Hastings Communications and Entertainment Law Journal

Volume 35 | Number 1 Article 4

1-1-2012

"I Agreed to What?": A Call for Enforcement of Clarity in the Presentation of Privacy Policies

David Thompson

"I Agreed to What?":

A Call for Enforcement of Clarity in the Presentation of Privacy Policies

by
DAVID THOMPSON

I. Introduction

If you've installed a computer application or joined an online social network in the past ten years, the following language should seem familiar to you: "Before proceeding, you must read and agree to the following Terms and Conditions," followed by a statement such as, "By checking the box titled 'I Agree to the Terms and Conditions,' you agree to be bound by this Agreement." If you're like most users, you treat this as a prompt to rapidly scroll through an inordinately long jumble of text, click the appropriate box, and get on with the more important business of installing your software or setting up your account. Even if you are among the elite ranks[1] of those diligent (or paranoid) enough to read through a twenty-five page contract before clicking through, chances are good that you liberally consulted Black's Law Dictionary or hired an attorney in order to translate it from legalese to plain English.

Most of us give little thought to these terms and conditions after installation or signup and they rarely resurface as a concern for the average consumer. Nonetheless, in an increasingly information-driven economy, there are important and compelling reasons to address corporations' widespread failure to make their privacy

1. Jo Rimmer, *Skandia Takes the Terminal Out of Terms and Conditions*, SKANDIA (Feb. 16, 2012), http://www2.skandia.co.uk/Media-Centre/2011-press-releases/May-2011/SKANDIA-TAKES-THE-TERMINAL-OUT-OF-TERMS-AND-CONDITIONS/. ("[O]nly 7% of adults always read full online terms and conditions when signing up for products and services.")

policies comprehensible and of reasonable length.[2] The Federal Trade Commission, whose principal mission is the promotion of consumer protection, has recently begun to acknowledge the extent and significance of this problem, finding most corporate privacy policies are "incomprehensible" and "consumers typically do not read, let alone understand" these privacy disclosures.[3] In response, the FTC has entered into multiple consent orders with companies over alleged failures to make proper privacy disclosures,[4] some of which can remain in effect for as long as 20 years.[5]

But why, exactly, should consumers and regulatory agencies be concerned about the average consumer's ability to understand a company's privacy policy? For one, it is a matter of courtesy to the user, whose information and online behavior is often tracked and recorded for the purpose of improving the efficacy of targeted advertising and/or improving the company's analysis of consumer trends.[6] More important from a legal perspective, however, is the issue of informed consent. [7]

The regulatory model for nearly all consumer issues in the United States, from food packaging to credit cards, is traditionally based on disclosure.[8] If, however, people do not understand what they are reading, there is a compelling argument that the rote exercise of disclosure is inadequate and the putative "agreement" should not be considered valid.[9] The mortgage crisis of 2008 is a salient and still-smarting example of the shortcomings of uninformed consent.[10]

2. Paul Bond and Chris Cwalina, Making Your Privacy Policy Comprehensive and Comprehensible, Corporate Counsel (Sep. 1, 2011), http://www.law.com/jsp/cc/PubArticleFriendlyCC.jsp?id=1202512963808.

3. Id.

4. Id.

5. Id.

6. Andy Chen, The Three Dimensions of Behavioral Targeting, ClickZ (Sep. 1, 2004), http://www.clickz.com/clickz/column/1710638/the-three-dimensions-behavioral-targeting.

7. Telephone Interview with Mark Melodia, partner at Reed Smith, LLP (Oct. 29, 2011).

8. See The Fair Packaging and Labeling Act, 15 U.S.C. §§ 1451-1461 ("[R]equiring that all consumer commodities other than food, drugs, therapeutic devices, and cosmetics be labeled to disclose net contents, identity of commodity, and name and place of business of the product's manufacturer, packer, or distributor.") and the Fair Credit Reporting Act, 5 U.S.C. §§ 1681-1681u, available at http://www.ftc.gov/ogc/stat3.shtm.

9. Telephone Interview with Mark Melodia, partner at Reed Smith, LLP (Oct. 29, 2011).

10. Celeste M. Hammond & Ilaria Landini, The Global Subprime Crisis as Explained by the Contrast between American Contracts Law and Civil Law Countries' Law, Practices and Expectations in Real Estate Transactions 1 (2011).

Invalidating an agreement simply because the user failed to understand its provisions would seem to violate the fundamental precept that ignorance of the law is no excuse for transgressing it.[11] Historically, this tenet also extends to consumer transactions; i.e., if you say you read a contract and agreed to its terms, you should be bound by those terms.[12] But this maxim is not without exception.[13] Certain contractual doctrines, such as adhesion and unconscionability, recognize that not all formally agreed-upon contracts are valid; they chip away at the presumption that a consumer has read, and more importantly, *understood*, everything in the contract.[14] However, common law standards enabling the court to refrain from enforcing an offending provision, such as fraud and duress, are very limited and often difficult to prove. Thus, the current legal landscape governing privacy policies is an uncanny one; the industry is expected to regulate itself, yet very little recourse is available to the average consumer who has been injured as a result of an unfair policy.[15]

Though the federal government has enacted statutes regulating privacy policies in limited contexts,[16] there is no generally applicable law governing the nature of privacy policies across all industries.[17] In light of the ever-increasing prevalence of user data collection and the widespread failure of companies under the self-regulatory model to make their policies readable, of reasonable length, and placed in a noticeable location, I argue that such a regulation should be promulgated.

This note will address the difficulties of preserving one's privacy in the digital era, discuss common shortcomings of privacy policies,

11. Ray v. William G. Eurice & Bros., 201 Md. 115, 125 (1952). ("The law is clear, absent fraud, duress or mutual mistake, that one having the capacity to understand a written document who reads and signs it, or, without reading it or having it read to him, signs it, is bound by his signature in law, at least.").

12. *Id.*

13. Unconscionable Contract or Term, Unif. Commercial Code § 2-302.

14. *Id.*

15. Steven A. Hetcher, *Norm Proselytizers Create a Privacy Entitlement in Cyberspace*, 16 BERKELEY TECH. L.J. 877, 921 (2001).

