INVASION CONTRACTS: THE PRIVACY IMPLICATIONS OF TERMS OF USE AGREEMENTS IN THE ONLINE SOCIAL MEDIA SETTING

Jared S. Livingston

TABLE OF CONTENTS

I. ABSTRACT

Online privacy is a concern of ever-growing importance. One fact that perhaps contributes to the concern is that there is nothing in website privacy policies that can adequately protect users. This note will take a close look at what, if anything, is failing that can explain the void of privacy policy terms that can protect users' information. It will do so by looking at both legal and non-legal enforcement mechanisms for electronic contracting in general to describe the enforcement framework, and then apply that framework to privacy policies specifically to identify any failures. This note eventually finds that certain conditions must hold in the market (e.g., competition and a value on reputation) to allow non-legal sanctions and enforcement to keep parties from breach or opportunism leading to exploitation of private individuals. This note further finds that in the market for social networking, these conditions fail, and create opportunities for exploitation of consumers' private information.

II. INTRODUCTION

A law student turns on her computer to check her email. She accesses the online browser-based email server. She peruses the Internet looking for information on case law for the next day's reading. She might also use Google to search for legal job openings in her area. Intermittently, she may tell her friends what cool things she has been doing. And she does so by updating her Facebook status, or by sending a Tweet to inform her followers of the day's activities.[1] And she does it all for free.

[1] "For many people, Facebook is the first stop in any Web surfing session." Mark Sullivan, *How Will Facebook Make Money?*, PCWORLD.COM (June 14, 2010, 10:00 PM), http://www.pcworld.com/article/198815/how_will_facebook_make_money.html?tk=hp_new. *See* Andy Kazeniac, *Social Networks: Facebook*

Or so she thinks.

The price she has paid, however, is her privacy.[2] This user, like all other search engine and social networking users, has actually paid for these convenient services with the private information that she provided the service providers by, among other things, posting personal information on their "private" profile. Search engines and social networking services mine the information that users "give" in exchange for services, and then sell it to external developers or marketers.[3] After being sent to private third parties, users' own private information is "held far away on remote network servers."[4] At that point, even if the user abandons use of the search engine or social network, the information that had been provided is not only no longer in the user's control, but is also beyond the website's control as well.[5] All this because the user initially agreed, by either checking an "I [A]gree" box or perhaps just by being on the site, to the sellers terms of privacy and use.[6]

Takes over Top Spot, Twitter Climbs, COMPETE PULSE (Feb. 9, 2009, 2:01 PM), http://blog.compete.com/2009/02/09/facebook-myspace-twitter-social-network/ (noting that Facebook has become the most popular social networking site, while Twitter has also become one of the hottest social networking sites).

[2] *See* John Henry Clippinger, *Facebook Is Betting Against Its Users*, HUFFINGTON POST (June 3, 2010, 12:00 PM), http://www.huffingtonpost.com/john-henry-clippinger/facebook-is-betting-again_b_599231.html. Clippinger explains the "price" of Facebook, as the relinquishing of one's personal information in exchange for Facebook's tools. *Id.* *See also* Sullivan, *supra* note 1 (explaining that, to make money, Facebook collects personal data from its users that is valuable to marketers and advertisers).

[3] *See* Sullivan, *supra* note 1(explaining that Facebook collects "personally identifiable information" from its users, which it may be planning to sell or license to Web marketers).

[4] Matthew A. Goldberg, Comment, *The Googling of Online Privacy: Gmail, Search-Engine Histories and the New Frontier of Protecting Private Information on the Web*, 9 LEWIS & CLARK L. REV. 249, 260 (2005).

[5] Robert Terenzi, Jr., Note, *Friending Privacy: Toward Self-Regulation of Second Generation Social Networks*, 20 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1049, 1068–69 (2010); N.V., *Fleeing Facebook*, ECONOMIST (June 3, 2010, 9:50 PM), http://www.economist.com/blogs/babbage/2010/06/techview_social_network_redux (discussing users' inability to effectively restrict Facebook from profiting from their personal information).

[6] The degree of action required on the part of the user in order to "accept" the terms separates "clickwrap" agreements from "browsewrap" agreements. While clickwrap agreements are typically formed when a user must check, or "click" a box labeled "I agree" or "I have read and understood the terms" before entering or using a site, "browsewrap" agreements are formed by simply using, or "browsing," the site. *See* Sarah E. Galbraith, *Second Life Strife: A Proposal for Resolution of In-World Fashion Disputes*, 2008 B.C. INTELL. PROP. & TECH. F. 90803, 19 (2009); Saami Zain, *Quanta Leap or Much Ado About Nothing?: An*

This is more than users are bargaining for. That is, if there is any bargain at all. If privacy problems are this prevalent, persistent and unwanted, why can the governing privacy policies not include terms that keep firms out of its users' private information? If these problems are stemming from the electronically agreed upon privacy policies, this result would be especially surprising because writers have applauded the fact that electronic contracts have not caused much legal uproar.[7] If electronic privacy policies are permitting such frowned-upon behavior, there must be something that is failing.

This note will take a close look at what, if anything, is failing that can explain the void of privacy policy terms that can protect users' information. It will do so by looking at both legal and non-legal enforcement mechanisms for electronic contracting in general to describe the enforcement framework, and then apply that framework to privacy policies specifically to identify any failures.

But before this note explains how contract law may be able to enforce privacy, it will explain a brief history of privacy law, developments in privacy invasion and proposals in curing those invasive developments. With that in mind, it will become clearer how contract enforcement plays a role in privacy protection.

A. A History of Privacy and the Current Problem

Though the right to privacy has only recently become a more widespread public concern, the right's roots reach back to this nation's founding.[8] From even colonial times, the law protected against unwanted invasion of private information,[9] with a particular interest in protection against unwanted government intrusion.[10] This concern eventually manifested itself by the

Analysis on the Effect of Quanta vs. LG Electronics, 20 ALB. L.J SCI. & TECH. 67, 110 n.199 (2010); Robert L. Oakley, *Fairness in Electronic Contracting: Minimum Standards for Non-Negotiated Contracts*, 42 HOUS. L. REV. 1041, 1049–52 (2005) (discussing the history and distinctions between browsewrap and clickwrap agreements).

[7] *See, e.g.*, Nathan J. Davis, Note, *Presumed Assent: The Judicial Acceptance of Clickwrap*, 22 BERKELEY TECH. L.J. 577, 589–90 (2007) (noting that "very few of the most onerous [contract] terms have resulted in litigation" and claiming that over the past few years, only seven, or less than ten percent of all such disputes, were over controversial terms).

[8] Terenzi, *supra* note 5, at 1057 & n.26 ("Information privacy law is relatively new, although its roots reach far back.").

[9] *Id.* at 1057–58.

[10] *Id.* at 1057–58 (citing Daniel J. Solove, *The Origins and Growth of*

Framers' inclusion of these rights in the Bill of Rights—specifically in the Third, Fourth and Fifth Amendments.[11] In the more modern era, the Supreme Court has reaffirmed the Constitutional right to privacy,[12] at least with respect to protection from government intrusion.[13]

While courts have resisted using the Constitution to blanket privacy invasion by private actors, legislation has stepped up to try to supplement Constitutional protection for privacy in a variety of settings. Statutory law has carved out limited protections for private information, including protection of financial information,[14] stored electronic communication,[15] and even specifically email.[16]

Much of this legislation, however, has proved to be ineffective and not useful in enforcing privacy rights in the modern internet-frenzied era.[17] In fact, if the Internet has proved anything, it is that it can adapt much more quickly than legislation can pass.[18] Previously-passed legislation could not have anticipated the developments that would occur because of the internet, and are thus ill-equipped to handle methods that developers have come up with that invade internet users' privacy. And while aggrieved

Information Privacy Law, 828 P.L.I./PAT. 23, 27 (2005)).

[11] Terenzi, *supra* note 5, at 1058–59.

[12] *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 485–86 (1965) (holding that a state statute prohibiting contraceptive use violated a constitutional right to marital privacy); Lawrence v. Texas, 539 U.S. 558, 562, 578, 580 (2003) (holding the state statute criminalizing same-sex sodomy unconstitutional on the basis that individuals are "entitled to respect for their private lives" without governmental intervention).

[13] Andrew Hotaling, Comment, *Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting*, 16 COMMLAW CONSPECTUS 529, 542–43 (2008) ("[T]he [Supreme] Court has resisted all attempts to create a constitutional right to privacy enforceable against private actors.").

[14] *See id.* at 544–45 (discussing the protections offered by the Right to Financial Privacy Act of 1978, Bank Secrecy Act of 1970, Fair Credit Reporting Act of 1970, and the Gramm-Leach-Bliley Act).

[15] *See* Goldberg, *supra* note 4, at 260–61 (discussing the ability of the Stored Communications Act to protect against invasions of privacy).

[16] *See id.* at 257–58 (discussing California's "Gmail Bill" of 2004).

[17] *See id.* at 262–63, 267–69, 272 (discussing the Stored Communications Act's ineptness regarding protecting against modern invasions of privacy); *see also* Hotaling, *supra* note 13, at 548–49 (stating that "behavioral targeting" "(BT) technology invades . . . privacy while escaping liability under federal data privacy statutes").

[18] *See* Clippinger, *supra* note 2 (stating that the combined efforts of the FTC, the White House, the FCC and DOD are not moving as fast as "technology, the market and the money").

users seeking redress are waiting for legislation to pass, they likely will not have any other sources of protection, as common law remedies have also been able to offer little help in the privacy battle.[19]

The fact is that the law has just not been equipped to deal with the latest information mining tools. What began with eavesdropping and wire-tapping has now grown into a covert system by which any user-input information is tracked to round out a picture of an individual's tastes, preferences, and, to some extent, their identity.[20] This system, called "behavioral targeting," is becoming a more and more widespread phenomenon on today's internet.[21] The result of this virtually invisible monitoring[22] is that information-collectors are able to sell the surveillance information to external third parties—most likely marketers and advertisers—who highly value the detailed and personal information.[23]

As an example, Facebook data can be particularly valuable:

To marketers, the Facebook data is potentially more valuable than the data collected by other massively popular sites, like Google. That's because Facebook collects a rich set of personally identifiable information (PII) from its user profiles. The data contains not only the user's demographic data, but also data about their online and offline likes and dislikes—and those of their friends. The personal and social detail of Facebook's data could give marketers unprecedented power to find new customers.[24]

The inadequacy with which legislation has prevented invasion concerns internet users. According to a recent poll by the Marist Institute for Public Opinion, "[h]alf of all U.S. residents who have a profile on a social networking site are concerned about their

[19] *See* Hotaling, *supra* note 13, at 549–51 (discussing how and why behavioral tracking may fly under the radar of the common law).

[20] For an explanation of a marketing company's perspective on the ability of Facebook to gather data about a user's tastes and preferences, and even a user's friend's tastes and preferences, see Sullivan, *supra* note 1. The result is the creation of a "'social graph' of preferences" with which companies can target advertising. *Id.*

[21] *See* Hotaling, *supra* note 13, at 536–38, 548–49 ("[Behavioral targeting] offers companies the highest rate of return on investment for dollars spent on e-advertising . . . ."). By some estimates, almost 35% of internet sites employ some variation of behavioral tracking. *Id.* at 548–49.

[22] *Id.* at 548.

[23] *See* Sullivan, *supra* note 1.

[24] *Id.*

privacy."[25] Another poll indicates that a majority of consumers are concerned with having their online activity tracked.[26] The vast majority of people, according to this poll, believe that it is inherently "'unfair' when Internet firms relax their privacy policies after having collected personal information from users."[27]

Suffice it to say that the developments taking place over the internet have taken privacy from bad to worse; from being merely "a fractured and incomplete right"[28] to verging on the brink of erasure of privacy and anonymity altogether.[29]

B. Proposed Solutions to Privacy Invasions

Recognizing both privacy problems and public demand for protection, writers and lawmakers have begun to explore possible solutions to the recently-developed invasions.[30] While proposals may not have looked directly at the possibility of enforcement through contract law, they have explored legislative, judicial, and administrative solutions. This note will briefly discuss generally some of these proposals and their respective merits.

