1-1-2012

"Do-Not-Track" as Contract

Joshua A.T. Fairfield
Washington & Lee University School of Law, fairfieldj@wlu.edu

"Do-Not-Track" as Contract

Joshua A.T. Fairfield[*]

> Individual liberty is individual power, and as the power of a community is a mass compounded of individual powers, the nation which enjoys the most freedom must necessarily be in proportion to its numbers the most powerful nation.
>
> -John Quincy Adams, Letter to James Lloyd October 1, 1822[1]

ABSTRACT

Support for enforcement of a do-not-track option in browsers has been gathering steam. Such an option presents a simple method for consumers to protect their privacy. The problem is how to enforce this choice. The Federal Trade Commission (FTC) could enforce a do-not-track option in a consumer browser under its section 5 powers. The FTC, however, currently appears to lack the political will to do so. Moreover, the FTC cannot follow the model of its successful do-not-call list since the majority of Internet service providers (ISPs) assign Internet addresses dynamically—telephone numbers do not change, whereas Internet protocol (IP) addresses may vary.

This Article explores whether, as a matter of contract law, a browser do-not-track option is enforceable against a corporation, and concludes that it is. The emerging standard of online consent has been whether a party proceeds with a transaction after the counterparty informs the party of the terms of the contract. Adhesion contracts in electronic contexts have bound consumers for over a quarter century in precisely this manner.

This Article argues that what applies to consumers should apply to corporations. When a consumer expresses her preference, in the very first exchange between the consumer and corporate computers, for the corporation not to track her information, the company is free to refuse the transaction if it does not wish to continue on the consumer's terms. This Article therefore proceeds in three broad parts. Part I

 The Author is an Associate Professor of Law and

1. *See* Daniel W. Sutherland, *Homeland Security and Civil Liberties: Preserving America's Way of Life*, 19 NOTRE DAME J.L. ETHICS & PUB. POL'Y 289, 302 n.39 (2005).

introduces the current methods of corporate surveillance of consumers, which have reached dizzying heights. Part II discusses the law of e-commercial and mass-market contracts, which courts have held to bind consumers even on the merest fig leaf of a legal theory of consent. Part III proposes a solution: the answer is not to continue making consumers read more privacy policies on various websites, but instead to enforce the simple preferences that the consumer expresses once.

TABLE OF CONTENTS

This Article asks whether, as a matter of contract law, a court can enforce against a corporation a do-not-track option selected in a consumer's browser.[2] Currently, this approach is under theorized in the legal literature.[3] This Article concludes that courts can enforce

2. For purposes of this Article, tracking is the identification, storage, and analysis of who you are, where you are, and what you do online. *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1845 (2011) (discussing tracking online in the context of personally identifiable information).

3. *See* Dustin D. Berger, *Balancing Consumer Privacy with Behavioral Targeting*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 3, 17-27 (2011) (outlining the problems of behavioral advertising on consumer privacy and the needed regime of broad mandatory regulation combined with an audit requirement to address the root causes of the potential harm); Julie Brill, *The Intersection of Consumer Protection and Competition in the New World of Privacy*, 7 COMPETITION POL'Y INT'L 7, 7 (2011), *available at* http://www.ftc.gov/speeches/brill/110519CPI.

consumer privacy preferences using fairly mundane contract law principles,[4] and more importantly, concludes that courts should enforce consumer preferences, since this is an important method of returning control over private information to citizens.[5] This Article

---

pdf (explaining how the FTC might balance consumer protection concerns, such as do-not-track arising in the context of privacy, with competition issues); Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1650 (2011) (discussing the role of website design in contracting online and how it should be part of an online agreement when it is incorporated into or consistent with the terms of use); Matthew S. Kirsch, Note, *Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising*, 18 RICH. J.L. & TECH. 2, 54-74 (2011) (discussing the upcoming revision of the European Union's Data Protection Directive and how it should require advertisers to use and respect a do-not-track mechanism for consumers to meaningfully consent, or not, to online tracking for use in behavioral advertising); Tracy A. Steindel, Note, *A Path Toward User Control of Online Profiling*, 17 MICH. TELECOMM. & TECH. L. REV. 459, 466-84 (2011) (discussing the problem of online tracking for consumers and the problems that can arise, and how a do-not-track browser option should be implemented in federal legislation to protect consumers).