16. *See* Children's Online Privacy Protection Act (COPPA) 15 U.S.C. § 6501 et. seq. (2006), which regulates websites that target children under the age of thirteen; The Gramm-Leach-Biley Act, 15 U.S.C. § 6801 et. seq., governing institutions that are "significantly engaged in financial activities; and Health Insurance Portability and Accountability Act (HIPPA), 42 U.S.C. § 201 et. seq., requiring written notice of privacy policies in health care services.

17. *What is a Privacy Policy?*, PRIVACY POLICY ONLINE, http://www.privacypolicyonline.com/what-is-a-privacy-policy/ (last visited Mar. 2, 2012).

explore the negative consequences of these shortcomings, then analyze best practices and discuss how they might be integrated into a regulatory framework.

II. Background: The Problem of Maintaining Privacy in the Digital Age

In the seminal 1890 Harvard Law Review article titled, "The Right to Privacy," future Supreme Court Justice Louis Brandeis and his former law school classmate, Samuel Warren, observed that recent innovations such as photography and newspapers compromised one's ability to control the "public dissemination of details relating to . . . [his or her] private life."[18] Troubled by the potential harm that could befall the hapless citizen as a result of these developments, they argued for the creation of a "general right to privacy which would protect the extent to which one's thoughts, sentiments, and emotions could be shared with others."[19] This purported "right" was to be distinguished from that which protects the fruits of one's thoughts and emotions, i.e., intellectual property rights.[20] Rather, it was meant to protect the integrity of the most intimate sphere of one's being; the very "right to one's personality."[21] Warren and Brandeis insisted that this concept was not born of their whim or invention, but that it was deeply ingrained and interwoven throughout the common law.[22] Nonetheless, "new technology made it important to explicitly and separately recognize this protection under the name of privacy."[23] Thus, in their famous declaration of the inviolable "right to be let alone,"[24] Warren and Brandeis "laid the foundation for a concept of privacy that has come to be known as control over information about oneself."[25]

Brandeis' and Warren's clarion call for the development of a legal mechanism that would offer shelter from the increasingly intrusive nature of mass media and other technologies was both prescient and timely. The advent of mass media, the dawn of the Information Age,

18. Judith DeCew, *Privacy*, THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (2008), http://plato.stanford.edu/archives/fall2008/entries/privacy/.

19. *Id*.

20. *Id*.

21. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 207 (1890).

22. DeCew, *supra* note 18.

23. *Id*.

24. Warren & Brandeis, *supra* note 21 at 194.

25. DeCew, *supra* note 18.

and the unprecedented, life-altering advances, conveniences, and privacy invasions that would come along with them were within a century of realization.[26]

Yet, the comprehensive privacy protections called for by Brandeis and Warren have not come to fruition. Though the Supreme Court ultimately recognized and established a general right to privacy in the 1965 case, *Griswold v. Connecticut*,[27] the right has thus far only ensured protection from the most egregious, fundamental invasions of one's personal life carried out by a *government actor* (i.e., it only offers protection against state action).[28] Today, however, perhaps the greatest threat to our privacy does not stem from government action, but from private enterprises that profit from disclosures we make about ourselves in an online forum.

Take the online social network, Facebook. It is the fastest-growing online social network, having accumulated 400 million users in its first four years,[29] with nearly 700 million users as of 2011.[30] By 2010, it had surpassed Google as the most visited website on the internet.[31] Now, "Facebook usage is so ubiquitous as to almost be seen as a public service," [32] if not "a requisite for most internet users."[33] Cory Doctrow, a blogger, journalist, and science-fiction author, argues that Facebook and other online social networks are particularly troubling in terms of privacy implications because they employ "powerful, game-like mechanisms" that reward disclosure of

26. Randy Kluver, *Globalization, Information, and Intercultural Communication*, OKLAHOMA CITY UNIVERSITY (last visited Mar. 3, 2012), http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002006.htm. (Generally describes the process of "informatization" beginning in the 1990s).

27. 381 U.S. 479, 486 (1965).

28. *See id.* (Preserving the integrity of the marital bedroom by striking down a law prohibiting the use of contraceptives); Roe v. Wade, 410 U.S. 113 (1973) (prohibiting government interference with a woman's right to decide whether or not to carry a pregnancy to term prior to viability); Lawrence v. Texas, 539 U.S. 558 (2003).

29. CHRISTINA CORDOVA, THE END OF PRIVACY AS WE KNOW IT?: THE ETHICS OF PRIVACY ON ONLINE SOCIAL NETWORKS 3 (Professor Bob Reich et al., eds,, 2010), *available at* http://www.scribd.com/doc/31183528/The-End-of-Privacy-as-We-Know-It-The-Ethics-of-Privacy-on-Online-Social-Networks.

30. Catharine Smith, *Facebook Users Number Almost 700 Million: Report*, HUFFINGTON POST (Jul. 7, 2011), http://www.huffingtonpost.com/2011/05/31/facebook-users-number-almost-700-million_n_868967.html.

31. CORDOVA, *supra* note 29 at 4.

32. Gary L. Baker, *Privacy Online*, EL ZOCALO (Nov. 12, 2011), http://www.coetail.asia/bakergarry/2011/11/12/adding-to-anothers-digital-footprint/.