Scholars have discussed judicial intervention, for example, as a means for more immediate resolution by consistently supplying applications of current statutes that favor users and consumers.[31] But the deficiencies in the legal status quo are part of the problem, and trying to effect change using case-by-case analysis

---

[25] Mathew Ingram, *Half of Those with Social Networking Profiles are Worried About Privacy*, GIGAOM (July 14, 2010, 5:15 PM), http://gigaom.com/2010/07/14/half-of-those-with-social-networking-profiles-are-worried-about-privacy/.

[26] Juliana Gruenwald, *Poll Finds Public Concern Over Online Privacy*, TECH DAILY DOSE (June 8, 2010, 3:01 PM), http://techdailydose.nationaljournal.com/2010/06/poll-finds-public-concern-over.php.

[27] *Id.*

[28] Terenzi, *supra* note 5, at 1094–95 (citing Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 879 (2003)).

[29] *See* Terenzi, *supra* note 5, at 1095–97, 1105 ("Over the past several years, as social networking has taken a more central role in people's lives, courts and legislatures have been attempting to regulate and remedy the privacy concerns and issues raised by the widespread use of networks such as Facebook and Twitter . . . .").

[30] *See* Gruenwald, *supra* note 26 (reporting that draft privacy legislation is in consideration by Congress); Reidenberg, *supra* note 28, at 877–78, 885, 887–90, 897–98 ("The real search behind the efforts to remedy privacy violations is a search to create new legal rights.").

[31] *See, e.g.*, Goldberg, *supra* note 4, at 249, 260–61, 266 (stating that federal statutes "offer[ ] privacy protection to Internet users who may be unprotected by the Fourth Amendment").

may result in more ambiguity and confusion than certainty and clarity.[32]

Others have suggested complex self-governance mechanisms that would eliminate the need for government intervention and could thus hypothetically create a solution more finely-tailored to the industry problems.[33] Yet, other writers have been skeptical of such an approach,[34] and as this note will further develop, firms in this particular market for behaviorally-tracked information have few incentives for self-regulation and enforcement.[35]

Still others have suggested that legislative action may be an effective solution, whether proposing modification of existing statutes that have expired in relevance,[36] or drafting and enacting completely new laws.[37] While legislative action could be the most comprehensive and could provide a more direct solution to current problems, these proposals also have its problems. To say nothing of the risk that intervention would shackle a productive industry,[38] proposed legislative actions overlook underlying problems and consequently might only make

[32] *See generally* Margaret Jane Radin, *Regime Change in Intellectual Property: Superseding the Law of the State with the "Law" of the Firm*, 1 U. OTTAWA L. & TECH. J. 173, 180, 183–84 & n. 24, 187 (2004) (arguing that "case-by-case review of contractual terms" is "haphazard" and will "vary in intensity by jurisdiction").

[33] *See* James P. Nehf, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, 2005 U. ILL. J.L. TECH. & POL'Y 1, 2–4 (2005) (explaining how the FTC threatened regulatory action unless Internet firms took steps to self-regulate).

[34] *See* Allyson W. Haynes, *Online Privacy Policies: Contracting away Control over Personal Information?*, 111 PENN ST. L. REV. 587, 610–12 (2007).

[35] *See infra* Part III.A.

[36] *See, e.g.*, Goldberg, *supra* note 4, at 272 (proposing that Congress update the Stored Communications Act (SCA) to "account for today's pervasive Web technologies").

[37] *See, e.g.*, Jeff Sovern, *Toward a New Model of Consumer Protection: The Problem of Inflated Transaction Costs*, 47 WM. & MARY L. REV. 1635, 1642–43,1685–86, 1705–09 (2006) (explaining that norms can be instituted, at least with respect o prohibiting inflation of transaction costs, by enacting legislation that addresses the issue). There are also reports of the kind of legislation (privacy legislatio) that is currently being proposed in Congress. *See* Jia Lynn Yang, *Washington's Growing Interest in Privacy*, POST TECH (June 15, 2010, 7:28 PM), http://voices.washingtonpost.com/posttech/2010/06/washingtons_growing_interest_i.html; Sara Jerome & Puneet Kollipara, *Good Morning Tech*, HILLICON VALLEY (July 23, 2010, 5:18 AM), http://thehill.com/blogs/hillicon-valley/technology/110519-good-morning-tech (reporting that a bill introduced in the House "would require companies to get consent from individuals before collecting their personal information").

[38] *See* Jerome & Kollipara, *supra* note 37 (nothing the concern that online privacy legislation could "harm businesses").

marginal improvements. Legislation that mandates certain website disclosures, for example, might do little to create the right incentives for users to actually invest in educating themselves about the agreements they are making, or to create the right disincentives to discourage website exploitation of consumers.[39] Other legislative actions may offer greater protections for consumers, but would do little to provide consumers greater bargaining position to fix the very market failure that is causing unbalanced agreements. All of this on top of the fact that privacy may be a lower priority for legislatures, and would thus require a longer timeline before it could promulgate effective legislation.[40]

There is no consensus about the most effective solution to the privacy problem. But this note argues for a new proposal. It contends that these previous proposals would only patch the problem instead of attack its roots. Conversely, because contract law already governs the relationships in which privacy invasions take place,[41] this note argues that correcting any failures in the market that inhibit the *contracting* process is the most effective method of correction and invasion prevention. In order to so argue, this note will determine: (1) whether there are any market conditions that must hold to justify the enforceability of online contracts on which these relationships are based; and (2) whether the privacy problem is the product of the failing of any of these conditions; and (3) how those failures can be remedied based on particular failures. And because social networking firms have been a significant target as offenders who are committing these privacy breaches,[42] it is within the social networking setting that

[39] *See* Robert A. Hillman, *Online Boilerplate: Would Mandatory Website Disclosure of E-Standard Terms Backfire?*, 104 MICH. L. REV. 837, 842–44 (2006) (asserting that many e-consumers fail to read standard forms and that businesses assure they present terms in a manner most likely to deter consumers from reading them).

[40] *See* Boris Segalis, *Support for* ***Privacy Legislation*** *Survives Change of Power in Congress;* ***Privacy Legislation*** *May Advance*, INFOLAWGROUP (Jan. 26, 2011, 3:05 PM), http://www.infolawgroup.com/2011/01/articles/data-privacy-law-or-regulation/support-for-privacy-legislation-survives-change-of-power-in-congress-privacy-legislation-may-advance/ (reporting that while "federal privacy legislation may see the light of day in 2011," saving and creating jobs is Congress' top priority).

[41] This note discusses how contract law applies to privacy policies. *See infra* Part III.

[42] *See* Yasamine Hashemi, Note, *Facebook's Privacy Policy and Its Third-Party Partnerships: Lucrativity and Liability*, 15 B.U. J. SCI. & TECH. L. 140, 141–42, 149, 152–53 (2009) (discussing users' critical response to certain

this note aims to answer these questions.

In Part II, this note describes the legal and non-legal enforcement mechanisms that justify the enforcement of online contracts. In Part III, this note applies those enforcement mechanisms to the privacy problem in the online social networking setting. This note eventually finds that certain conditions must hold in the market (e.g., competition and a value on reputation) to allow non-legal sanctions and enforcement to keep parties from breach or opportunism leading to exploitation of private individuals. This note further finds that in the market for social networking, these conditions fail, and create opportunities for exploitation of consumers' private information. As a result, this note discusses in Section IV a proposal that aims to remedy the failure of those crucial market conditions.

III. GOVERNANCE STRUCTURES OF ELECTRONIC CONTRACTS

Before focusing on privacy policies and the applicability of contract law to these policies, this note first discusses online contracting in general. The reason for doing so is to provide a framework for a discussion of privacy policies and how well they fit into the mold of online contracts. To provide that framework, this section specifically discusses unique features of e-contracts and whether they are enforceable contracts notwithstanding those idiosyncrasies. The reason for a discussion on enforceability is more than just because of the fact that the basic issue of enforceability is "the central question in both the paper and the virtual worlds of contracting"[43]— demonstrating that online agreements (including privacy policies) can be enforceable contracts also provides a framework of enforcement and remedies

Facebook features that share user information). One need but read the news on any given day to learn of the legal trouble in which social networks are finding themselves. *See id.* at 147–50, 153, 156 (noting the Washington Post's coverage of Facebook users' privacy concerns); Susan J. Campbell, *Facebook Slapped with Class Action Lawsuit over Privacy*, TMCNET.COM (July 9, 2010), http://callcenterinfo.tmcnet.com/Analysis/articles/91511-facebook-slapped-with-class-action-lawsuit-over-privacy.htm?utm_medium=twitter (reporting that a 2010 lawsuit was not the first legal attack on Facebook regarding user privacy). Scholars have recognized this market as one of particular interest, and have begun to address the issue. *See, e.g.*, Hashemi, *supra* note 42, at 141–42 (investigating the legality of Facebook's advertising scheme).

[43] Robert A. Hillman & Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. REV. 429, 434 (2002).

by which consumers might have recourse against opportunistic sellers.

This section thus also treats the existing governance structure for contract enforcement and remedies, and how it has been able to cope with the unique challenges present in online agreements. Section III will then determine whether these governance mechanisms are equipped well enough to handle the even more unique set of circumstances in which the aforementioned privacy invasions are occurring.

A. The Enforceability of Paper and Electronic Standard Form Contracts

In many ways, clickwrap agreements are very similar to typical adhesion or standard form contracts,[44] and those online agreements face the same hurdles that affect contract formation. First, sellers typically have a cognitive advantage over consumers. "In both the paper and electronic worlds, businesses choose between adopting a set of boilerplate terms that are mutually beneficial or exploitative. In both worlds, they know more than consumers about the contractual risks, thereby creating an opportunity to exploit consumers."[45]

There are other features common between adhesion and online contracts that magnify that opportunity to exploit consumers. In both paper and electronic worlds, for example, the consumer lacks bargaining power because contracts are generally presented on "take-it-or-leave-it basis", and the terms found among competitors in the same industry will seldom have significant differences.[46]

Because of this common imbalance in party bargaining power, advantaged sellers have opportunities to take advantage of ignorant consumers. And they will, if they can get away with it. This is because opportunism is a basic assumption of human behavior in the calculation of contracting transactions costs.[47] If sellers[48] are opportunistic, they will take advantage of consumers

[44] Davis, *supra* note 7, at 577–78 ("Clickwrap agreements are generally thought to be a form of adhesion contract.").

[45] Hillman & Rachlinski, *supra* note 43, at 495.

[46] *Id.* at 434–37.

[47] *See* OLIVER E. WILLIAMSON, THE ECONOMIC INSTITUTIONS OF CAPITALISM 29–31 (1985) ("Transaction cost economics assumes that human agents are . . . given to opportunism.").

[48] It is not just sellers that are opportunistic, consumers are opportunistic too. *See id.* (describing the impact of opportunism from both parties on contract

when they can to get gain; they will take "calculated efforts to mislead, distort, disguise, obfuscate, or otherwise confuse" if it means the sellers become better off.[49] What this means is that any factor of electronic contracting that might contribute increasing sellers' bargaining positions will necessarily increase the likelihood of sellers' exploitation of consumers.

1. Additional Challenges of Electronic Contracts

The introduction of internet agreements has indeed presented new concerns that affect party bargaining positions that have created "novel opportunities for businesses to take advantage of consumers."[50] One aspect of online agreements that may make enforceability more questionable is that users may not even know they are subject to contracts.[51] Brick-and-mortar stores can hand consumers an actual copy of adhesion contracts, or better yet, can even make consumers sign the terms before agreeing to them. Companies can also send notice by a relatively reliable means in the mail, and notwithstanding the possibility that recipients will automatically consider it junk mail, companies can at least be reasonably certain that consumers obtain at least notice that there is an agreement. But with electronic agreements, consumers are even less likely to be on notice of the existence of a governing arrangement. There is no face-to-face meeting, and

execution). It is just that, in this setting, consumers simply lack the opportunity to take advantage of sellers because of the information imbalance. *See* Hillman & Rachlinski, *supra* note 43, at 435–37 (stating that while businesses repeatedly use standard form contracts in which they have "invested time and money perfecting," consumers often will not take the time to read the form or will not understand its boilerplate language).