> Adoption of online privacy policies could facilitate a market-based licensing approach to personal data protection. When Web sites post notices saying personal data will not be collected, disclosed, or used except for named purposes, users who supply data in reliance on those restrictions may be able to enforce the restrictions. A market-based licensing approach may also arise if technology evolves to allow 'negotiated' agreements on the collection, use, or disclosures of personal data.

Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1129 (2000).

4. *See* discussion *infra* Part III.B. This discussion highlights an important distinction with the literature above. This Article argues for a simple and unitary do-not-track option that courts can enforce as a matter of contract law. The options presented rely on federal legislation or the FTC directly. Federal legislation may be watered down in order to balance competing interests, and the FTC does not seem willing as of yet to move forward, an option it is considering is a repeat of a prior failed effort. *See* Declan McCullagh, *FTC Official: Do Not Count on Do Not Track Just Yet*, CNET NEWS (Oct. 20, 2011, 9:00 AM), http://news.cnet.com/8301-31921_3-20123158-281/ftc-official-do-not-count-on-do-not-track-just-yet (discussing different approaches by two different FTC commissioners and that there is no time table for any immediate action); *see also FTC Says Significant Steps Made For DNT—Still Work To Be Done*, FUTURE PRIVACY FORUM, http://www.futureofprivacy.org/2011/10/18/ftc-says-significant-steps-made-for-dnt-still-work-to-be-done (last visited Dec. 21, 2011) [hereinafter *FTC Significant Steps*] ("FTC Commissioner Julie Brill spoke at the Online Trust Alliance (OTA) Forum today and noted . . . . 'I don't see this as a toggle switch-on or off,' but rather 'a place where consumers can choose through a dashboard mechanism what they want . . . .' She further stated that the World Wide Web Consortium (W3C) Tracking Protection Working Group is working around issues like 'what does tracking mean' and other technical issues.").

5. Courts do not currently enforce consumer preferences because the balance of favor is in corporate hands with technological solutions. *See* Emily Steel, *FTC's Proposed Changes to Web Privacy Rules Give Parents More Control*, WALL ST. J., Sept. 16, 2011, http://online.wsj.com/article/SB10001424053111903927204576573021939728718.html ("'The Internet revolution makes snapshot photography and wiretap technology look like child's play,' FTC Commissioner Julie Brill said . . . . As proof that the use of consumer data is wading into dangerous territory, Ms. Brill cited a 2010 story from the Wall Street Journal's 'What They Know' series on online privacy issues about a life insurer that used tracking data about consumers to help determine their life expectancy, rates and insurance coverage."); *see also* Scott Thurm & Yukari Iwatani Kane, *Your Apps are Watching You*, WALL ST. J., Dec. 17, 2010, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html ("An examination of 101 popular smartphone 'apps' . . . . reveal the intrusive effort by online-tracking companies to gather personal data . . . . Smartphone users are all but powerless to limit the tracking. With few

also asks the deeper question of whether courts can succeed in protecting consumers solely by construing corporate-drafted contract terms. The Article argues that they cannot: a corporate-drafted contract will still favor the corporation on balance,[6] no matter what tools of interpretation or equity a court brings to bear.[7] On the contrary, the modern tools of automated contract formation should be available to the consumer and corporation alike. Courts therefore can and should enforce consumer-offered contract terms—such as the preference not to be tracked—as part of a broader effort[8] to restore balance to online contract law and the consumer information market.

Corporations constantly track US consumers.[9] This consistent and pervasive surveillance means that consumers are easily tracked

---

exceptions, app users can't 'opt out' of phone tracking . . . ."). Cookies are small pieces of code installed on a user's computer or smartphone that allow third parties to identify a computer so that they can save information, such as a password or login name, or track user information. *See* Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 271 (2008) (detailing what cookies are and how they work).