33. CORDOVA, *supra* note 29 at 3.

the intimate details of a user's life.[34] Likening this mechanism to B.F. Skinner's famous thought experiment now known as the Skinner Box,[35] Doctrow asserts that "Facebook uses that same mechanism; it lavishes you with more attention from the people you love the more you disclose about your life."[36] Users are incentivized to post details about their lives because doing so might be "that one disclosure that will give you back that jolt of social reinforcement," via "likes" or comments.[37] However, the network "is not there because Facebook thinks that disclosing information is good for you; it's there in service to a business model that cashes in the precious material of our social lives and trades it for pennies."[38]

The business model to which Doctrow refers is selling user information and behavioral data to third party advertisers, which enables the advertisers to deliver more relevant ads to particular users and/or analyze trends of online behavior for product research.[39] This model is not exclusive to online social networks; it is an integral component of a host of online companies' revenue generation.[40] In an era where we expect our email services, social networking memberships, and virtually every other kind of online service to be free, it's easy to forget why they cost nothing in the first place: "A few advertisers pay for content so lots of consumers can get it cheap or free."[41] As Chris Anderson of the Wall Street Journal points out, "[t]he last decade has seen the extension of . . . this model far beyond media, and today it is the revenue engine for all the biggest Web companies, from Facebook and MySpace to Google itself."[42] Indeed, this model "is powering everything from photo sharing to online bingo," and will become even more pervasive as consumers' sense of entitlement to free goods and services begins to manifest itself.[43]

34. TEDxObserver, *Cory Doctrow*, YOUTUBE (Mar. 22 2011), http://www.youtube.com/watch?v=RAGjNe1YhMA&feature=player_embedded.

35. *Skinner Box*, MEDILEXICON.COM, www.medilexicon.com/medicaldictionary.php (last visited Oct. 14, 2012).

36. TEDxObserver, *supra* note 34.

37. *Id*.

38. *Id*.

39. David S. Evans, *The Online Advertising Industry: Economics, Evolution, and Privacy*, UNIVERSITY COLLEGE OF LONDON 3, *available at* http://www.intertic.org/Policy%20Papers/EvansEOAI.pdf.

40. Chris Anderson, *The Economics of Giving It Away*, WALL STREET JOURNAL ONLINE (Jan. 31, 2009), http://online.wsj.com/article/SB123335678420235003.html.

41. *Id*.

42. *Id*.

43. *Id*.

> [C]onsumers are saving their money and playing free online games, listening to free music on Pandora, cancelling basic cable and watching free video on Hulu, and killing their landlines in favor of Skype. It's a consumer's paradise: The Web has become the biggest store in history and everything is 100% off.[44]

It may be a fool's paradise. As we become seduced by an ever-increasing array of free online services, we broadcast an ever-increasing number of details about our personal habits, tastes, and opinions to the entire internet community, and this "disclosure" is "irrevocable:"[45] the loss of "control over information about oneself,"[46] i.e., our privacy.

Despite many users' behavior to the contrary, most of us still value privacy.[47] Few of us would like to accept the words of Sun Microsystems CEO, Scott McNealy, who famously declared in 2001, "[p]rivacy is dead, deal with it,"[48] or casually accept the assertion that a "piece of privacy dies with each and every technological innovation."[49] After all, one "does not give out his home phone number or home address to someone he does not know,"[50] just as one zealously guards his or her banking and social security information. The implications of indelibly broadcasting our personal information to casual observers and third party advertisers in a global forum carry just as much potential for harm.

Preserving these rights in an age when privacy guarantees are rapidly eroding is a challenge. An extreme solution is to simply abandon all use of online services. However, given the integral role online services play in modern life, that option is probably not a desirable one for most people. After all, full abandonment also requires foregoing the substantial benefits of online services, such as convenience, education, and "fight[ing] isolation with [social] networks."[51] More appealing is a middle-ground solution, where one could continue using online services while understanding the implications of that use.

44. *Id*.
45. TEDxObserver, *supra* note 34.
46. DeCew, *supra* note 18.
47. CHRISTINA *supra* note 29, at 3.
48. *Id*.
49. *Id*.
50. *Id*.
51. TEDxObserver, *supra* note 34.

One such solution is the provision of a privacy policy, a statement that informs the user as to what specific information is gathered from them, and whether it is kept confidential, shared with partners, or sold to other firms or enterprises.[52] In theory, a privacy policy is a simple yet effective method of furthering Warren's and Brandeis's vision of enabling an individual to assert control over the dissemination of "information about one's self"[53]; the user is free to give away as much or as little information about himself as he wants in exchange for the use of a service, and is fully informed regarding the implications of his participation. In reality, however, most privacy policies suffer from a number of substantial shortcomings that compromise their efficacy as a means of combating privacy attrition. These shortcomings include a general lack of education among users regarding how their information is commonly used by online services, frequently changing policies, and lack of notice of these changes, as well as the widespread failure of companies to construct these policies in a readable and understandable manner.[54]

III. Factors Compromising the Efficacy of Privacy Policies

A. Lack of Education Regarding How to Assess Online Privacy

Studies reveal that there is "a good deal of confusion as to what online privacy actually means" and confusion regarding what purpose privacy policies actually serve.[55] Chris Hoofnalge, senior staff attorney at the Samuelson Clinic at UC Berkeley's School of Law states that "[c]onsumers fundamentally misunderstand the rules of the marketplace."[56] He bases this conclusion on the findings of a 2007 study "in which up to 75% of consumers think as long as the site has a privacy policy it means that it won't share data with third parties."[57] That is, "[t]hey equate the presence of the policy with substantive privacy rules."[58]

52. *privacy policy*, BUSINESSDICTIONARY.COM, http://www.businessdictionary.com/definition/privacy-policy.html (last visited Feb. 26, 2011).

53. DeCew, *supra* note 18.

54. Rimmer, *supra* note 1.

55. Robert Gorell, *Do Consumers Care about Online Privacy?*, FUTURE NOW (Oct. 30, 2007), http://www.grokdotcom.com/2007/10/30/do-consumers-care-about-online-privacy/ (Feb. 29, 2011).

56. *Id*.

57. *Id*.

58. *Id*.

Another study from the Stanford Persuasive Technology Lab suggests that factors other than a site's privacy policy have a disproportionately large impact on consumers' perceptions about the site's credibility: "[P]eople rarely used . . . rigorous criteria when evaluating credibility (e.g. they almost never referred to a site's privacy policy.)"[59] Instead, "[t]he data showed that the average consumer paid far more attention to the superficial aspects of a site, such as visual cues, than to its content," especially "visual design."[60]

The findings of the two aforementioned studies suggest that the average consumer is not only uninformed about how companies use their information, they are also ignorant about what a privacy policy actually achieves and how to properly assess a site's credibility with respect to privacy treatment. However, the onus of educating customers about privacy implications is on the companies; they have a responsibility to make it abundantly clear how a user's information is collected and for what purposes.