[49] *See* WILLIAMSON, *supra* note 47, at 47 ("[O]pportunism refers to incomplete or distorted disclosure of information, especially to calculated efforts to mislead, distort, disguise, obfuscate, otherwise confuse.").

[50] Hillman & Rachlinski, *supra* note 43, at 433.

[51] Writers have acknowledged that contracts may be completed and perfectly valid even when an individual is unaware of its electronic existence. *See* Jean-Francois Lerouge, *The Use of Electronic Agents Questioned Under Contractual Law: Suggested Solutions on a European and American Level*, 18 J. MARSHALL J. COMPUTER & INFO. L. 403, 417, 418, 422 (1999) (stating that under section 107(d) of the Uniform Computer Information Transactions Act, a person who manifests assent through an electronic agent is bound "'even if no individual was aware of . . . the agent's operations'"). Additionally, consumers may not be completely aware of the contract terms, which could be equated with not being aware of its existence—without knowing the details of any governing terms of use or privacy policy agreement, users cannot understand what is expected of either party. *See* Hashemi, *supra* note 42, at 153–54.

there may be no hard-copy agreement that comes in the mail.[52] Instead, firms have the opportunity to hide a pro-seller contract, and it is thus more likely that the consumer herself must do her own research to discover whether there is an agreement and what the terms are (which is not likely to happen).[53]

Further, even if a consumer were to recognize the existence of a binding contract, they may be unable to get the assistance they might require to understand and appreciate the terms. Since standard form contracts, whether paper or electronic, are full of legalese and may already be difficult for a lay person to understand, online consumers are less likely to be able to get the help they would need to understand the terms.[54] And where they did not like any terms they were able to understand, online firms would rarely be able to offer live agents capable of negotiating the agreement.[55]

Whether consumers do not realize the existence of a contract, or cannot get help from a live agent, these challenges contribute to consumers "flying blind" to the risks of entering into the agreement.[56] Consequently, where consumers may be disadvantaged when it comes to standard form agreements, electronic agreements provide sellers even greater liberty to impose all of the risk-bearing responsibilities on the ignorant consumer.[57] Indeed, they have both opportunities and incentives

[52] At best, consumers may finally become aware that there is a governing agreement when they have ordered something online and they receive the agreement under the shrinkwrap of the item ordered. Ronald J. Mann & Travis Siebeneicher, *Just One Click: The Reality of Internet Retail Contracting*, 108 COLUM. L. REV. 984, 988–89 (2008). This is a different, but still related issue, treated in the line of cases dealing with shrinkwrap agreements. *See, e.g.*, ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1448–50, 1455 (7th Cir. 1996) ("Shrinkwrap licenses are enforceable unless their terms are objectionable on grounds applicable to contracts in general . . . .").

[53] *See* Mann & Siebeneicher, *supra* note 52, at 989–91 (explaining how users can passively assent to the terms of a browserwrap agreement).

[54] Hillman & Rachlinski, *supra* note 43, at 446.

[55] *Id.* at 468. That this is a true disadvantage of electronic contracts assumes that consumers would otherwise seek help with terms that they would need if they were entering into a hard-copy adhesion contract, and would further bargain over the terms. This assumption, however, may admittedly be a stretch. However, there is nevertheless the possibility of even a marginal decrease of bargaining power as a result of the loss of *opportunity* to review or edit terms. Additionally, perhaps this loss of opportunity makes sellers more willing to take risks regarding the inclusion of pro-seller terms.

[56] *See* Douglas G. Baird, *The Boilerplate Puzzle*, 104 MICH. L. REV. 933, 935–36 (2006).

[57] *See generally* Hillman & Rachlinski, *supra* note 43, at 433, 467-69; *id*. at

to exploit consumers.[58] What better circumstance for an opportunistic entrepreneur than one in which its opposing contracting party cannot or does not do much to protect herself from unfavorable terms?

2. Counterbalancing Factors

But just as there are unique problems for online contracts, there are similarly unique remedies. Writers thus contend that there are sufficient reasons for which online contracts should be enforceable notwithstanding challenges. Writers make a wide range of arguments, including economic and efficiency benefits of electronic contracting,[59] the fact that websites have ways to extract meaningful assent, online contracts actually bestow on consumers increased bargaining power, and that, in the end, websites still do not exploit consumers.[60]

Websites have devised ways to try to notify consumers of the existence of an agreement and simultaneously receive the consumer's assent to the terms. What courts have found to be the method most likely to put a consumer on notice is to make entrance or use of a firm's site or services contingent upon taking some action.[61] Perhaps most frequently, this action takes the form of nothing more than a click of the mouse, signaling that "I agree" to whatever terms may apply, before the consumer gleefully continues on their way, soon to forget any content of the agreement. Some still contend that this clickwrap method is inadequate, though. It is easy for consumers to ignore meager attempts to put them on notice of contract terms. With only a click of the mouse separating users from the opportunity to enjoy

935–37.

[58] Hillman & Rachlinski, *supra* note 43, at 433.

[59] *See, e.g.*, Davis, *supra* note 7, at 577–79 (arguing that electronic standard form contracts offer economic benefits such as lowered costs to consumers, increased flexibility, and alternatives to litigation).

[60] *See, e.g.*, Daniel D. Barnhizer, *Propertization Metaphors for Bargaining Power and Control of the Self in the Information Age*, 54 CLEV. ST. L. REV. 69, 82–84 (2006) (arguing that online contracts "increase[ ] the ability of the consumer to achieve a preferred outcome"); Davis, *supra* note 7, at 577–79, 582 ("[C]ontractors are not vigorously exploiting their ability to extract assent in a way that requires a drastic judicial response.").

[61] *See, e.g.*, Feldman v. Google, Inc., 513 F. Supp. 2d 229, 237–38 (E.D. Pa. 2007). *See generally* Oakley, supra note 6, at 1051, 1078–80 (stating that inaction does not show manifestation of assent, but "the action of clicking on a button that is labeled with an indication of acceptance" does seem to be sufficient).

"free and instantaneous availability of many online resources," users become "'click-happy'" and consent to any agreement put on the screen in front of them.[62] There is also another, perhaps less effective way websites try to notify consumers of the existence of contract governance—some may post a link to the agreement terms on the bottom of the website.[63] These browsewrap agreements, though, are visible only if the user seeks out the policy and reads it.[64] And if consumers are not even going to read contracts that are put directly in front of them or those that are linked to a box they must click before using a site, they are going to be even less likely to seek out agreements and privacy policies that are tucked away at the bottom of web pages.

Additionally, there is an argument that consumers do not even need additional protection when it comes to online contracts, because consumers actually have greater bargaining power for negotiating such agreements. Their bargaining power increase comes from the investment savings that consumers might theoretically enjoy by not having to sign a contract in the presence of an anxious salesman, and having the opportunity to review contract terms in the convenience of their own homes.[65] This argument assumes, though, that consumers are somehow aware of the existence of the agreement—an assumption that may not be safely made given the online setting. But even making this assumption that consumers know about the agreement, consumers are still leaving themselves in a disadvantaged condition. Despite decreased costs that come with the convenience of reading agreements on their own terms, users apparently still feel that the costs of wading through legalese in lengthy agreements outweigh any potential benefits to a careful examination of the agreement, and consequently, still do not examine their contracts.[66] Putting aside the question of whether electronic contracts really do disadvantage consumers more so than standard form contracts, writers suggest that, in the end, website entrepreneurs may be more altruistic than they have to be.[67] While it seems to follow that sellers might have much to

[62] Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract?: Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1, 13–14 (2009).

[63] *See* Haynes, *supra* note 34, at 617.

[64] *See id.*

[65] *See* Hillman & Rachlinski, *supra* note 43, at 480–81.

[66] *Id.* at 479–80.

[67] A website entrepenuer just like any seller of goods will be concerned with

gain from including pro-seller contract terms where sellers have the opportunity to exploit buyers, one recent study concluded that pro-seller contract terms are less beneficial to them than it seems.[68] Reasoning that "the mere possibility of disgruntled customers is not enough to justify" the extra costs needed to make a pro-seller contract enforceable; this study found that fewer than six percent of retailers with websites actually create such enforceable agreements.[69] This result, with the merit of the other counterbalancing factors make it easier for courts to lay aside the theoretical challenges of clickwrap agreements and find them enforceable.

3. Enforceability

Despite the weaknesses and challenges of online contracts, precedent has been nearly unanimous in deciding that, as long as users are provided with an adequate opportunity to review the terms and manifest their assent,[70] these electronically-made agreements create enforceable contracts.[71]

Given the challenges with respect to consumers' bargaining position, and sellers' inclination towards opportunism,[72] the result of enforceability could be questioned. Then again, if sellers are truly not taking advantage of their opportunity to exploit consumer weakness as some scholars posit, the enforceability issue may not be so puzzling.[73] It turns out that these sites are not just altruistically and mercifully giving consumers more even playing fields. Rather, there is in place a framework that is able to cope with electronic contracting challenges. This framework happens to be comprised of the same contract enforcement mechanisms that are installed into a paper world and can nevertheless apply in the electronic world, notwithstanding new

securing customers. "A seller concerned about its reputation can be expected to treat customers better than is required by the letter of the contract." Lucian A. Bebchuk & Richard A. Posner, *One-Sided Contracts in Competitive Consumer Markets*, 104 MICH. L. REV. 827, 827–28 (2006).

68 Mann & Siebeneicher, *supra* note 52, at 984.

69 *Id*. at 987, 993, 998, 1000–01.

70 Haynes, *supra* note 34, at 613–15; Davis, *supra* note 7, at 579.

71 Gindin, *supra* note 62, at 27.

72 Barnhizer, *supra* note 60, at 80–81; Sirkka L. Jarvenpaa & Emerson H. Tiller, *Customer Trust in Virtual Environments: A Managerial Perspective*, 81 B.U. L. REV. 665, 665–66 (2001).

73 *See, e.g.*, Bebchuk & Posner, *supra* note 67, at 827–28; Davis, *supra* note 7, at 577.

features and challenges.[74] This note then next explores this framework, separating legal and non-legal enforcement mechanisms, and determining how these prevent exploitation. By doing so, this note hopes to uncover some of the conditions that must hold in order for the non-legal sanctions to be operative. What this note will eventually show is that, if certain conditions fail, there may not be adequate checks to opportunism and a tendency to exploit weakened consumers.

B. Whether Contract Mechanisms Discourage Seller Opportunism

1. Traditional Legal Enforcement Mechanisms

Sellers and websites have not universally acted on opportunistic urges to exploit users' weakened bargaining position perhaps because clickwrap agreements are still subject to traditional contract remedies and enforcement. As discussed above, courts have held that electronic contracts are still enforceable.[75] And while courts have applied traditional contract theory in so holding, they have tailored the requirements for contract formation to overcome the hurdles of e-contracting.[76]

Focusing requirements on ensuring consumers the greatest possibility of receiving notice and manifesting assent, courts generally hold that in order to have a binding contract, these four steps should be satisfied:

"The user must have adequate notice that the proposed terms exist;

The user must have a meaningful opportunity to review the terms;

The user must have adequate notice that taking a specified, optional action manifests assent to the terms; and

The user must, in fact, take that action."[77]

---

[74] *See* Hillman & Rachlinski, *supra* note 43, at 433–34 ("[T]he basic structure and underlying economics of the standard-form transaction are consistent in both the paper and electronic worlds.").

[75] *See supra* notes 70–71 and accompanying text.