6. *See* Charles L. Knapp, *Opting Out or Copping Out? An Argument for Strict Scrutiny of Individual Contracts*, 40 LOY. L.A. L. REV. 95, 101-05 (2006) (discussing how dominance of the drafter has become typical in contract law and mentioning certain defenses such as unconscionability or duress as potential defenses to abiding by standardized form contracts that are simply accepted by consumers without negotiation); Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 459 (2006) ("Today, by contrast, more and more courts and commentators seem willing to accept the idea that if a business writes a document and calls it a contract, courts will enforce it as a contract even if no one agrees to it.").

7. ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1452 (7th Cir. 1996) ("A vendor, as master of the offer, may invite acceptance by conduct, and may propose limitations on the kind of conduct that constitutes acceptance. A buyer may accept by performing the acts the vendor proposes to treat as acceptance."); Fisher v. MediSense, Inc., No. 95-1004-PFK, 1995 WL 396613, at *6 (D. Kan. June 29, 1995) ("Undue influence is not proven, nor is a contract unconscionable, merely because a corporation drafts a contract."); *see also* Knapp, *supra* note 6.

8. *Compare* Susuk Lim, Litigation, *Death of the Spam Wrangler: CAN-SPAM Private Plaintiffs Required to Show Actual Harm*, 6 WASH. J.L. TECH. & ARTS 155, 167 (2010) ("One of CAN-SPAM's stated aims is to address the states' disparate standards for commercial e-mail, which it found to be incompatible with the geographically independent nature of e-mail."), *with* Marc Lifsher & Jessica Guynn, *Online 'Do Not Track' Bill Introduced in California Senate*, L.A. TIMES, Apr. 6, 2011, http://articles.latimes.com/2011/apr/06/business/la-fi-do-not-track-20110406 ("[P]roponents of do-not-track laws point to California's 2002 passage of a do-not-call telemarketing bill as a precedent. However, the California law never took effect because the federal government issued its own do-not-call regulations in mid-2003."), *and* S.B. 761, 2011-2012 Leg. Reg. Sess. (Cal. 2011) ("This bill would require the Attorney General, by July 1, 2012, to adopt regulations that would require online businesses to provide California consumers with a method for the consumer to opt out of the collection or use of his or her information by the business.").

9. *See* 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, 11 (2009) ("Although behavioral tracking has typically been reported to be anonymous, there are indications that information collected online is being combined with data collected offline."); *see also* James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 2 (2003) ("Americans have only the vaguest idea how much of their lives is

everywhere they go, even as they move from one website to another.[10] Consumers are even tracked offline.[11] Because cell phones are miniature Global Positioning System (GPS)-enabled tracking devices,[12] corporations can often gain detailed pictures of where consumers go in real space and can correlate that information with consumers' online behaviors.[13] In short, there is no longer any place to hide, online or off. A number of different companies—ranging from Google to Internet service providers (ISPs) to smartphone application providers to data brokers and marketers—gather, index, sell, and resell all of American consumers' data.[14]

The Federal Trade Commission (FTC) has suggested a do-not-track list that would follow the model of the successful federal do-not-call list.[15] This list would be an important step forward in permitting consumers simple, unitary, and default controls over their personal privacy. Several bills are before Congress concerning

---

recoded in databases . . . . the widespread and fast-growing data aggregation industry, and the harm that can result from information collection and sharing.").

10. Nehf, *supra* note 9, at 20 ("When a user explores a site, the user leaves electronic footprints behind. By following the footprints, the site can record information about the user . . . . The site can also record . . . the website previously visited . . . .").

11. *See* Gindin, *supra* note 9; *see also* Bob Tedeschi, *E-Commerce Report; Critics Press Legal Assault on Tracking of Web Users*, N.Y. TIMES, Feb. 7, 2000, http://www.nytimes.com/2000/02/07/business/e-commerce-report-critics-press-legal-assault-on-tracking-of-web-users.html ("DoubleClick . . . has begun adding information about consumers' offline behavior to its huge database. . . . DoubleClick . . . has [also] begun combining its online data with information gleaned from consumers offline purchases from major retailers, catalog companies and publishers.").

12. *See* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 713 (2011) ("Increasingly, smart phones come equipped with GPS locators . . . . Even traditional cell phones, without Internet capabilities, now include GPS technology so that providers may comply with federal regulations requiring them to pinpoint locations during emergency calls.").