B. Deficient Notice of Changes in Policy

Many organizations reserve the right to unilaterally alter their privacy policies and practices without notifying the user of the change. Companies like Facebook justify doing so on grounds that "privacy norms are in flux" such that "many are now comfortable with sharing the information they perceived as private just ten years ago."[61] Mark Zuckerberg has personally defended this practice, stating that Facebook revises its privacy practices as if they were starting the company anew every time the public changes its approach toward privacy protection: "We decide [what] would be the social norms now and we just [go] for it."[62] While many of these changes have gone without notice from consumers, it has raised red flags with the Electronic Frontier Foundation (EFF), which began a service in 2009 that tracks changes in terms of service agreements "for 44 different services, including Facebook, YouTube, Amazon, Twitter, and eBay."[63] Notwithstanding the EFF's efforts, the ever-changing

59. B.J. Fogg et al., *How Do People Evaluate a Web Site's Credibility?*, STANFORD PERSUASIVE TECHNOLOGY LAB. 6 (Oct. 29, 2002), http://www.consumerwebwatch.org/pdfs/stanfordPTL.pdf.

60. *Id*.

61. CORDOVA, *supra* note 29, at 4.

62. *Id*.

63. Chris Walters, *TOSBack Keeps Track of Changes to Terms of Service Policies Around the Web*, ELECTRONIC FRONTIER FOUNDATION (Jun. 8, 2009), https://www.eff.org/press/mentions/2009/6/8.

nature of privacy policies and lack of adequate notice thereof is a serious impediment to users' comprehension of "what strings are attached" to their reliance on a particular online service.[64]

C. Average Reading Comprehension Level and Actual Policy Readership

Even if a user reads a privacy policy, doing so may seem like a daunting task, especially given the often voluminous number of provisions and terms with which one must familiarize him or herself in a single agreement.[65] And even if one had the time to peruse such a document, doing so may prove to be a prohibitively difficult task in light of the abundance of specific terms pertaining to the service's technology and/or legal terminology.[66]

Even among those of us with legal or technical training, the task may seem Sisyphean in light of the large quantity of these agreements one would have to read to make fully informed policy choices across the myriad and ever-increasing number of electronic services we use every day.[67] The task is even more challenging for someone without a legal education.

Shannon Wheatman, Ph.D., a notice expert with Kinsella Media, LLC, addressed the problem of privacy policy comprehension in a scientific manner.[68] In order to quantify the degree of inaccessibility of a typical company's policy, she compared the reading comprehension level of the average American with the average reading comprehension level required to fully understand an average company's privacy policy.[69] The study entailed an analysis of the privacy policies of ninety-seven of the Fortune 100 companies (three

64. Brady Forrest, *TOSBack: EFF's Much-Needed Terms of Service Tracker*, O'REILLY RADAR (Jun 4, 2009), http://radar.oreilly.com/2009/06/tosback-effs-much-needed-terms.html.

65. Baker, *supra* note 32. ("In this privacy policy readability study it was determined that the language of privacy policies is changing to the detriment of users. Not only language, but the length of the statements, based on the number of words, has also increased.").

66. Dong Ngo, *Keep Tabs of Terms of Service with TOSBack.org*, CNET.COM (Jun. 5, 2009), http://www.cnet.com/8301-17914_1-10258081-89.html. ("It would be even more helpful, however, if the site provided translation of these terms of service into layman's terms, as not everyone has the legal background to really understand what they mean.").

67. Walters, *supra* note 63. ("It's difficult enough to parse a lengthy TOS for web-based service, let alone dozens...").

68. Paul Bond and Chris Cwalina, M*aking Your Privacy Policy Comprehensive and Comprehensible*, CORPORATE COUNSEL (Sep. 1, 2011), http://www.law.com/jsp/cc/PubArticleFriendlyCC.jsp?id=1202512963808.

69. *Id.*

of them did not have privacy policies).[70] The results were harrowing in several respects: First, she discovered the average adult in the United States reads at an eighth-grade level.[71] Second, she found the privacy policies of these ninety seven organizations were, on average, only intelligible to those whose reading comprehension abilities were at least equal to a junior in college.[72]

Statistics regarding actual readership of privacy policies are no less discouraging. A study commissioned by the investment specialist company Skandia showed that "only 7% of adults always read full online terms and conditions when signing up for products and services, with 43% of those who don't always read them saying they are boring or they don't understand."[73] Additionally, "nearly six in ten (58%) adults said they would rather read an instruction manual or their utility or credit card bill than go through online terms and more than one in 10 (12%) would rather read the phone book."[74]

The studies confirm what most of us already suspected: The policies of most major corporations are written in a manner that is well beyond the comprehension of the general public, and as a result, very few of us actually read them.[75]

D. Negative Consequences Arising from Inadequate Privacy Policies

The aforementioned shortcomings of privacy policies present serious dangers for both the user and the online business.[76] In this section, I will present a non-exhaustive list of such hazards.