[76] *See* Davis, *supra* note 7, at 590–91, 597–98 (explaining that the terms of clickwrap agreements are susceptible to review under traditional contract doctrines such as unconscionability and public policy in addition to "specialized doctrines that can be applied to some types of terms that arise frequently in clickwrap litigation").

[77] Terenzi, *supra* note 5, at 1079–80 (citing the American Bar Association's recommendations found at Jason Haislmaier, *How Do I Build an Enforceable*

In terms of an enforcement mechanism, the formation requirements set a minimum standard that, if not reached, could render a pro-seller agreement unenforceable.[78] But even though cheated consumers could theoretically try to challenge a pro-seller agreement by arguing it was never formed, it would be a steep uphill battle.[79] Such an argument may have been more meritorious early in the development of online contracting. By now, though, most firms have the requirements figured out. Generally, a firm can meet these requirements, and thus form a binding clickwrap agreement, when users must click an "I Agree" box that at least refers to a governing terms of use or privacy policy.[80]

Users may find more reliable means of challenging an online agreement in the same "doctrines that form the traditional framework used by courts to determine the validity of boilerplate terms in the paper world."[81] Specifically, courts use the doctrines of unconscionability, reasonable expectation, and public policy to ensure electronic contracts do not cross any lines in exploiting consumers.[82] Thus, if an agreement is too one-sided and unfairly exploits consumers, courts can curb abuse by intervention with one of these doctrines.

But these remedies do have limits. Courts may find that a pro-seller agreement that "'shock[s] the conscience'" to be unconscionable and may accordingly correct the contract.[83] But for anything less, such as a contract that may only mildly disturb

Online Agreement?--Not (Always) the Way SalesForce.com or Google Would, THINKINGOPEN (Mar. 8, 2008), http:// thinkingopen.wordpress.com/2008/03/08/how-do-i-build-an-enforceable-online-contract-not-always-what-salesforcecom-or-google-would-do).

[78] *See* Haynes, *supra* note 34, at 613–15 (discussing cases wherein courts found electronic agreements unenforceable due to lack of assent).

[79] There have been court decisions that both have accepted the lack of assent argument and have rejected it. *See id.* However, decisions finding favor with the argument (and thus holding that there was no contract) "have been criticized by commentators and disagreed with by courts." *Id.* at 616–17. While there is arguably less evidence of manifestation of assent regarding a browsewrap agreement, the precedent upholding clickwrap agreements is sufficiently clear so as to make the argument a rather difficult one with which to win. *See id.* at 613–15, 617–18.

[80] Terenzi, *supra* note 5, at 1079–80.

[81] Hillman & Rachlinski, *supra* note 43, at 429.

[82] *See id.* at 454–56, 487–90; Davis, *supra* note 7, at 579–80. For examples of cases in which courts have invalidated online adhesion contracts on the basis that they violated public policy, see Oakley, *supra* note 6, at 1043, 1086–87.

[83] Hillman & Rachlinski, *supra* note 43, at 456–58.

the conscience, courts may be less willing to interfere.[84] Additionally, while the reasonable expectation doctrine could provide consumers with coverage against unreasonable terms, the protection may not reach those terms that are unfair because they are merely one-sided.[85]

There are other protections, though. In addition to common law doctrines of unconscionability and reasonable expectation, tort-based private actions may offer some protection against unfair contracting practices.[86] Whether these remedies are actually effective in voiding the effects of one-sided or otherwise unfair contracts is an issue that writers have discussed at length.[87] While most writers agree that torts would be insufficient to nullify all but the most egregious offenses,[88] the discussion alone indicates that there exists at least some risk of tort-based retaliation, and the threat could thus serve as at least a marginally additional deterrent.

Because of the potential holes in the applicable legal enforcement mechanisms that could keep sellers in check, sellers may just not be held in check and give in to their opportunistic urges. But these mechanisms are not alone, and can be supplemented by a "[m]uch less apparent" check on seller action: non-legal sanctions.[89]

2. Non-Legal Enforcement Mechanisms

"Virtually all commercial transactions involve nonlegal commitments — commitments enforced only or predominately by

[84] *See id.* at 457–58.

[85] *See id.* at 459–60.

[86] *See* Hotaling, *supra* note 13, at 541–42.

[87] *See, e.g.*, *id.* at 532, 548–51 (discussing the inadequacy of common law tort remedies); William Dalsen, Comment, *Civil Remedies for Invasions of Privacy: A Perspective on Software Vendors and Intrusion upon Seclusion*, 2009 WIS. L. REV. 1059, 1060–62 (2009) ("[M]any civil remedies designed to protect privacy in the physical world are proving to be feeble solutions to privacy problems in cyberspace."); Gehan Gunasekara & Alan Toy, *"Myspace" or Public Space: The Relevance of Data Protection Laws to Online Social Networking*, 23 N.Z. U. L. REV. 191, 192, 194–96, 213 (2008) ("The tort of privacy faces severe constraints when it is applied to an arena such as [online social networking].").

[88] *See, e.g.*, Gunasekara & Toy, *supra* note 87, at 194–95 (explaining that the tort law is constrained in online situations in part because "identifiable personal information such as one's address, social security number, spending habits and financial information are public matters the disclosure of which is not sufficiently offensive to enable an action to be brought").

[89] For a discussion of non-legal sanctions, see David Charny, *Nonlegal Sanctions in Commercial Relationships*, 104 HARV. L. REV. 373, 375–79 (1990).

nonlegal sanctions . . . ."[90] Electronic contracts are no exception. Though "legally unenforceable," these sanctions can provide an "alternative mechanism" for discouraging online sellers to exploit consumers, even and perhaps especially when legal sanctions are not present or insufficient.[91]

[N]on-legal sanctions operate side-by-side with legal sanctions. Most commercial relationships involve some commitments that are legally enforceable; some commitments that are legally enforceable but are also, or primarily, enforced by nonlegal sanctions; and some commitments that are enforced exclusively by nonlegal sanctions . . . .Indeed, contracts that formally provide for legal sanctions depend upon nonlegal sanctions for their effectiveness whenever the legal sanctions are ineffective in inducing the promisor to perform.[92]

Thus, non-legal sanctions are an integral part of the "workable set of rules that protects consumers from surprise and unfair terms while supporting the economically beneficial use of standard forms."[93]

This note does not seek describe in detail all types of non-legal sanctions, but it does seek to determine whether any conditions must exist for the imposition of non-legal sanctions. Thus, this note will discuss specifically the effects of only market competition and reputation concerns on the imposition of non-legal sanctions.

i. Competition

This note first discusses how competition limits the opportunities for seller opportunism. Competition, first of all, is the "'force' which, by equating prices and marginal costs, assures allocative efficiency in the use of resources. . . . [T]hrough competition, resources 'gravitate' toward their most productive uses, and, through competition, price is 'forced' to the lowest level which is sustainable over the long run."[94] These forces of competition are "the result of free entry of a large number of" competitors.[95]

[90] *Id.* at 376.
[91] *See id*. at 376–78.
[92] *Id*. at 394.
[93] Hillman & Rachlinski, *supra* note 43, at 433.
[94] Paul J. McNulty, *Economic Theory and the Meaning of Competition*, 82 Q. J. ECON. 639, 643 (1968).
[95] *Id.* at 642.

Largely because of the number of competitors and desire to offer the lowest possible price (and thus minimize costs), conditions in a competitive market are such that they may keep sellers from exploiting their own leveraged bargaining position:

> [A]nalysts have suggested that in competitive markets a small number of readers, whom businesses cannot afford to lose, may be sufficient to deter overreaching. Competition for market share in the e-environment may therefore deter businesses from drafting onerous terms or even motivate them to write terms favorable to consumers. Because e-consumers can easily spread the word about the nature of the terms, the Internet should increase this incentive.[96]

It is important to clarify, though, that the "[c]ompetition for market share" that deters businesses from drafting onerous terms is not competition for contract terms, but is competition for products.[97] While sellers could use beneficial terms to increase their competitiveness in a certain product market (e.g., offering more favorable arbitration terms than the next competitor), doing so would incur costs.[98] And if consumers are not going to appreciate any competitive advantages that businesses create,[99]

---

[96] Hillman, *supra* note 39, at 843, 845–46. *See generally* LAWRENCE J. GITMAN & CARL MCDANIEL, THE FUTURE OF BUSINESS: THE ESSENTIALS 308–09 (4th ed. 2009) (explaining how competition can cause prices to fall thereby attracting more consumers). *But see* Florencia Marotta-Wurgler, *Competition and the Quality of Standard Form Contracts: An Empirical Analysis of Software License Agreements* 5 (N.Y. Univ. Sch. of Law & Econ. Research Paper Series, Working Paper No. 05-11, 2005), *available at* http://ssrn.com/abstract=799274 ("[T]he overall quality of standard terms is essentially uncorrelated with competitive conditions. While competition does significantly reduce product *prices*, it does not, from the buyer's perspective, improve [contract] *terms*."). While Marotta-Wurgler's conclusion about the lack of correlation between competition and standard form contract terms may undermine the argument that competition enhances consumer bargaining position, it may not have that devastating of an effect on the same argument in the setting of online social media. *See infra* Part III.

[97] *See* Hillman, *supra* note 39, at 842–43.

[98] The costs of competing on terms would include costs of market research to determine the terms other competitors were offering, and the costs of drafting tailored terms. *See generally* Wolfgang Kasper, *Competition*, CONCISE ENCYCLOPEDIA ECON., http://www.econlib.org/library/Enc/Competition.html (last visited Mar. 25, 2011) (describing the costs that must be incurred to compete effectively in a market).

[99] *See* Hillman & Rachlinski, *supra* note 43, at 441–43 ("Exploiting the ignorance of the vast majority of consumers might be more lucrative for some businesses than competing for the smart consumers."); *see also* Marotta-Wurgler, *supra* note 96, at 7–8 (suggesting that buyers may not even perceive variations in terms in a competitive market).

the costs would likely exceed any resulting marginal benefits.[100] In other words, a company that tries to allure consumers to their product with favorable contract terms would have a higher price (because of increased costs), and because consumers would not likely appreciate the difference, the consumers would not pay for a product that, *ceteris peribus*, has more favorable contract terms and a higher price. And because no consumer would pay, the firm loses business. It is thus competition in the market for the actual products or services that provides "assurance that businesses will not supply exploitative terms."[101]

In fact, sellers' desire to keep their costs, and thus their product price low is one reason that competition can check seller opportunism. Not only will product market competition keep firms from competing with regard to contract terms, but it can also keep sellers from allocating excessive costs on drafting *pro-seller*—as opposed to pro-buyer—contract terms. Whether a seller drafts competitive, pro-buyer terms or tries to sneak pro-seller contract terms past the buyer, taking the time to draft any tailored agreement requires a particular allotment of firm resources.[102] And sellers get very limited, if any, benefit from investing any resources to contract drafting.[103] Albeit a small cost in the long run, it is nevertheless a cost that increases total costs of production and increases final prices.[104] So as long as market competitors are pushing that firm for lower and lower prices to be able to attract consumers, the possibility of increased prices would be sufficient to keep a firm from allocating resources to drafting onerous, pro-seller terms.[105]

---

[100] *See* Sovern, *supra* note 37, at 1680–81 ("[F]irms should advertise terms that are more favorable to consumers if the profits from increased sales generated by those terms exceed the cost of the advertising together with the lost profits from eschewing terms that are less favorable to consumers.").

[101] Hillman & Rachlinski, *supra* note 43, at 441–42 (citing Richard L. Hasen, Comment, *Efficiency Under Informational Asymmetry: The Effect of Framing on Legal Rules,* 38 UCLA L. REV. 391, 426–27 (1990)).

[102] *See* Mann & Siebeneicher, *supra* note 52, at 999–1000 ("[R]etailers should extract consent to pro-seller terms whenever the costs of an additionally complex interface are less than the benefits of the more favorable terms.").