13. *See* Nehf, *supra* note 9, at 20 ("Many websites secretly track a customer's surfing practices through the use of 'cookies' and similar technologies."); *see also* Tedeschi, *supra* note 11.

14. *See, e.g.*, Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 362 ("Acxiom, is 'a billion-dollar player in the data industry . . . .' [and] provides information to marketers for profiling consumers, manages credit records, sells data for background checks, and provides data to government agencies . . . ."); Thurm & Kane, *supra* note 5 (discussing mobile app tracking); *Advertising and Privacy*, GOOGLE, http://www.google.com/privacy/ads (last visited Nov. 8, 2011) ("To serve ads in applications and other clients where cookie technology is not available, we have engineered an anonymous ID by associating your device ID with a random, anonymous string of characters. You may choose to reset or opt out of anonymous IDs at any time. . . . The ads that appear with search results on Google can be personalized based on your Google Account or customized for your web browser. Using previous queries and Web History can help us provide more relevant ads to you.").

15. *See FTC Testifies on Do Not Track Legislation*, FTC (Dec. 2, 2010), http://www.ftc.gov/opa/2010/12/dnttestimony.shtm. This was done at the urging of Congress. *See* Do-Not-Track Online Act of 2011, S. 913, 112th Cong. (2011) ("To require the Federal Trade Commission to prescribe regulations regarding the collection and use of personal information obtained by tracking the online activity of an individual, and for other purposes.").

do-not-track efforts and data privacy.[16] However, these bills are not focused on a unitary do-not-track option enforceable by the consumer herself. There is promise in the proposed Consumer Privacy Bill of Rights (CPBOR) by the White House, which suggests that consumers should have the option to withdraw their information from use by corporations.[17] The focus of the CPBOR is on collaboration between consumers, corporations, and other stakeholders. The CPBOR suggests new legislation, or new industry codes of conduct.[18] Government-brokered industry self regulation will almost inevitably yield the same results that industry self regulation has produced to date—consumers bear all the cost of protecting their privacy. This Article outlines how contract law might provide relief for consumers who seek to protect their data.[19]

This Article notes one problem of terminology that is both important to clarify and revelatory of the problem. When one says "corporate contracts," it is clear that the contract is offered by and entered into by a corporation. But when one says "consumer contracts" in this field of academic inquiry, it almost never means "contracts written by consumers," but instead means only those entered into by consumers.[20] As most often used in the contracting literature, "consumer contracts" actually means the same thing as "corporate contracts." This usage reveals the basic problem: consumers under modern contracting regimes generally cannot offer their own terms and expect courts to enforce them. This Article seeks

16. *See, e.g.*, S. 799, 112th Cong. (2011); H.R. 654, 112th Cong. (2011); H.R. 653, 112th Cong. (2011); H.R. 611, 112th Cong. (2011).

17. *See* Press Release, Office of the Press Sec'y, The White House, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill Of Rights" to Protect Consumers Online (Feb 23, 2012), http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights ("The blueprint will guide efforts to give users more control over how their personal information is used on the Internet and to help businesses maintain consumer trust and grow in the rapidly changing digital environment. At the request of the White House, the Commerce Department will begin convening companies, privacy advocates and other stakeholders to develop and implement enforceable privacy policies based on the Consumer Privacy Bill of Rights."); *see also* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 11 (2012) (hereinafter CPBOR), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf ("Companies should offer consumers means to withdraw or limit consent that are as accessible and easily used as the methods for granting consent in the first place."). The proposal does not elaborate further on what tools consumers can use to withdraw or stop the use of their information. *See id.* The problem with this current language is that it assumes that consumers' data has already been collected, a point this Article hopes to address by preventing data collection in the first place.

18. CPBOR, *supra* note 17.

19. *See* discussion *infra* Part III.B (discussing a do-not-track browser option).

20. *See* Knapp, *supra* note 6, at 98; Lemley, *supra* note 6, at 462.

to reverse that trend.[21] Therefore, when this Article uses the term "consumer contract," it means a contract offered by a consumer, usually through a software intermediary, and accepted by the corporation.