E. Inaccurate Consumer Expectations

When a company's actual policy information deviates significantly from the expectations of its users, a relatively innocuous outcome for the business is that a customer will become disillusioned or frustrated.[77] This is not uncommon; a study commissioned by Skandia

70. *Id.*
71. *Id.*
72. *Id.*
73. Rimmer, *supra* note 1.
74. *Id.*
75. Bond & Cwalina, *supra* note 68.
76. *Id.* ("This is more than a style problem; it can actually affect perception of your company's attitude toward transparency.").
77. Hetcher, *supra* note 15, at 921. ("Consumers currently have little legal recourse, but they may nevertheless possess a moral response that is, from the website's perspective, functionally equivalent. Morally speaking, customers will disdain disrespectful websites. They will view such websites as less reputable, trustworthy, and worth of continued business relationships.").

revealed that "over a fifth (21%) of the people surveyed say they have suffered as a result" of misunderstanding terms and conditions.[78]

The worst possible outcome is that the user will claim to have suffered an injury from use of the service and that the injury was the result of fraudulent or deceptive practices.[79] Regardless of the merits of such claims, the company will suffer some expenditure of legal resources as a result.[80] Its public relations will also suffer.[81]

For consumers, the consequences of inaccurate expectations are equally undesirable. After private information has been disclosed to a third party or used in a manner incommensurate with the consumer's wishes, the only remedies available are ex post facto.[82] Whether the injury consists merely of a discomfort resulting from a sense of one's privacy having been degraded, or whether more material consequences occurred such as job loss or intrusive advertising, the horse is out of the barn once the injury has taken place.[83] The problem is compounded by the lack of practical legal recourse available, since breach of contract claims generally will not succeed when the argument is predicated on a lack of understanding of the terms to which one agreed.[84]

F. Lack of a Real Choice

The problems arising from an incomprehensible or otherwise unclear privacy policy are compounded when the user is faced with the task of comparing such policies. Trying to discern the meaning of two or more privacy policies is enough to persuade the average person to decide which program to use on a basis other than

78. Rimmer, *supra* note 1.

79. Hetcher, *supra* note 15, at 921. ("More aggressive customers may feel that disrespectful websites deserve to be sanctioned or otherwise reciprocally ill-treated.") *See also* James Temple, *Local Class Action Complaint Filed over Google Buzz*, THE TECH CHRONICLES (Feb. 17, 2012), http://blog.sfgate.com/techchron/2010/02/17/local-class-action-complaint-filed-over-google-buzz/.

80. *Google to Pay 8.5 Million Dollars to Settle Buzz Case*, AFP (Sep. 3, 2010), http://www.google.com/hostednews/afp/article/ALeqM5g3yF0MKx3iORpW3tEYx7UuIhSoVw. (The aforementioned dispute was ultimately settled for $8.5 million and was made public).

81. *Id.*

82. As mentioned in the introduction, relevant contract modes of recourse, such as asserting fraud and duress, can only provide relief for a harm already suffered.

83. Temple, *supra* note 79. ("Among other things, critics raised concerns that this [breach] could – or possibly did – aid stalkers, jeopardize journalist sources, or hint at affairs.")

84. *Ray,* 201 Md. at 125.

conformance with privacy expectations.[85] This may lead to some of the problems mentioned in the previous section, such as disdain for the company or sanction seeking.[86]

The lack of real choice among consumers may also be deleterious to businesses, because their ability to distinguish themselves on the basis of strong privacy protections is compromised. A study performed at Carnegie Melon University showed that when clear privacy "information is made available, consumers tend to purchase from online retailers who better protect their privacy."[87] Furthermore, "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites," suggesting that "businesses may be able to leverage privacy protections as a selling point."[88] However, this element of competition vanishes if policies are so long or so complex that customers aren't able to effectively contrast the company's policy with that of other websites.[89] Another survey found that "65% of users decided not to use a website because they were unsure of how their personal information would be used."[90]

G. Increased Costs to Consumers

Consumers who actually perform their due diligence in reviewing the complex privacy policies of websites will have to invest an enormous amount of time to engage in even the most routine online activities. For example, a user would have to read the privacy policies of Orkut, Facebook, MySpace, and Friendster before deciding which social networking website to use. It would take a sophisticated lawyer several days to do this, much less an average user without any legal training whatsoever.[91] Furthermore, privacy policies often change

85. JANICE TSAI ET AL., THE EFFECT OF ONLINE PRIVACY INFORMATION ON PURCHASING BEHAVIOR: AN EXPERIMENTAL STUDY 24 (Carnegie Mellon University Workshop on the Economics of Information Security, 6th ed. 2007), *available at* http://weis2007.econinfosec.org/papers/57.pdf. (Participants in the study who did not view a prominently displayed and/or accessible privacy policy "generally made purchases from the lowest priced vendor" instead of that which protected privacy the most.).

86. Hetcher, *supra* note 15, at 921.

87. Tsai, *supra* note 85, at 1.

88. *Id.*

89. *Id.* at 24.

90. CORDOVA, *supra* note 29, at 19.

91. Ngo, *supra* note 66. ("It would be even more helpful, however, if the site provided translation of these terms of service into layman's terms, as not everyone has the legal background to really understand what they mean.").

with new developments in the company's technology.[92] Such changes compound the problem of time investment.

IV. Integration of Best Practices into a Statutory Regime

In light of the tangible costs inadequate privacy information imposes on businesses and consumers alike, best practices have emerged that seek to fix the problems. I argue that some of these practices are ill-suited as the subject of government oversight, while others should be integrated into a regulatory framework and stringently enforced. At the end of this section, I will describe how such a law should be implemented, how such a law would differ from existing FTC guidelines, the benefits of such a regulation, and address potential criticisms.

A. Best Practice: Policy Text Formatting

Bearing out intuition, a 2006 study of financial privacy notices found that "subheadings and standard formats dramatically improved readability."[93] Bart Lazar, a partner with Seyfarth Shaw, also advocates an easy-to-read, clear format, complimenting the American Express privacy policy for doing so: "It is navigable, and it breaks things up into nice chunks."[94]

Though clear formatting may be regarded as a best practice, it would be impractical for a regulatory agency to micromanage the paragraph-by-paragraph formatting of every privacy policy. However, such an agency could mandate certain font sizes[95] or prohibit a "wall-of-text"[96] approach by letting courts infer that font below a certain size or a certain degree of text density is probative of a lack of adequate transparency.

92. *Id*. (*See* AT&T anecdote).

93. ALEECIA M. MCDONALD ET AL., A COMPARATIVE STUDY OF ONLINE PRIVACY POLICIES AND FORMATS 1 (2006), *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00036.pdf.

94. Erika Morphy, *Privacy Policies: The Good, the Bad, and the Witty*, E-COMMERCE TIMES (Dec. 23, 2008), http://www.ecommercetimes.com/rsstory/65618.html.