[103] *See id.* at 986 ("[T]here is a substantial cost to making contracts enforceable and relatively little benefit to making them one-sided . . . .").

[104] *See generally* JERRY J. WEYGANDT, DONALD E. KIESO & PAUL D. KIMMEL, MANAGERIAL ACCOUNTING: TOOLS FOR BUSINESS DECISION MAKING 341 (5th ed. 2010) (describing how firms set prices based on costs in a less competitive market).

[105] *See generally* GITMAN & MCDANIEL, *supra* note 96, at 308–09 (explaining the various pricing schemes available to sellers wishing to attract customers

Instead, firms will invest the least amount of resources in contract drafting as long as they can still reach a cost-minimizing allocation of contractual risks. They do this not necessarily by drafting a simple agreement, but by borrowing what other similarly-situated firms have adopted as the best risk allocation schemes. In other words:

> Just as the drive to reduce costs pushes manufacturers to use similar component parts, it also pushes businesses to employ comparable terms to allocate contract risks. Because the best allocation of risks is not likely to vary between businesses within an industry, most businesses will offer terms similar to those offered by their competitors.[106]

Thus, competing firms will not just resist competition on product terms, but they actually end up sharing similar terms because the benefits of minimizing contract drafting costs are greater than any benefit from drafting tailored, pro-seller terms.

A second way that competition helps to "shoulder some of the oppressiveness" that may otherwise be imposed on consumers is by providing market alternatives.[107] "[M]arket alternatives help[ ] the bargaining position of the aggrieved party"[108] by allowing "consumers to locate competition, advice, and general information relating to the companies with which they intend on contracting."[109] Thus, if one firm's excessively costly terms create a supra-competitive price, consumers can simply shop elsewhere. Because of this threat of losing the consumers that might leave a seller to go to another, "sellers have incentives to make certain favorable terms salient to consumers."[110] The existence of market alternatives coupled with consumers who can gather information about those alternatives will strengthen consumer bargaining power, especially if sellers are concerned with their reputation.

---

and maintain profits); WEYGANDT, KIESO, & KIMMEL *supra* note 104, at 341 ("[I]n a competitive common-product environment the market price is already set . . . .").

106 Hillman & Rachlinski, *supra* note 43, at 438–39.

107 Cory S. Winter, Comment, *The Rap on Clickwrap: How Procedural Unconscionability is Threatening the E-Commerce Marketplace*, 18 WIDENER L.J. 249, 278 (2008).

108 *Id*.

109 *Id*. at 278–80.

110 Clayton P. Gillette, *Pre-Approved Contracts for Internet Commerce*, 42 HOUS. L. REV. 975, 977 (2005).

ii. Reputational Checks

Concerns about reputation can supplement the disincentives that a competitive market provides by further discouraging seller exploitation. This is because "sellers who attempt to capture the marginal buyer [and] who face reputational constraints . . . will face competitive pressures inconsistent with efforts to exploit nonreaders."[111] In other words, if a firm "improperly breaches his commitments, he damages his reputation and thereby loses valuable opportunities for future trade" with future consumers.[112] This is true as long as firms care about their reputation,[113] consumers have opportunities and incentives to damage a seller's reputation if that seller has damaged the consumer, and potential consumers can have access to information left by past consumers.[114]

The fact that firms care about their reputation follows from the fact that firms are cost-minimizing, and that reputation is a resource in which firms invest.[115] If reputation is lost because of exploitation or opportunism the investment is lost.[116] But this cost is only incurred where potential buyers are able to gain information about reputation. In order for this to happen, 1) customers must be able to recognize when a seller has damaged them; 2) customers must be able and willing to transmit information about the damage; and 3) potential customers must be able to access that transmitted information.[117]

Generally, customers are able to recognize seller misbehavior or misconduct, whether it is the result of a breach or some other unreasonable behavior, because the customer suffers some

---

[111] *Id*.

[112] Charny, *supra* note 89, at 393.

[113] Hillman & Rachlinski, *supra* note 43, at 442–44.

[114] *See* Gillette, *supra* note 110, at 977 ("Consumers who have negative experiences with a seller . . . have incentives to publicize their experience, inducing sellers to avoid adverse reputational gossip.").

[115] That reputation is a resource in which firms make investments is evidenced by the fact that reputation is similar to, if not synonymous with goodwill, which is an actual asset that is quantified an on which taxes are paid. *See* Tammy L. Barham, Note, *The Battle over the Depreciablity of Goodwill: Was the Victory Worth the Wait?* 15 MISS. C. L. REV. 115, 116–17 (equating good will to reputation and reviewing federal case law regarding the tax scheme imposed on goodwill).

[116] *See* Bebchuk & Posner, *supra* note 67, at 829–30 (stating that if sellers behave opportunistically, they risk "suffer[ing] a loss of reputation, which is a cost").

[117] *See* Gillette, *supra* note 110, at 977.

damage[118]—damage that could be in the form of an unreasonable late check-out fee or the publication of an unapproved transcript.[119] In terms of consumers' abilities to transmit information, it is ironically the same internet that allows sellers to hide pro-seller terms and exploiting clauses that can also afford customers opportunities to damage seller reputation and prevent sellers from so exploiting. And where consumers can transmit information is also where consumers may access reputation information—there are many forums and other websites dedicated to spreading and gathering information on seller reviews.[120]

Spreading reputation information benefits consumers by providing them bargaining power while likewise encouraging better seller behavior. Access to costless reputation information endows consumers with significant bargaining power by providing them "a variety of effective sanctions, ranging from casual criticism and correction, to more discomfiting forms of communal disapprobation, to boycott, ostracism, excommunication, or violent self-help."[121] Consumers can thereby hang the threat of publication of damaging information over the heads of bad businesses. And if a business exploits consumers, consumers will simply refuse to transact with them.[122] And in a competitive internet-based market, where e-businesses can develop as soon as one disappears, and where trust and reliability is crucial to a site's success, this threat is enough to scare sellers into forgoing their opportunities and incentives to exploit. In fact, just because reputation is so important, some scholars have argued that sellers will even err on the safe side when it comes to exploitation. A study conducted

[118] *See id.* at 977 (suggesting that ignorance on the part of buyers is "less pervasive than feared"). This condition only generally holds because, specifically, there may be settings in which customers are not able to recognize that sellers have wronged them. The privacy setting is one such setting. The effects of the failure of consumers to recognize damage are discussed in the next Section. *See infra* Part III.

[119] Bebchuk & Posner, *supra* note 67, at 833–34. Bebchuk and Posner discuss how sellers will include one-sided, pro-seller terms in order to counter the possibility that consumers damage their reputation. *See id.* at 827–28, 831–32.

[120] A quick browse on any internet search engine reveals lists of retail review sites including: www.resellerratings.com, www.retailreviews.com, www.epinions.com, www.bizrate.com, www.bbbonline.org, and more.

[121] Charny, *supra* note 89, at 388, 392–93.

[122] Hillman & Rachlinski, *supra* note 43, at 441.

to support this theory indicated that firms concerned about reputation will actually treat consumers better than they have to.[123]

Non-legal sanctions from competition and reputation thus provide additional barriers against exploitation and opportunism where traditional legal sanctions may be insufficient. In fact, because these influences effectively discourage opportunistic behavior, "legal intervention may disrupt a delicate social equilibrium by tilting the pre-established balance of power toward one social group and against the other."[124] This discussion of non-legal sanctions has also helped to identify market conditions that must hold in order to justify the enforceability of online contracts—there must be competition in the *product* market, and sellers must care about reputation while consumers have opportunities to damage that reputation. Whether these conditions may fail in a social media setting may help to determine further whether the failing of these conditions can result in privacy invasion. This note answers these questions in the next section by trying to apply the framework for e-contract enforcement to privacy policies specifically.

IV. WHETHER EXISTING GOVERNANCE STRUCTURES OFFER EFFECTIVE PROTECTION OF PRIVACY RIGHTS

With a backdrop of the current enforcement and protection mechanisms, this note may be able to determine whether the same enforcement mechanisms can properly protect against privacy invasion. This section will do this by first describing the current enforcement of privacy, and will then apply the aforementioned enforcement mechanism to privacy policies. Because much of the contention over privacy has been within the online social media setting, this section will observe this setting specifically. If the conditions on which online contract enforcement rests fail in this setting, regulators should take action to correct the areas in which the enforcement mechanisms fail.

This section will demonstrate that there are indeed both market failures and a failure of the necessary conditions described above as being necessary to the effectiveness of non-

[123] Bebchuk & Posner, *supra* note 67, at 833–34.
[124] Charny, *supra* note 89, at 388.

legal sanctions. Specifically, in the market for social networking, there is no or limited competition in the product market, sellers care less about reputation and consumers have restricted abilities to damage reputation. Additionally, asymmetric information contributes further to uneven bargaining positions that can open the door for opportunism. This section will ultimately demonstrate that because the market cannot provide circumstances sufficiently even to allow for a fair contractual exchange, intervention is needed.

A. The Enforcement of Privacy through Privacy Policies

Internet sites have adopted privacy policies with such universality that it is uncommon to come across a website without one.[125] Placed on websites for the purpose of notifying users of the information the site collects and to what protections users are (not) entitled, privacy policies generally appear in the same forms as those of other electronic contracts: in a hyperlink at the bottom of the website, or in a hyperlink that appears upon registering for the use of a certain website. [126] Web sellers draft and post these privacy policies to satisfy legislative requirements and to at least feign concern for privacy to gain consumer confidence.[127]

Because this discussion is taking place within the online social media setting, taking a specific look at Facebook's governing privacy policy illustrates the use of privacy policies. Currently, if a user registered to become a user on Facebook, she would have to enter her name, email address, gender and birth date.[128] After clicking on a "Sign Up" button, the user would be taken to a "Security Check" page on which the user must enter two randomly generated words before clicking another "Sign Up" button.[129] Below this button is the following text: "By clicking Sign Up, you are indicating that you have read and agree to the Terms of Use and Privacy Policy," and the words "Terms of Use" and "Privacy Policy" are hyperlinked text which directs the

[125] Haynes, *supra* note 34, at 593–94.

[126] *Id.*; Jessica P. Meredith, Note, *Combating Cyberbullying: Emphasizing Education over Criminalization*, 63 Fed. Comm. L.J. 311, 319 (2010).

[127] Haynes, *supra* note 34, at 593.

[128] *See* FACEBOOK, http://www.facebook.com (last visited Mar. 15, 2011) (the registration procedure as of March 22, 2011).

[129] *See id.*

curious consumer to each respective document.[130]

Whether the privacy policy to which a user is directed is actually an agreement is "speculative," but because case law finds enforceability when users click to indicate their agreement, as they must do to sign up with Facebook, courts would probably find that Facebook's privacy policy is an enforceable contract.[131]

So while a contract may be formed, there may be no guarantee that it will contain any terms about privacy. In fact, sellers are leery of making any representations that they include in the contracts about privacy.[132] This is because if they defect from these representations, the Federal Trade Commission—the most active actor in privacy enforcement—may be able to hold firms to those representations. As the nation's advocate for consumer protection, the FTC is entrusted with the protection of users' privacy by regulating "unfair or deceptive" trade practices.[133] But the FTC's jurisdiction and authority is limited to only those acts that are unfair or deceptive or otherwise in violation of a firm's privacy policy.[134] As a result, the FTC could not regulate acts that would offend principles of justice or ethics if an offender made no representations either way about the act. Specifically, because the FTC's role is *enforcement* rather than regulation,[135] firms have an incentive to exclude protection provisions in privacy policies—if there is no representation about privacy, there cannot be any *mis*representation about privacy, and the FTC is a mere toothless enforcer. In other words, "'[i]f the

130 *Id.*

131 Hashemi, *supra* note 42, at 152.

132 Online firms may be cautious about making privacy-related representations because of the involvement of third parties. Even the sellers may not know what third-parties may be involved, and further, sellers may not know what those third parties will do. *Cf.* Hashemi, *supra* note 42, at 142–46 (describing the controversy surrounding the disclosure of Facebook users' activities on third-party affiliate websites). Making representations about such unknown conditions would force sellers to bear significant risks, especially because of the FTC's ability to enforce representations. *See* Federal Trade Commission Act § 5, 15 U.S.C. § 45 (a)(1), (2), (l) (2006).