In examining the question of whether a consumer can expect a court to enforce her contractual preference against tracking, this Article begins with the somewhat sorry state of the law regarding mass-market corporate contracts targeted at consumers. After reviewing some of the relevant legal trends, this Article asserts that, since corporations have been busy binding consumers to standardized take-it-or-leave-it contracts since the advent of the Internet,[22] courts should take seriously the possibility that consumers can do the same to corporations. The Article goes on to propose that the power to determine terms in basic contracts has been taken away from consumers, that it can be quickly and easily given back, and that doing so addresses the heart of the current problem—the lack of power that consumers have to determine the contractual terms governing the sale or use of their data.[23] In short, this Article argues that what is good for the corporate goose is good for the consumer gander.

The Article proceeds in three parts. Part I discusses the mechanics of online tracking and corporate surveillance of consumers. Part II considers the legal literature and law of mass-market consumer contracting. Part III offers a straightforward solution: that courts accept and enforce consumer-offered standardized agreements on the same terms as corporate-offered agreements.

I. ONLINE CORPORATE SURVEILLANCE

Corporate surveillance of consumers has now achieved such low costs as to be truly ubiquitous.[24] The exhaustive nature of this

---

21. *See* sources cited *supra* note 20; *see also* Florencia Marotta-Wurgler, *What's in a Standard Form Contract? An Empirical Analysis of Software License Agreements*, 4 J. EMPIRICAL LEGAL STUD. 677, 678 (2007) (addressing the lack of consumer choice in accepting boilerplate language in standard form contracts).

22. *See* Lemley, *supra* note 6, at 465-66.

23. *See* discussion *infra* Part II (discussing online contracting).

24. *See* Anne Klinefelter, *When to Research is to Reveal: The Growing Threat to Attorney and Client Confidentiality from Online Tracking*, 16 VA. J.L. & TECH. 1, 3 (2011) ("The online tracking industry is growing, inspired by decreasing costs of technology along with largely unregulated access to a vast amount of information sent online." (footnotes omitted)); Jonathan Zittrain, *Law in a Networked World: Privacy 2.0*, 2008 U. CHI. LEGAL F. 65, 80 n.58 (discussing the use of cheap sensors and networks by corporate entities to create "digital dossiers"); *see also* Julia Angwin, *Tracking the Companies that Track You Online*, NPR (Aug. 19, 2010), http://www.npr.org/templates/story/story.php?storyId=129298003 ("[N]early all of the most commonly visited websites gather information in real time about the behavior of online users. . . .

section is necessitated by the extreme nature of the technology involved. It is worth exploring how pervasive and ubiquitous surveillance of consumers has become, so that one can understand the need for the legal reform proposals detailed further on.

In the US scheme of consumer data gathering, there are multiple levels of surveillance,[25] with the primary goal of behavioral advertising—tailoring online advertisements to the individual.[26] Even if a consumer tried to take reasonable measures to avoid being tracked, she would find the process nearly impossible.[27] This difficulty is due, in part, to the varied tracking methods that companies have at their disposal.[28]

The present analysis begins with a simple premise: law is often necessary to solve technological problems by stopping technological arms races.[29] This premise runs contrary to a popular view of the

---

[There are] more than 100 tracking companies, data brokers and advertising networks collecting data — which are then sold on a stock market-like exchange to online advertisers.").

25. *See* Louise Story, *How Do They Track You? Let Us Count the Ways*, N.Y. TIMES, Mar. 9, 2008, http://bits.blogs.nytimes.com/2008/03/09/how-do-they-track-you-let-us-count-the-ways ("The . . . study tallied five types of 'data collection events' on the Internet for 15 large media companies[:] . . . [p]ages displayed, search queries entered, videos played, . . . advertising displayed . . . . [and] ads served on pages anywhere on the Web by advertising networks owned by the media companies. . . . Typically, Web compan[ies] receive[] information about the type of page the user is looking at, the user's I.P. address . . . and for advertising, the content of the ad. Most Web sites and advertising networks place cookies on users' browsers . . . .").