95. The Fair Credit Reporting Act, 5 U.S.C. §§ 1681-1681u, *available at* http://www.ftc.gov/ogc/stat3.shtm.

96. Aza Raskin, *Making Privacy Policies Not Suck*, AZARASKIN.IN http://www.azarask.in/blog/post/making-privacy-policies-not-suck/ (last visited Feb. 16, 2012).

B. Best Practice: Concision—Applying Occam's Razor to Privacy Policies

As Paul Bond and Chris Cwalina of Reed Smith LLP have observed, some information in a privacy policy will be obvious to any user who is even vaguely familiar with the Internet.[97] For example, in their article regarding how to make a business's privacy policy comprehensible, Bond and Cwalina point out that Google used to explain that they "may present links in a format that enables us to keep track of whether these links have been followed."[98] Google's privacy policy now excludes this "obvious information."[99] Google also shortened its policy by placing definitions of widely-understood terms (such as "cookie") in a less conspicuous location within the document so as to enable the already-familiar reader to delve immediately into the substance of the policy.[100] This makes for a more efficient, less tedious reading experience and fosters improved comprehension.[101]

Given that the average attention span of an adult reading online content is an astoundingly low nine seconds,[102] brevity is an important element of comprehension. However, it is also an inherently subjective quality: What may seem like a superfluous definition to one person may seem useful to another. Furthermore, given the rapidly-changing nature of technology, it is difficult to assess what technological terms have entered the popular lexicon and which are still unfamiliar to most.[103] For these reasons, the best practice of relegating "well known" terms to a less conspicuous section of the policy is not suitable for legal enforcement.

C. Best Practice: Avoiding Highly Specific, Technical Terms in Favor of Plain Language

Bond and Cwalina also suggest that privacy policies "should not read like a technical manual."[104] Terms that are technologically complex or not used in common parlance should either not be used or used infrequently. Provision of clear definitions in the opening section may be helpful, but the use of such terms should nonetheless

97. Bond & Cwalina, *supra* note 68.
98. *Id.*
99. *Id.*
100. *Id.*
101. *Id.*
102. *Turning Into Digital Goldfish*, BBC NEWS (Feb. 22, 2002), http://news.bbc.co.uk/2/hi/1834682.stm.
103. Bond & Cwalina, *supra* note 68.
104. *Id.*

be limited to places where the term is essential to convey a particular meaning. Bond and Cwalina rightfully argue that terms such as "query string," "web beacon," "trace route," and "anonymization" will not assist actual understanding and will often "mean nothing to your audience."[105] Bond and Cwalina also discuss how many of these technical details will change very quickly, which could render a privacy policy outdated on a more frequent basis.[106] The takeaway is that policies should dedicate less content to describing the excruciatingly technical intricacies of how data is collected and instead strive to describe in colloquial terminology what kinds of service use will lead to data collection and how that mechanism works.[107] Again, however, any attempt to identify what constitutes a highly specific, technical term for legal purposes would become a subjective mess, akin to Justice Stewart's struggle to categorize a phenomenon (pornography) that lacks clearly defined parameters ("I know it when I see it").[108]

D. Best Practice: Transparency Regarding Use of Consumer Information

In order for a privacy policy to be a useful guide to consumer behavior, it should clearly describe how a user's information will be employed by the service provider. Bond and Cwalina regard the description of privacy issues in "if this, then that" terms as a best practice.[109] Bond and Cwalina enumerate several more specific examples of how these "if/then" statements should appear in a policy. For example, a policy should read "[I]f you use the Web site, then this is what we will collect . . ."; "If you want to create a registered account, this is what we need . . ."; "If you give us this piece of information, we will share it with so-and-so."[110] This will engender a solid understanding of how one's behavior within the service or website will affect one's privacy exposure.[111]

Mandating the use of if-then statements is feasible. It would simplify the language of policies across the board, create predictability, and would clearly delineate how information and behavioral data is used. An if-then statement should be required for each facet of a company's service. For example, a statement could

105. *Id.*
106. *Id.*
107. *Id.* ("As much as possible, describe privacy issues in 'if this, then that' terms.").
108. Jacobellis v. State of Ohio, 378 U.S. 184, 197 (1964).
109. Bond & Cwalina, *supra* note 68.
110. *Id.*
111. *Id.*

read, "If you use X application, the following data will be recorded and we will use it for Y purpose."

E. Best Practice: Clear Placement

While the content of the policy itself is an extremely important consideration, so is the placement of the policy within the site or the time of presentation during the sign-up or registration process.[112]

Bond and Cwalina demonstrate the various complications that can arise with respect to the physical placement of the policy within the site, such as (a) where the consumer would find the policy on the actual interface, and (b) if a link to the policy exists, whether the link is salient enough to be obvious to most users (i.e. in a prominent position on the site or whether it is in a reasonably-sized font).[113]

Another issue of concern with respect to placement is the timing when the policy is displayed. Bond and Cwalina note that "[p]rivacy groups have been especially critical of requests for information that only pop up in the middle of a transaction."[114] If a consumer has already invested a substantial amount of time and effort into signing up for a particular service, they may "feel compelled to provide the information rather than abandon a purchase or subscription that is almost complete."[115] Thus, a notice placed at the very beginning of the signup or registration process is probative of an honest, good-faith effort to disclose all potential privacy issues prior to a consumer's investment of time and effort.