133 *See* 15 U.S.C. § 45 (a)(1), (2); *FTC Bureau of Consumer Protection*, FED. TRADE COMM'N, http://www.ftc.gov/bcp/index.shtml (last visited Mar. 22, 2011).

134 *See* Haynes, *supra* note 34, at 599-600. For example, the settlement with Twitter included a prohibition only from "'misleading consumers about the extent to which it . . . protects . . . nonpublic consumer information.'" Cecilia Kang, *Twitter Settles with FTC over Hacking Breach*, WASH. POST, June 25, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/06/24/AR2010062406473.html.

135 Terenzi, *supra* note 5, at 1067–68.

website complies with its own promises, there is little else to prevent the site from doing with [users' private] information whatever it wants—sharing, selling or otherwise making use of the information—besides the website company's own interest in attracting and maintaining customers.'"[136]

This result should be bothersome. The FTC is trying to enforce private contracts, but is doing so with limited statutory firepower. Consequently, firms have a perverse incentive to contract around privacy so that they offer no protection for users. But if online social media firms are subject to the same checks as those online sellers in other settings in which opportunism is curbed or restricted, then online social media would likewise not be able to get away with exploitation. The Federal Trade Commission may certainly be limited in its ability to regulate privacy, but are legal and non-legal contract enforcement mechanisms likewise limited? This note now observes the ability of those enforcement mechanisms to protect privacy.

B. Whether Legal Mechanisms Are Effective Means of Protecting Privacy

This section will determine whether contract-based or other legal doctrines equip users with causes of action to keep sellers from intruding privacy. Arguably the best methods consumers have for challenging the enforceability of a policy are claiming a lack of assent or unconscionability.[137] Aside from other contract doctrines like reasonable expectation, private and common law tort principles and privacy statutes may offer additional protection against privacy invasion.

First, consumers could theoretically challenge the formation of a privacy policy if it permitted the seller to invade the consumer's privacy. But just as with typical clickwrap agreements, social networking sites have shaped privacy policies with well-established precedent in mind, and winning the formation argument could be difficult.[138]

Consumers may have marginally better chances making a challenge based on unconscionability. Whether a claim of unconscionability is aimed at invalidating credit card terms of

[136] *Id.* at 1067–68 & n.109 (quoting Haynes, *supra* note 35 at 588).

[137] Haynes, *supra* note 34, at 624.

[138] *See id* at 588-90, 593–94, 613–15, 618 (analogizing the case law on online contract formation, which has found that users are bound where "they have 'clicked' acceptance or where they have actual notice of the terms").

use or an electronic privacy policy, the claimant in most cases must show both procedural and substantive unconscionability before a court would refuse enforcement of a contract term.[139] Because procedural unconscionability is concerned with the contracting process and because privacy policies and other clickwrap agreements have similar processes, the argument that a privacy policy is procedurally unconscionable will likely mirror that for a similar clickwrap contract.[140] In either setting, an agreement's adhesive nature, take-it-or-leave-it basis, and party bargaining positions are relevant considerations and could provide a reasonably strong argument in favor of procedural unconscionability.[141]

Where the typical clickwrap and privacy policy settings may differ is substantive unconscionability, which deals with the unfairness of terms resulting from excessive risks or costs that one party must bear.[142] Arguably, the substantive unconscionability argument would be stronger in the privacy setting. This is so because the costs that an unfair contract would impose on a consumer would be greater if those costs derived from the exploitation of private information, rather than from unfavorable arbitration, forum-selection or other less-harmful boilerplate terms.

But at this point, the strength of the substantive unconscionability argument may not be any more than speculative. In the end, chances that an unconscionability-based challenge can succeed are far from promising. Regardless the setting, unconscionability is a relatively high standard that only acts that "'shock[ ] the conscious'" can meet.[143] As a result, most courts have agreed that contracts of adhesion, including privacy policies, are still enforceable notwithstanding the possibility of unconscionability.[144] Therefore, there may not be much about unconscionability that could add much protection for users, whether sellers did or did not include terms about privacy.

Unfortunately for aggrieved consumers, they are not likely to

---

139 *Id.* at 619.

140 *Id.* at 619–20.

141 *Id.*

142 *See id.* at 620–21 (stating that contract terms have been found substantively unconscionable where the "language was so one-sided as to render it an unenforceable illusory promise").

143 Oakley, *supra* note 6, at 1056 (alteration in original) (quoting Hillman & Rachlinski, *supra* note 43, at 457).

144 Bebchuk & Posner, *supra* note 67, at 829.

get much more help from other legal sources.[145] Consumers would not likely get much mileage from the reasonable expectation doctrine, about which one writer points out that social network users would hardly have any expectation of privacy given the fact that the very purpose of creating online profiles is to make information available to others.[146] Moreover, privacy statutes have not been able to keep up with changing technology and have therefore offered insufficient protection for consumers.[147] And finally, courts have consistently rejected tort-based remedies.[148]

Are consumers thus left without recourse? Are they left to wait for legislators to step up to the plate to draft comprehensive and strict guidelines that can finally adequately protect against unwanted invasion? Before they are left to settle with these dire results, there may yet be one other source of enforcement of consumer rights found in non-legal enforcement and sanction mechanisms. Scholars believe that these non-legal sanctions play a large part in the justification for allowing generic clickwrap and other e-contracts.[149] Can the same be true for justifying the enforceability of questionably fair privacy policies?

C. Applying Non-Legal Checks and Sanctions to Privacy Policies

In the general clickwrap setting, market competition and a seller's concern for its own reputation provide sufficient deterrent from opportunistic behavior. Because legal enforcement is sparse and apparently insufficient, the ability of these conditions to do the same in a privacy policy setting will determine whether intervention is necessary to enforce online privacy. On one hand, if the market for online social media is functioning so as to provide consumers with information and substitutes and sellers with incentives to protect their reputation, then non-legal

145 Several scholars have explored in depth the ability of alternative legal sources to protect privacy. *See, e.g.*, Hotaling, *supra* note 13, at 532.

146 Hashemi, *supra* note 42, at 153.

147 *See* Gunasekara & Toy, *supra* note 87, at 191–92, 213.

148 *See* Hashemi, *supra* note 42, at 159–60 (providing examples of cases in which courts refused to impose tort liability on interactive computer service providers). *Cf.* Hotaling, *supra* note 13, at 549–51 ("[C]ommon law tort remedies . . . apply only indirectly to privacy violations by online advertising companies.").

149 *See, e.g.*, Hillman & Rachlinski, *supra* note 43, at 441–43 ("[C]onsumers' best protection is not the courts, but their own vigilance and acumen.").

sanctions will have saved the day and, according to scholars' hypotheses, no intervention would be necessary.[150] If, on the other hand, the online social media market fails to provide sufficient pressure and other forces to discipline businesses and discourage exploitation, then it will demonstrate that there are indeed certain conditions that must hold for the enforceability of non-legal sanctions, that the exploitation of private information may indeed be a contractual problem, and that intervention is needed to remedy the market failures.[151] This section argues that there are indeed settings in which non-legal enforcement mechanisms cannot function—the online social media setting being an example—because of the failing of prerequisite conditions, and that the privacy problem apparently requires legal intervention.

1. Market Competition

Competition can help curb seller opportunism because sellers' concerns with minimizing costs prevents them from allocating excessive resources to drafting a unique, pro-seller contract, and because consumer bargaining power is strengthened by the possibility that they avoid exploiting sellers and turn to substitutes. Scholars have recognized however, that these fruits of market forces "may not work under all conditions."[152] As an example, in an "insufficiently competitive industr[y where] businesses can afford to lose the small cadre of readers and dictate onerous terms to nonreaders," "market pressure may be insufficient to discipline businesses."[153] The market for online social media may be one such market that lacks sufficient competitiveness. But what *is* the market for online social media, and how can it lack competition when there are so many kinds of social media available?

To understand the online social media market, imagine a group of miners. These miners are equipped with abilities to gather valuable resources from all kinds of mines that they would turn into money by selling to a third party. For purposes of this illustration, assume that this third party has no preference regarding *what* is mined or *how* the miners mine it as

150 *See, e.g.*, *id.* at 478, 480.
151 *See* Hillman, *supra* note 39, at 843.
152 Winter, *supra* note 107, at 280–81.
153 Hillman, *supra* note 39, at 843.

long as they can buy some resource. Though the miners are competing, the diverse varieties of valuable resources available allows them to specialize in mining a particular kind of resource, allowing themselves each to have a metaphorical piece of the pie. In other words, instead of all trying to make mining gold profitable, one miner may mine gold while another mines copper or granite. As a result, though they are competing for the eventual cash receipt for their mined goods, they have the opportunity of doing that competition in a specialized, non-substitutable commodity so that the competition for the actual commodity is minimal.

The market for social networking is not unlike this mining analogy. These social networking sites are after one valuable resource: private information. The private information they mine can in turn be cashed in from third party advertising firms. This is significant because it allows these sites to mask the market. Though different social networking sites may be grouped into the same market, they are competing for private information using different, non-substitutable interfaces to do so.[154] Each interface has its distinct features, sufficiently different from the next to be able to offer unique products and attract a certain crowd.[155] If the user wanted to post videos, photos and use applications to compare friends and rate movies,

[154] Some may argue that there is indeed competition among social networking firms. It is conceded that these social networking firms each want larger pieces of the pie, and will thus try to out-collect other social networking firms. *See* Nicholas Carlson, *Facebook Versus Twitter Is Getting Ugly for Twitter*, BUS. INSIDER, (Aug. 11, 2009, 1:22 PM), http://www.businessinsider.com /facebook-is-crushing-twitter-2009-8. That there is competition among these firms, however, does not preclude the existence of market power. This situation would be no different than bicycle manufactures trying to get auto-driving consumers to switch to bike transportation—though bike and auto products are certainly in two different markets, they are simply different "interfaces" of transportation. Similarly, Facebook and Twitter, for example, may be members of a broad categorization of social networking, but because of the unique interfacing features they promote, they still may have created their own market in which they enjoy market power. *See* Steve Thornton, *Twitter Verses Facebook: Should You Choose One?*, TWITIP (Jan. 13, 2009), http://www.twi tip.com/twitter-versus-facebook.

[155] An internet search of the name of any social network (e.g., "Facebook") "vs." any other social network (e.g., "Twitter") reveals a long list of comparisons between different social networks. For a specific comparison, see Thornton, *supra* note 154. The comparison reports differences between the two so substantial that "a direct comparison between the two is actually difficult to make." *Id.*

Facebook may be the favorite.[156] Meanwhile, if music is the user's main musing, Myspace may come to mind.[157] That consumers treat these sites as offering distinct services is only strengthened by the fact that consumers are unable to identify the common characteristic shared among these sites—their collection of private information.[158] But even if consumers did recognize this fact, the interfaces are sufficiently unique that consumers would still not substitute,[159] thereby creating market power[160] for each distinct social networking firm.[161]

With market power, firms would have even greater

[156] *See* Nick O'Neill, *The Top 25 Facebook Applications*, ALL FACEBOOK (Oct. 22, 2007, 5:20 PM), http://www.allfacebook.com/the-top-24-facebook-applications-2007-10; Thornton, *supra* note 154.

[157] *See* Erik Sherman, *MySpace vs. Facebook: The Fight Isn't over*, BNET (Jan. 4, 2011), http://www.bnet.com/blog/technology-business/myspace-vs-facebook-the-fight-isn-8217t-over/7659.