26. *See* Gindin, *supra* note 9 ("[T]he tracking of a consumer's online activities *over time*—including the searches the consumer has conducted, the web pages visited, and the content viewed—in order to deliver advertising targeted to the individual consumer's interests." (internal quotation marks omitted)); *see also* Daniel B. Garrie & Rebecca Wong, *Demystifying Clickstream Data: A European and U.S. Perspective*, 20 EMORY INT'L L. REV. 563, 565-66 (2006) ("Clickstream data is compiled from cookie based technology . . . . [and] is used in part because web server technologies cannot store, sort, and render to a user the vast amounts of data required to deliver the respective web solutions to each individual user to a site or to authenticate a user.").

27. *See* Riva Richmond, *Resisting the Online Tracking Programs*, N.Y. TIMES, Nov. 10, 2010, http://www.nytimes.com/2010/11/11/technology/personaltech/11basics.html ("Keeping your computer free of tracking programs is not easy because of the ad industry's aggressive and sophisticated efforts . . . . A number of tools can *minimize* tracking, but using them requires considerable effort and tech know-how." (emphasis added)).

28. *See* Gindin, *supra* note 9; *see also* Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1144-45 (N.D. Cal. 2008) (discussing tracking, in the broader context of copyright concerns, as it relates to online user's actual identity or their IP address); Schwartz & Solove, *supra* note 2; Solove & Hoofnagle, *supra* note 14, at 362-63. *But see FTC Significant Steps*, *supra* note 4 ("[T]he World Wide Web Consortium . . . Tracking Protection Working Group is working around issue like 'what does tracking mean' . . . .").

29. *See* E. I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970) ("[O]ur devotion to . . . industrial competition must not force us into accepting the law of the jungle as the standard of morality . . . . Our tolerance of the espionage game must cease when the protections required to prevent another's spying cost so much that the spirit of inventiveness is dampened."); *see also* Lee Kovarsky, *A Technological Theory of the Arms Race*, 81 IND. L.J. 917, 950 (2006) ("The DMCA . . . represents copyright law's most conspicuous institutional response to arms race phenomena.").

Internet, which suggests that computer code is a replacement for legal rules online.[30] This view misses the point because legal rules are most needed when technology enables something that society deems immoral or inefficient.[31] Laws can prevent moral failures and expensive defensive countermeasures.[32] In the context of criminal law, for example, legal prohibitions on new methods of technological intrusion into private life are necessary to stop an arms race between citizen and government, in which the government develops ever more powerful tools, and citizens must take ever more elaborate and expensive countermeasures.[33] Outside of the criminal context, legal rules operate to stop technological arms races between intellectual property rights holders and developers of tools that can be used to infringe those rights.[34] The same analysis applies in the context of consumer privacy: law can either give legal force to consumer privacy preferences by permitting consumers to offer and enforce legal terms on the Internet,[35] or it can abdicate and return consumers to an ever

30. *See* LAWRENCE LESSIG, CODE: VERSION 2.0 5 (2006) ("Cyberspace demands a new understanding of how regulation works. It compels us to look beyond the traditional lawyer's scope—beyond laws, or even norms. . . . That regulator is the obscurity in this book's title—Code."). Lessig details in the preface to the second edition that the fundamental arguments in the first edition of *Code* did not change in *Code 2.0*. *Id.* at ix. *But see* Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 680-83 (2003) (discussing how Lessig's proposal of code replacing and becoming law goes too far and rather that code can supplement law). This discussion details two important points. First, the discussion is what matters because debate over the power of code and role of law is critical to preserving an open Internet. Second, Lessig is right in that code can be corrosive to liberty and that now the Internet is marked by control. This is not because of consumer demand, but because corporations control code and consumers are powerless. *See* LESSIG, *supra* note 30, at 38; discussion *infra* note 32.

31. *See* Nick Bilton, *Congress Presses Apple on App Privacy*, N.Y. TIMES, Mar. 14, 2012, http://bits.blogs.nytimes.com/2012/03/14/congress-presses-chief-on-app-privacy; discussion *infra* notes 36-39; *see also duPont*, 431 F.2d at 1016-17.

32. *See duPont*, 431 F.2d at 1016-17; *see also* Scott Cleland, *Why We Need A 'Do-Not-Track' Bill*, WASH. POST, May 10, 2011, http://live.washingtonpost.com/why-you-cant-trust-google-scott-cleland-0510.html ("People deserve the right to vote for themselves if they want to be tracked so they can get targeted ads, or they don't want to be tracked to protect their privacy/security and that of their family. [R]ight now people have no real choice because the technology is way ahead of what people want and the state of the law."); discussion *infra* notes 36-39.