Mandating a privacy policy to be displayed in lieu of a homepage upon log on, or in an otherwise intrusive manner with each log on attempt would be unreasonable. It would only serve to create confusion and annoyance. What is feasible, however, is the mandatory inclusion of a noticeable link to one's privacy policy. Such a requirement could follow similar guidelines to those which govern privacy policies under the Gramm-Leach-Bliley Act (GLBA), a statute which seeks to provide "limited privacy protections against the sale of . . . private financial information" by modernizing financial services.[116] Under the GLBA, financial service providers are compelled to provide links to privacy policies on their websites that

112. *Id.*
113. *Id.*
114. *Id.*
115. *Id.*
116. *The Gramm-Leach-Bliely Act*, ELECTRONIC PRIVACY INFORMATION CENTER, http://epic.org/privacy/glba/ (last visisted Feb. 3, 2012).

are "designed to call attention," instructing institutions to "design [their] notice to call attention to the nature and significance of the information in it" by using "text or visual cues to encourage scrolling down the page to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice."[117] Furthermore, it requires the site to either "place the notice on a screen that consumers frequently access, such as a page on which transactions are conducted," or to "[p]lace a link" in a conspicuous location that "is labeled appropriately to convey the importance, nature, and relevance of the notice."[118]

While the FTC guidelines propose a similar construction, the GLBA provides support for this note's position that it is feasible to implement these suggestions as mandatory regulations, not merely as recommendations.

F. Best Practice: Notice of Changes in Technology or Policy

Similar to the proposed requirements discussed in the previous section, changes in policy should be made salient and apparent to the average user.

Bond and Cwalina acknowledge that companies frequently change the technology they use and these changes often affect the company's privacy guarantees.[119] Thus, privacy policies should be prepared for "this likelihood of change, even though the specific changes are not foreseeable."[120] That is, the important point is not that companies need to predict the exact nature of the anticipated changes, but they must "[m]ake clear to consumers how [the company] will communicate changes to [their] privacy policy and what will constitute their content."[121]

This best practice is reflected by the manner in which Google's recent change of policy was communicated to users. On virtually all of its pages and applications, a popup window with bold font read, "We're changing our privacy policy and terms. This stuff matters.

117. *Final Rule: Privacy of Consumer Financial Information*, U.S. SECURITIES AND EXCHANGE COMMISSION (Nov. 13, 2000), www.sec.gov/rules/final/34-42974.htm.

118. *Id*.

119. Bond & Cwalina, *supra* note 68.

120. *Id.*

121. *Id.*

Learn more."[122] The notice was often highlighted and attracted attention. Such a practice would be feasible to mandate in a manner commensurate with the requirements set in the Gramm-Leach-Bliley Act discussed in the prior section.

V. Implementing Best Practices into a Regulatory Scheme

Like the Gramm-Leach-Bliley Act, this note's proposal does not seek to "prescribe any specific format or standardized wording for these notices."[123] Rather, the focus should be on clarity in presentation and language. Clear formatting of privacy policy text should mimic the aforementioned requirements of the Gramm-Leach-Bliley Act, such as providing "wide margins and ample line spacing" as well as "a typeface and type size that are easy to read."[124] Transparency regarding use of user information will be achieved by requiring the use of if/then statements which stipulate in plain language the exact types of information that will be collected and how that information will be subsequently disseminated. Obvious placement of the policy should also be enforced in a manner emulating the requirements of the GLBA, planting it in locations that notify new users and those about to undertake transactions. Distractions should be limited and efforts should be made to make the notice as salient as possible. Failing to do so should militate in favor of a finding of infraction. Finally, notice of changes to the policy should be equally salient. This is a particularly important requirement given the rapidly-evolving nature of the tech industry.

While best practices such as concision and avoidance of highly-specific, technical terms are too subjective to integrate into an umbrella mandate, they could be used as mitigating or aggravating factors to be considered by a finder of fact in a legal proceeding.

Also like the GLBA, the pertinent enforcement body could provide examples and/or sample clauses that organizations could employ to satisfy the new rule.[125]

122. GOOGLE, *Policies & Principles: One Policy, One Google Experience* (Mar. 1, 2012), https://www.google.com/intl/en-GB/policies/#utm_source=googlehp&utm_medium=hpp&utm_campaign=en_all-hpp_pp.

123. Final Model Privacy Form under the Gramm-Leach-Bliley Act, DEPARTMENT OF THE TREASURY, ET AL., 8 http://www.ftc.gov/privacy/privacyinitiatives/PrivacyModelForm_Rule.pdf (last visited Feb. 17, 2012).

124. *Final Rule: Privacy of Consumer Financial Information*, *supra* note 117.

125. *Gramm-Leach-Bliley*, *supra* note 123, at 8.

VI. How this Note's Proposal Differs from Existing FTC Practices

As mentioned above, there are currently no federal statutes that establish a comprehensive regulatory approach to all matters involving privacy policies or a uniform set of specific requirements.[126] However, the Federal Trade Commission (FTC), whose raison d'etre is "to protect consumers against unfair, deceptive, or fraudulent practices in the marketplace,"[127] is the current governing body that enforces terms of privacy policies.[128] Under Section 5 of the FTC Act, the FTC may bring an action for unfair or deceptive practices, but only if a specific provision of the policy is violated.[129]

In 2000, the FTC issued the "Fair Information Practice Principles," which contained a series of recommendations to the web site industry "to follow the core principles of notice, choice, access, and security."[130] In 2007, the FTC promulgated a more detailed set of recommendations "with additional emphasis on transparency in data collection, limited data retention, and affirmative express consent to changes in privacy policies or collection of more sensitive data."[131]

However, these guidelines remain exactly that—guidelines—not statutory mandates. In contrast, my proposal seeks to make the principles embodied in these guidelines legally binding. Furthermore, the 2007 guidelines suggest that a substantive, irreducible minimum of privacy protections should be granted by companies. My proposal does not seek to determine the amount or kind of privacy that should be preserved; reflecting free market principles, companies should be able to do as they please with user data as long as the consent of the user has been obtained in advance.

In addition to the guidelines, the FTC has instituted a number of legal actions where online services have employed user information in a manner that violates the Act's prohibition against unfair trade practices.[132] However, this litigation has either taken the form of (a) suits alleging that a company has failed to provide a minimum

126. MCDONALD, *supra* note 93.

127. *About the Bureau of Consumer Protection*, FEDERAL TRADE COMMISSION, http://www.ftc.gov/bcp/about.shtm (last visited Feb. 21, 2012).

128. *Id*.

129. *Id*.

