, a more stringent notice standard is required. The notice model in these contexts should be analogous to that of the "knowing and voluntary" standard in arbitration clause disputes.

Though the knowing and voluntary standard of review is not the default means of evaluating arbitration contracts, it may be applied in special cases where arbitration agreements prompt signatories to forfeit guaranteed legal rights. As the Ninth Circuit suggested in *Nelson v. Bagdad Copper Corp.*, when websites collect data that is protected by state and federal statutes, higher standards of notice should be in place.[464] Websites' privacy terms should not contravene or undermine the purposes of established privacy laws. Though websites need not mold their privacy practices according to the privacy laws of every state or nation, they should provide elevated notice when collecting particularly sensitive consumer information that is sometimes protected by statute. Health and financial information, in particular, should require a more stringent standard of notice. Not only is this data protected by both state and federal privacy laws, but it also tends to create greater risks of privacy harms when collected and shared.[465]

---

463. The Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et. seq. (2012). Additionally, data handling practices that covertly collect consumer data may undermine the intent of some state privacy laws. California's Consumer Protection Against Computer Spyware Act, for instance, prohibits companies from installing spyware on consumers' computers for data collection purposes. CAL. BUS. & PROF. CODE § 22947-22947.6 (West 2015).

464. *See* Nelson v. Bagdad Copper Corp., 119 F.3d 756, 762 (9th Cir. 1997) ("Any bargain to waive the right to a judicial forum for civil rights claims, including those covered by the [Americans with Disabilities Act] . . . must at least be express."); Lindgren v. Pub. Storage, 290 F. App'x 971, 972 (holding that forms signed by a former employee did not effectuate knowing agreement to submit civil rights claims against a former employer to arbitration).

465. *See, e.g.*, VT. STAT. ANN. TIT. 9, § 2480e(a)(2) (West) ("A person shall not obtain the credit report of a consumer unless the person has secured the consent of the consumer, and the report is used for the purpose consented to by the consumer."); TENN. CODE ANN. § 45-10-104 ("[A] financial institution may not disclose to any person, except to the customer or the customer's agent, any financial records relating to that customer . . . ").

To adapt the "knowing and voluntary" standard for the online world, companies could expressly notify consumers of their collection of health or financial data on their homepages. Though websites are limited in that they cannot apprise consumers with personal warnings, they can put mechanisms in place to prevent consumer interaction with their content until a notice statement is acknowledged. A conspicuous opt-out option would fortify the legal significance of consumers' consent. If consumers were actually given the choice to deny a website's collection of their sensitive, personally identifiable data, then their decision to allow this collection to proceed would be more voluntary and meaningful.

CONCLUSION

Existing legal models can provide valuable insight into the elements of effective online notice. FDA labeling rules demonstrate that changing the format of privacy policies could improve their readability and eye-appeal. Shortening lengthy paragraphs and distilling long sentences into brief phrases could reduce consumers' cognitive load and enhance their understanding of key terms. FTC enforcement actions also provide insight into the essential content of online notice statements. These actions show that websites should apprise consumers of material changes to privacy policies and give them the opportunity to expressly consent to those new terms.[466] Finally, jurisprudence of arbitration agreements reveals that there should be elevated standards of consent when privacy policies prompt consumers to waive protected legal rights. The "knowing" agreement standard, as applied to the privacy space, demonstrates that sensitive health and financial data should not be any less protected online than it is under federal privacy laws.[467]

Nevertheless, even if websites were to incorporate essential elements of effective notice into their privacy statements, notice problems would remain. Improving notice would not address issues relating to companies' unnecessary retention[468] of and failure to secure[469] personally identifiable data. Additionally, companies may not always have notice or control of the data collection practices of

---

466. *See, e.g.*, Facebook, Complaint, *supra* note 288, at 7-9.

467. *See* Lindgren v. Pub. Storage, 290 Fed. Appx. 971 (9th Cir. 2008); Morrison v. Circuit City Stores, Inc., 317 F.3d 646, 668 (2003); Nelson v. Cyprus Bagdad Copper Corp., 119 F.3d 756, 761 (9th Cir. 1997); Gibson v. Neighborhood Health Clinics, Inc., 121 F.3d 1126, 1130 (7th Cir. 1997).

468. *See* Reidenberg, et al., *supra* note 47, at 24.

469. *See, e.g.,* Eli Lily Complaint, *supra* note 322, at 2.

third party advertisers that routinely access their websites. Therefore, even if a company were to draft an ideal privacy policy that effectively conveyed notice, third party data collection practices could easily contravene the promises of that policy.[470]

Despite these limitations, notice remains a vital tool for the prevention of privacy harms. Companies should draft and format privacy policies to provide consumers with clear and accurate notice of websites' actual data collection practices. Improving the content and format of privacy policies to mirror legally accepted notice standards would enhance policies' usability and eye-appeal to consumers. Consumers would be more likely to read privacy policies and actively manage their privacy if they found policies readable and trustworthy. At the very least, improved policies would supply constructive notice, and enable inquiring consumers to have a fair chance of learning about websites' actual data collection practices.

---

470. *See* Barocas & Nissenbaum, *supra* note 56, at 5; PROTECTING CONSUMER PRIVACY, *supra* note 38, at 76-77.

Table 1: Format of Effective Notice

TYPE OF NOTICE	NOTICE MECHANISM
Symbolic disclosures	Symbols, pictograms, and bulleted statements to accelerate understanding of terms
"Chunked" formatting	Statements that are "chunked" into brief phrases as opposed to blocks of text; "chunked" disclosures organized into lists can serve as user-friendly companions to longer privacy statements
Standardized sequences of notice statements	Standardizing the order in which data collection practices are disclosed (similar to how all drug labels disclose drug facts in the same sequence) to enable consumer comparisons of different privacy statements
Conspicuous disclosures and warnings	Manipulation of type size, capitalization and bold type to emphasize critical privacy terms, especially those relating to collection of personally identifiable data

Table 2: Content of Effective Notice

Clear disclosures	Short, action-oriented warning statements that direct consumer behavior; precise, definite language and use of the active voice	FDA OTC drug labels, which clearly describe steps to take before consuming a drug ("i.e. see your doctor if . . . " "keep out of reach from children"). *See* 21 C.F.R. § 201.66 (5)(ii)(x).
Accurate disclosures	Privacy policies that describe the actual nature and scope of privacy practices; privacy policies that do not make promises that contravene companies' actual data collection practices	*See* e.g., *In re* Upromise, Inc., Complaint, FTC File No. 102 3116 at 3 (Finding that a company told users its toolbar collected browsing data to offer savings, but it actually collected personally identifiable data such as banking information).
Notice statements that require express, "knowing and voluntary" consumer assent	Privacy policies that require express and informed consumer consent prior to engaging in data practices that implicate legally protected privacy rights	Elevated notice standards for the collection of financial information like bank and credit card numbers (otherwise protected by the Gramm–Leach–Bliley Act); elevated notice standards for the collection of health information such as medical history (HIPPA).

Regular notification of modified privacy policy terms	Privacy statements that routinely update consumers of material changes and require express consent before such changes go into effect	Requiring express notice and affirmative consent when making private consumer data public. *See,* e.g. *In re* Facebook, Inc., Complaint, FTC File No. 092 3184.