[158] The fact is that users have erroneous beliefs about privacy policies—they "believe they have more privacy simply because of the proliferation of privacy policies. One survey found that 75% of consumers believed that just because a site has a privacy policy, it is not allowed to sell to others the personal information customers disclosed to it." *See* Haynes, *supra* note 34, at 611 (citing JOSEPH TUROW, ET AL., ANNENBERG PUB. POLICY CTR. UNIV. OF PENN., OPEN TO EXPLOITATION: AMERICAN SHOPPERS ONLINE AND OFFLINE 3 (2005)). Generally, users are not aware of the "intricate details of . . . privacy polic[ies]." Hashemi, *supra* note 42, at 154.

[159] The website, http://www.twitip.com/twitter-versus-facebook/, discusses the advantages and disadvantages of either Twitter or Facebook and concludes that each might "appeal more to different types of people and for different reasons." Steve Thornton, supra note 154. The sentiment of the report is that the sites are sufficiently different that based on what one is "trying to accomplish in a given situation," the networks have different uses and are not substitutes. *Id.*

[160] High substitutability indicates market power because it essentially is a manifestation of a narrow market. *See, e.g.,* William M. Landes & Richard A. Posner, *Market Power in Antitrust Cases*, 94 HARV. L. REV. 937, 948 (1981) (asserting that typically, when defining the product market, product substitutability plays a significant role in that determination). Thus, the market power that these social networking sites have derives from the narrow interface market these firms are actually in.

[161] Even if each distinct social networking firm did not have market power, Facebook certainly has. With 78% of all social media traffic, Facebook has emerged as the dominant firm in the social networking arena. Eunju Lie, *When it Comes to Marketing, Twitter Destroys Facebook*, BUS. INSIDER (Dec. 13, 2010, 10:29 AM), http://www.businessinsider.com/twitter-destroys-facebook-2010-12. While this note assumes for the sake of argument that other social networks are able to create their own market with a unique interface, even if this assumption failed, this discussion about the effects of market power on non-legal sanctions could still take place by observing Facebook alone. Nevertheless, this note continues to assume that social networking firms, because of their unique interfaces, do have some degree of market power.

opportunities to exploit users if users would have nowhere else to turn, and nothing with which to substitute the product they offer. There would be no competitors and no threat of consumer leaving that could curb a monopolist's incentives to mine as much private data as they please.[162] Some argue, however, that even if a firm did have monopoly power, that monopolist would simply charge a higher price instead of exploiting consumers with pro-seller terms.[163]

But in the social media setting, what is that price? The price is the very thing that is exploitative: private information. The price that users are paying to use the online services is the information that they provide the sites when they use them. A monopolist's higher price then becomes terms that permit even greater exploitation because consumers are "paying" with their information.

This confirms the notion that there may be some instances in which competition fails to adequately provide a deterrent effect. This section has demonstrated that not only does insufficient competition fail to discipline businesses, but market power arising from substitutability problems may also increase opportunities for opportunism. This also illustrates how, within the framework of online social media and governing privacy policies, the enforcement mechanisms that would otherwise justify enforceability and a non-interference approach for clickwrap agreements fail to offer sufficient protection to consumers exposed to privacy invasion.

2. Asymmetric Information

Information imbalance is another feature that the market for fair online social media agreements has failed to provide. There are several kinds of asymmetric information in this market: (1) failure to read provided information about the agreement; and (2) failure to appreciate the risk of loss of private information.

The first information imbalance is not unique to online social media. Found generally in clickwraps and other e-contracts, asymmetric information exists where consumers fail to read agreements to which they allegedly consent.[164] Writers have

[162] *See generally* Bebchuk & Posner, *supra* note 67, at 831–32 (discussing one sided contracts and individual protections).

[163] *Id.* at 828–29.

[164] *See generally* Sovern, *supra* note 37, at 1657–60 (citing studies and websites where a large amount of people do not read the agreements into which

speculated and tried to explain this phenomenon in many different ways, claiming that it is possibly because consumers lack sufficient cognitive ability to understand the terms or to appreciate the responsibility,[165] because consumers lack incentives to invest the time required to understand the terms of e-contracts,[166] because of social pressures and a free-rider problem,[167] or just because online consumers are generally click-happy.[168] Regardless, the failure of consumers to read their agreements "undermines market pressure to provide mutually beneficial terms."[169]

And firms know this. There not only exists this unfair bargaining arrangement, but firms are in a unique position to keep it that way by imposing additional transactions costs on users.[170] By keeping the print size of agreements small, by tucking the agreements away or by including legalese in the agreements, firms have the incentives and opportunities to impose additional costs on users to keep them from investing in research about the agreement.[171] And the transaction costs of information transmission can reach a level high enough to make efficient exchange achievable.[172] So not only do consumers already not care to read their agreements, but firms can also make it worse, both of which make exploitation more likely.

But this instance of asymmetric information does little to advance the argument that the market for fair agreements in the online social media setting is any different, or that it deserves

they enter).

165 Hillman & Rachlinski, *supra* note 43, at 450–51.

166 *Id.* at 486.

167 *Id.* at 447.

168 *See* Gindin, *supra* note 61, at 49. The fact that users are "click-happy" indicates their tastes and preferences about speed and convenience.

169 *See* Hillman & Rachlinski, *supra* note 43, at 454.

170 *See* Sovern, *supra* note 37, at 1641–43. Sovern discusses conditions that must hold in order for it to be more likely that a firm would impose transaction costs on users. It was Sovern's argument that it may not be likely that firms will try to impose increased transactional costs on users. Because of the uniqueness of the social networking market, those conditions arguably hold. As a result, according to Sovern, firms in the social networking market will indeed try to impose transaction costs on their users, as it is argued here.

171 *See id.* at 1640–42.

172 *See* Robert E. Scott, *The Case For Formalism in Relational Contract*, 94 NW. U. L. REV. 847, 863 (2000) ("If transactions costs are preventing the parties from completing contracts with efficient terms, then the state properly should fill the gaps with default terms that solve those problems whenever the state's contracting costs are lower than the contracting costs to the parties.").

any more attention than the rest of the e-commercial realm. In fact, despite this information imbalance, and notwithstanding other possible loopholes, courts have still upheld these agreements as arms-length and enforceable.[173] This might be so not only because a combination of legal and non-legal sanctions can contribute to counterbalancing the imbalanced information, but also arguably because consumers are getting what they bargain for. In exchange for the opportunity to use cool websites, consumers are offering up their private information.[174] Or so it seems.

That argument—that consumers are willingly bargaining with their private information in negotiations for website use—is flawed because of an erroneous conception of the "exchange." What makes the privacy policy setting still different from other e-contracts, and thus furthers the argument for intervention in this setting, is another type of asymmetric information—the information regarding the information that users are giving up to enter into the contract and use social media. Specifically, users are very likely not to know that their information is being sold, and therefore cannot appreciate the risks of entering into these e-agreements.[175] What users believe about the information they are providing and what websites know about what happens to this information could not be more at odds. Users are simply not aware of the possibility that their information is being sold, or being transferred to third-parties. In fact, a recent poll indicates that almost one in every four Facebook users did not even know anything about privacy settings at all.[176] And this is only one indication that users simply do not have enough information about the agreements to appreciate the risks of using online social media.

Because they cannot appreciate the risks of entering into these agreements, they cannot take precautions that parties of other

---

[173] *See id.* at 863–64.

[174] Eric Gertler, *Privacy Does Matter*, HUFFINGTON POST (June 21, 2010, 8:24 AM), http://www.huffingtonpost.com/eric-gertler/privacy-does-matter_b_619173.html (asserting that "many . . . argue that consumers willingly part with their information with little thought or concern").

[175] If users are not even aware of the significance of privacy policies and moreover erroneously believe that the mere presence of such will actually protect their information, then users are certainly not going to be aware that their information is being sold. *See generally* Clippinger, *supra* note 2 (showing that many users are not even aware that privacy agreements exist or that they are entering into these e-agreements).

[176] *Id.*

agreements could take. The purchaser of a toaster, for example, is aware of the risk that the toaster will fail to operate as advertised, will cause harm, or any other risks associated with purchasing and operating a toaster. Consequently, the consumer can take necessary precautions against those risks, whether it is by purchasing insurance or by relying on product warranties. On the other hand, consumers of online social media may not even know that they are getting a toaster (or that they are getting anything), and if they do, they have no idea what a toaster does, and what risks are associated with using it.[177] In this situation of online social media, then, where users may not know that an exchange has taken place, the internet is in a "'classic . . . market failure,'" and intervention could be warranted.[178]

3. Reputation Considerations

Similar to generic e-contracts, privacy policies may also be subject to and checked by the reputation non-legal sanction; the threat of a wronged consumer tarnishing the reputation of a defecting seller would theoretically be enough to discourage seller opportunism. But scholars have recognized that there is "significant space" for opportunism if the likelihood of reputational redress was sufficiently remote, where sellers would consequently "face little downside risk from efforts to exploit."[179] As this section will explain, sellers in the online social media market do face only a remote risk of reputational redress.

First, consumers lack sufficient opportunities themselves to provide a counterbalancing disincentive for sellers to not exploit consumers. This note argued above that if consumers are not aware of the exchange that is occurring, that they cannot know of or appreciate the risks of the exchange.[180] Consequently, they could not take precautionary measures to protect themselves against the risk by purchasing insurance, or ensuring the existence of warranties, etc. One other consequence of risk blindness is that consumers would be unable to be on notice to investigate a seller's reputation, or, in the case that one of the risks comes to fruition, would be unable to damage the seller's

[177] Many users simply have erroneous beliefs about what privacy policies do. *See* Hillman & Rachlinski, *supra* note 43, at 466–67.

[178] Terenzi, *supra* note 5, at 1095 (citing Joel R. Reidenberg, *supra* note 28, at 775).

[179] Gillette, *supra* note 110, at 978.

[180] *See* discussion *supra* Part III.C.b.

reputation in the same way that a disgruntled buyer of a faulty toaster could.

Secondly, even if consumers did have information about risks and could damage the seller's reputation, which, in some few instances they have, reputation considerations are less significant because of sellers' monopoly power.[181] Because consumers may hesitate to substitute away from their preferred social network, these networks may not put as much weight on reputation as a firm in a truly competitive market would otherwise.

A few examples may illustrate how social networking sites may be immune to reputational backlash. Take, for example, Facebook's "Beacon" program that it launched in 2007. The Beacon program tracked a Facebook user's Internet activity and published certain of these activities on that user's Facebook page.[182] This way, even if the Facebook user was not then logged onto their Facebook account, Facebook exchanged information between the partner site and disseminated through Facebook.[183] After over a year of consumer and outsider complaining of the program, Facebook finally cancelled it.[184] But even if consumers won the battle, Facebook is still winning the war—even after responding to consumer complaints about this and similar programs, Facebook maintains that users must "opt out" of its more favorable settings, rather than having a consumer-friendly "opt in" default.[185] From the implementation and eventual cancellation of this program, observers are able to draw several conclusions about Facebook's market power, consumer ignorance and the immunity of Facebook's reputation.

This example demonstrates the ease with which Facebook can quickly, and perhaps even with subtlety change its privacy policy

---

[181] A tarnished reputation imposes costs on a party, but if the costs of a bad reputation are imposed on a monopolist, the monopolist will likely be able to bear it more than a non-monopolist. Because the monopolist is charging supra-competitive prices (where the competitive price is at marginal cost), increasing the monopolists' costs would only shave its profit margin, but would not likely destroy the firm as it would one in a competitive market. As one scholar has said, "a monopolist might prefer a tarnished reputation than competition." Maurice E. Stucke, *How Do (and Should) Competition Authorities Treat a Dominant Firm's Deception?*, 63 SMU L. REV. 1069, 1102 (2010).

[182] Terenzi, *supra* note 5, at 1069–70.