130. Robert Todd Graham Collins, *The Privacy Implications of Deep Packet Inspection Technology: Why the Next Wave in Online Advertising Shouldn't Rock the Self-Regulatory Boat*, 44 GA. L. REV. 545, 571-72 (2010).

131. *Id*.

132. *Id*.

amount of privacy protection or (b) suits alleging failure to comply with one's own privacy practices.[133]

With respect to the former category, I do not propose any minimum amount of privacy protection. As for the latter, such litigation is a disincentive to provide a privacy policy in the first place, since there are no generally applicable "laws that actually require businesses to offer their customers a privacy notice," and only if they do will the FTC "see that it's honored."[134] Under my vision of privacy enforcement, suits would be instituted on grounds of insufficient notice/lack of consent and would mandate the use of a privacy policy.

VII. Benefits of Privacy Policy Regulation

The following benefits of a clearer privacy policy presentation will be actualized if companies are threatened with legal sanction from a generally applicable law.

A. Increased Accountability

A clearer explanation of what forms of data will be collected and for what purpose they will be used will improve the degree of accountability on the company side. Businesses will be unable to hide behind technical and complex terminology or excessive length to obscure the issues. Furthermore, when the language is more understandable, consumers will understand its provisions and will have a better standing to bring a claim for breach of contract if one of its provisions was indeed violated.

B. Cost and Time Savings

Clarity in privacy policies will save both time and money for the business and the consumer. For the business, the initial expenditure of time required to make a clear, comprehensible privacy policy will likely be more than the amount of time required for a lawyer to execute a "wholesale data dump" of information that includes all the necessary disclosures but is incomprehensible or not useful to the consumer.[135] It will require thoughtful tailoring and editing to ensure all the requisite information is presented while maintaining clarity. However, the extra time invested in the construction stage will be compensated by the reduction of hours required to explain to inquiring customers what specific provisions of their policies mean.

133. *Id*.
134. Morphy, *supra* note 94.
135. Bond & Cwalina, *supra* note 68.

For the consumer, a substantial amount of time will be saved in the process of reading and comparing various sites' policies. For those who currently refrain from reading privacy policies but will begin doing so if they became more comprehensible, the additional investment of time will be moderate but the improvements of understanding one's privacy exposure will be drastic.

C. Transparency

The U.S. Department of Commerce has identified "transparency" as a top priority in the promotion of privacy.[136] The department notes that "[w]hen information is presented in a way that is highly complex or detailed, it may not be transparent."[137] Policies drafted in plain language and otherwise clearly presented will greatly improve a company's transparency. Customers will view the business as more committed to being open and honest with its customers regarding its use of their personal information, which not only puts the consumer at ease but fosters benefits for the organization as well.

VIII. Addressing Potential Criticisms

A self-regulatory approach to privacy protection is largely consistent with America's hands-off approach and avoidance of micromanagement of businesses, a principle embodied by overruling of the *Lochner v. New York*[138] line of decisions that permitted government interference with the right to engage freely in contract.[139] Some potential arguments for the benefits of self-regulation include (a) a broad, sweeping privacy policy law might not provide the flexibility needed for different industries and different types of businesses; (b) such a law may inhibit the growth of electronic commerce; and (c) broad legislation might be too inflexible and fail to appease a diverse array of users with different tolerances for privacy.

With respect to the flexibility argument, it is certainly true that the industry of online business is diverse and always changing. However, my proposal does not seek to provide users with an irreducible minimum of privacy protection—it merely requests that companies inform consumers of their intentions regarding use of information and obtain informed consent prior to the transaction. The proposal is not industry-specific and would apply equally to

136. *Id.*
137. *Id.*
138. 198 U.S. 45 (1905).
139. *See* Ferguson v. Skrupa, 372 U.S. 726, 729 (1963).

online social networking sites, e-commerce sites, and email servers alike.

As for the argument that such a law would inhibit the growth of e-commerce, I have shown that it would actually open up new avenues for competition on the basis of privacy protection. Consumers, as mentioned previously, have been shown to be willing to pay a premium for sites that offer better privacy protection than its competitors. The only sector of the online service industry that would be harmed by such a general regulation would be those who benefit from exploiting users' ignorance about the ultimate fate of their behavioral information.

Finally, I disagree that broad legislation might be too inflexible and fail to appease a diverse array of users with different tolerances for privacy on the same grounds as those mentioned in addressing the first argument: namely, my proposal does not seek to inform the substance of a company's policy, it merely requires a company to fully inform the user about how his or her information will be used. Those who have a high risk tolerance with respect to dissemination of their information will continue to use sites that liberally distribute one's information; those who are more concerned about their privacy will refrain from doing so on a more informed basis.

IX. Conclusion

To summarize, confusion among users regarding the implications of their online behavior is endemic. This confusion is caused by a lack of education regarding how user data is employed by companies, deficient awareness of changes in privacy practices, and a mismatch between the average reader comprehension levels and the complexity of terms of service. The potential hazards of these problems are grave: They may create inaccurate consumer expectations, rob the user of a real choice between competing services, and increase costs to both consumers and businesses. Though best practices have emerged and certain organizations have risen to address the ethical and legal concerns of users, companies that faithfully employ these practices remain the exception, not the rule.

Given the shortcomings of the existing self-regulatory model of user privacy protection, a more effective supervisory framework is needed. I suggest privacy policies remain the most viable device for privacy protection, but not as they exist today: I envision the integration of existing best practices into a regulatory scheme coupled with stringent enforcement as a practical solution that would balance business interests with better user protection.

At the end of the day, my proposal is merely a starting point. A single article cannot hope to address or resolve the totality of concerns surrounding privacy protection, which are myriad, complex, and always evolving. However, what remains as stable and clear as ever is the importance of addressing the deterioration of privacy protection in the 21st century. The ever-increasing prevalence of free online services that collect behavioral data to generate profits, combined with users' impetuous attitude and ignorant approach to the use of these services, evokes a harrowing specter of a dystopian future where our secrets, relationships, and personalities are subject to unmitigated scrutiny and sold for a pittance. The nature of the device we employ to prevent this scenario is uncertain, but the necessity of engineering one is not.