[183] *Id.*

[184] *Id.*

[185] *Fleeing Facebook*, ECONOMIST, June 3, 2010, http://www.economist.com/blogs/babbage/2010/06/techview_social_network_redux.

terms to include language permissive of a more intrusive and invasive program.[186] Granted, there was a significant backlash against the Beacon program; consumers indeed complained that the changes encroached on their privacy. But one popular means of voicing disdain with the changes was, ironically, Facebook itself![187] What this demonstrates is that even if people know about a site's tendency to exploit their private information, the consumers may want the social networking experience more than they want to protect their privacy. To be fair, there may be people that voice their opinion on Facebook—because nowhere else would being heard about Facebook be more relevant than on Facebook—and then later defect, leaving the site completely. In fact, there were indeed several thousand users that eventually did leave the site during the time that the Beacon program was used.[188] But a few thousand lost users is not a great loss when it is coming from a pool of millions.[189] What about the other users that continued to use the site's services? Either they did not even know the differences, or they knew, but continued to use anyway—facts that amplify everything this note has indicated about consumer ignorance and about the immunity of Facebook's reputation.

One last conclusion is regarding the time that had passed before Facebook finally cancelled the Beacon program. As mentioned, over a year had passed from Beacon's implementation to cancellation. Specifically, why the cancellation of a remarkably unpopular program required such a long time is a matter of speculation, but it may be reasonable to posit that it was because either users were not becoming aware of the invasion fast enough, or that, perhaps more importantly, Facebook just did not have to make any changes because it was

[186] The ability to change a privacy policy without notice would not be unprecedented. Google, for example, has reserved the right to change its policy, or specifically, to share information for a supposed "'better experience.'" This is in spite of the fact that Google elsewhere that it will never rent, sell or share private information without permission. By allowing themselves this right to share information, they ensure that the possibility of sharing information is not ruled out. *See* Goldberg, *supra* note 4, at 254–55.

[187] Terenzi, *supra* note 5, at 1069–70.

[188] *Id*.

[189] "Facebook is the most popular social networking destination online, reaching a whopping 35% of all Web users. Nearly 500 million people worldwide have joined the social network." Anna Palmer, *Where Are Facebook's Friends on K Street?*, CNN MONEY(June 9, 2010, 12:29 PM), http://tech.fortune.cnn.com/2010/06/09/where-are-facebooks-friends-on-k-street/.

not suffering too greatly. Perhaps over a much longer period of time, the site may have seen greater amounts of defects. But a reaction this delayed is not the action of a site that is truly dependant on a good and favorable reputation to survive in the market.

The Beacon program is not the only time Facebook has implemented unpopular policy changes. In recent years, Facebook has developed and expanded the public accessibility of its users' private information through the indexing of information of Facebook.[190] This way, one's private profile information could appear on search results on public search engines. Here, too, there has been backlash, but at least as of the date of this note's composition, the searching for the author's name on Google yields results on Facebook (as well as on LinkedIn, Twitter and MySpace, who have apparently all followed Facebook's suit), indicating that Facebook can choose to ignore widespread criticism. Despite this criticism, there is no indication that these changes have resulted in any slowing of the network's growing popularity.[191]

The breaking down of non-legal reputational sanctions exposes consumers to seller opportunism and the market could thus be ripe for intervention. In fact, especially when transactions costs are high or when parties have limited information about the exchange, as in these cases, legal intervention may "improve transactors' welfare."[192] Intervention can increase welfare not only by promoting contracting that maximizes joint benefits, but also by preventing some parties (e.g., social networking sites) "from acting during the course of the relationship in ways that benefit themselves but that result in a net social loss."[193]

To conclude this section, current legal enforcement of contracts to protect privacy is spotty at best and must thus rely on non-

[190] Terenzi, *supra* note 5, at 1070–71. *See also* Ian Paul, *Facebook's Privacy Settings: 5 Things You Should Know*, ABC NEWS (Dec. 12, 2009), http://abcnews.go.com/Technology/GadgetGuide/facebooks-privacy-settings-things/story?id=9312771 (indicating that on December 12, 2009 the author found that the option to index his profile through public search engines had been turned on in his privacy search settings on Facebook despite the fact that he had previously turned off the setting).

[191] *See* Palmer, *supra* note 189 ("Facebook is the most popular social networking destination online, reaching a whopping 35% of all Web users. Nearly 500 million people worldwide have joined the social network, and all this talk about privacy isn't slowing its growth -- not yet, anyway.").

[192] Charny, *supra* note 89, at 430.

[193] *Id.* at 432.

legal enforcement mechanisms. And while other e-contracts could have relied on these mechanisms to supplement spotty legal protection, there are conditions that must hold in order for the market to be able to provide effective non-legal sanctions. Causing a breach in privacy, those conditions do not hold in the online social media market in particular. Specifically, a lack of competition, asymmetric information and reputation immunity all contribute to social networking sites' ability to take advantage of the opportunities that many online sellers have to exploit consumers for their own gain. Because of the failures in this market, intervention is thus needed. The types of intervention that have been proposed, along with this note's proposed method of curing the markets' failures, are in the next section.

V. PROPOSED INTERVENTION

Writers and scholars have devised a variety of proposals that they suggest might repair the privacy problem. There is much good to say about a lot of these approaches; proposed legislative action, administrative action or self-regulation ideas all have some merit. But none of these approaches have come at the problem from the angle of fixing the underlying problem: the market failures. Legislative-inspired proposals might over-intervene in the market, while self-regulative measures would leave the market failing with patchy incentives. No current proposal would enhance competition among competitors; would inform users of the risks of using certain online services; or would make firms more susceptible to reputation damage. This paper, therefore, proposes that the government adopt a minimalist approach[194] to merely fix the failure of the market to provide adequate safeguards for privacy.

The root problem of the market failures that intervention would need to remedy is associated with the transaction costs in agreeing to terms of use (including privacy) between a user and a website.[195] The market is not providing users with incentives to

[194] A minimalist approach might be preferred because, according to some, over-intervention can stifle entrepreneurship and innovation in the industry. Jerome & Kollipara, *supra* note 37.

[195] The market failure is consumers' failure to read the agreements—a failure which "undermines market pressure to provide mutually beneficial terms." Because the market is not providing the appropriate incentives, consumers are not apprised of associated risks, sellers are not checked by reputational constraints, and sellers have no reason to compete on the minimization of those risks for consumers. Hillman & Rachlinski, *supra* note

read the contract; is not properly notifying users of the risks associated with entering into the agreement; and is not incentivizing sellers to benevolently inform consumers of the risks, or to at least avoid exploiting consumers. The market has also developed in such a way that sellers are relatively immune to reputational damage, further weakening consumer positions. Therefore, the market requires appropriate incentives and options for both consumers and sellers.

The proposed solution is to grant the FTC authority to force the "exchange" associated with establishing terms of site privacy policies and agreements. It would not be an FTC first to regulate consumer choice and seller behavior—the national "Do Not Call" registry that the FTC enforces could be a type of this kind of regulation. But this market-failure-fixing solution would not necessarily exactly follow a registry format to take the form of a "Do Not Track" list, as some have proposed.[196] Because the industry depends on information to survive, giving consumers the final authoritative say without consequences, the industry would eventually fail.

Instead, the proposed forced exchange takes the middle ground. Some already argue that consumers are choosing to sell their private information when they agree to the terms of a website and enable themselves to use its services.[197] This argument may work except for when, as mentioned above, many, many users do not even realize they are in fact selling that information or when competitive pressures do not exist.[198] Therefore, the FTC could facilitate both the exchange of information (notifying consumers of the risk) and the exchange of

43, at 454.

[196] One poll indicates that people would favor a proposal from privacy group to create a "Do Not Track"' list akin to the "Do Not Call" list. This note's proposed solution would cater to those public demands because it would allow users to elect to not have their information tracked. Unlike the recipients of unwanted phone calls that can place themselves on the "Do Not Call" list, though, Facebook users are getting a service out of the very thing they want to stop. In other words, they are trying to have their cake, and eat it too. Therefore, this note's approach, however, takes a step back from a final "Do Not Track" requirement and would require something in exchange for the cessation of tracking. Gruenwald, *supra* note 26.

[197] *See* Hillman & Rachlinski, *supra* note 43, at 453–55 ("Courts recognize that standard-form transactions do not involve the required 'bargain'" but "understand that despite the lack of bargaining, competitive market pressures might ensure that standard-form provisions include a mutually beneficial exchange.").

[198] *Id.*

private information and of services by mandating that websites give users a choice. Either users can "sell" their private information—meaning the user permits the website to sell a limited type or amount of private information to those that they would normally sell that information—in exchange for the free use of their website. This is similar to the way social networking sites are currently set up, only giving consumers a choice provides assurance that consumers are on notice of the information they are selling. Otherwise, more privacy-minded users can pay some usage fee—an amount that the site would set as being approximately equal to the amount that that user's private information would otherwise be worth—in exchange for the use of the site. Essentially, this is quantifying the value of a marginal user's private information, and by doing so, this allows users to have the option just described.

This method could efficiently correct the problems and failures that this note has outlined. First of all, this still allows Facebook and other online social networking sites to operate predominately in the same fashion as they were before and without much government intrusion or intervention, avoiding a possible net negative effect of protection of consumers.[199] Second, this method produces a system that is more conducive to notifying consumers of the risk of e-contracting. When consumers see that they have an option and must choose between privacy-invading and a limited-privacy option, they are almost certainly put on alert that privacy is at issue, and that losing privacy is otherwise a risk of using certain online services. Finally, this system could be conducive also to competition among websites based on the terms of the policy. Where consumers would otherwise not invest in costly investigation and comparison of e-contract terms, consumers here could see the highlights of the terms (e.g., price, and private information that would be forfeit) with comparable ease. This would allow them to be able to compare terms with very little cost and effort. Further, competitors could offer competitive rates for their invasion-free plan usage rates, or

199 *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS, PRELIMINARY FTC STAFF REPORT 40–41, 58–59 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; s*ee also* Winter, *supra* note 107, at 257–58 (arguing that that if too many electronic contracts are struck down, firms will withdraw from the market. While this may not be possible, it at least indicates that there may be negative effects of over-protection); *see also* Terenzi, *supra* note 5, at 1069–70.

could likewise offer free service for more and more limited intrusions. By opening up this market to more robust competition, the market may more naturally cure its failures, with little to no further regulative intervention.

While enforcement[200] could be more involved than the simple theoretical forced "exchange," this proposal would still be able to correct the markets failures as the root causes to the inadequacies of non-legal enforcement mechanisms. As a result, the contract-based privacy policies would be able to afford consumers a greater degree of protection.

VI. CONCLUSION

This note has explored e-contracts in their various forms, and identified how e-contracts are enforced despite weakened consumer bargaining positions. With a framework of why and how general clickwrap agreements are enforced so that sellers do not exploit weakened consumer positions, this note then tried applying those enforcement mechanisms in the privacy setting in order to determine whether the concern over privacy was warranted, and whether intervention was needed. As it turns out, because of a lack of competition, asymmetric information and the reputational immunity of firms in this niche market, those enforcement mechanisms are less effective in protecting consumers and their privacy. Because of the failure of in-place mechanisms to do their job, government intervention is warranted. The most effective type of intervention is that which is aimed directly at curing the failures that makes intervention necessary. This can be accomplished by a system that the FTC would administer that would provide consumers with option of either turning over cash or their private information in order to use online services. This would minimize intervention in

[200] While the FTC could administer this system in a manner similar to the "Do Not Call" system and then enforce it by the FTC's Enforcement Division (which "litigates civil contempt and civil penalty actions to enforce federal court injunctions and administrative orders in FTC consumer protection cases") the most difficult aspect of enforcement would be detection. *Division of Enforcement*, FED. TRADE COMM'N (Nov. 15, 2010), http://www.ftc.gov /bcp/bcpenf.shtm. Unlike unwanted phone calls to numbers on the "Do Not Call" list, the average consumer would not be able to detect unauthorized tracking. The FTC would thus have to devise methods that could facilitate tracking of these sellers. Given that the very behavior that would be eliminated would be tracking, the technology is likely available and not difficult to implement.

commerce, notify consumers of the risk of entering into the agreements, and promote more robust competition in the market.