33. *See* United States v. Jones, 132 S. Ct. 945 (2012) (holding that attachment of a GPS unit to a car, and use of the GPS unit to track movements of the car, was a search under the Fourth Amendment); Kyllo v. United States, 533 U.S. 27, 34-35 (2001) (holding that the government's use of thermal imaging technology to observe behavior inside the home constituted a search under the Fourth Amendment); *see also* Stephen A. Josey, Note, *Along for the Ride: GPS and the Fourth Amendment*, 14 VAND. J. ENT. & TECH. L. 161, 170-77 (2011) (discussing United States v. Jones and the government's intrusion aided by technology—police use of GPS on cars to track citizen's movements constantly over an extended period of time).

34. *See* Kovarsky, *supra* note 29, at 969-70.

35. *See* Shmuel I. Becher & Tal Z. Zarsky, *E-Contract Doctrine 2.0: Standard Form Contracting in the Age of Online User Participation*, 14 MICH. TELECOMM. & TECH. L. REV. 303, 305 n.3 (2008) ("[T]he digital environment can potentially offer a very different contractual

more desperate technological battle to protect their privacy. This Part discusses the mechanics of online corporate surveillance with a view toward explaining why a legal, and not a technical, solution is necessary.

A. The Mechanisms of Surveillance

US corporations have unfettered access to information about every aspect of their customers' lives.[36] The original means of tracking consumers' online movements relied on a system of "cookies"—small bits of code located on a consumer's computer that would permit a given website to track where on the site the consumer had gone.[37] Corporations still use this technology, but it has largely been outmoded[38] by advertisement server tracking, which can track consumers across the Internet without cookies through Uniform Resource Locators (URLs), search queries, or assigned random ID numbers to end users.[39] Worse, spyware located directly on the user's computer or smartphone can secretly relay information to ISPs or other online services.[40]

This Section begins with the most obvious threat to consumer privacy: corporate tracking that puts software directly on the consumer's computer.[41] It then proceeds outwards, from the

---

setting, providing consumers with an 'electronic butler' that will automatically signal the consumers' contractual preferences to the various vendors.").

36. *See* Solove & Hoofnagle, *supra* note 14 at 359 ("Currently, the collection and use of personal data by businesses and government is spinning out of control. An entire industry devoted primarily to processing and disseminating personal information has arisen, and this industry is not well-regulated.").

37. *See* Rubinstein et al., *supra* note 5, at 271-72.

38. *See* Erik Larkin, *Browser Fingerprinting Can ID You Without Cookies*, PCWORLD (Jan. 29, 2010, 11:04 AM), http://www.pcworld.com/article/188161/browser_fingerprinting_can_id_you_without_cookies.html ("The specific combination of mundane information such as your plugins and system fonts can be used to create a 'fingerprint' for your browser that could potentially uniquely identify you."); *see also* Peter Eckersley, *Help EFF Research Web Browser Tracking*, EFF (Jan. 27, 2010), https://www.eff.org/deeplinks/2010/01/help-eff-research-web-browser-tracking ("Traditionally, people assume they can prevent a website from identifying them by disabling cookies on their web browser. Unfortunately, this is not the whole story.").

39. *See* Rubinstein et al., *supra* note 5, at 272 ("Today, concerns over cookies seem almost quaint. . . . Recent privacy concerns now center on web services—and especially search engines."); *see also Advertising and Privacy*, *supra* note 14.

40. *See* Ian Sherr & Anton Troianovski, *Tracking-Software Maker Stirs Phone-Privacy Fears*, WALL ST. J., Dec. 2, 2011, http://online.wsj.com/article/SB10001424052970204012004577072652397112014.html ("[S]oftware . . . from a company called Carrier IQ Inc.[,] . . . not transparently visible to consumers, is shown tracking actions such as when buttons are pressed and collecting personal data such as the content of text messages.").

41. It is useful at this point to add one major caveat. This article treats privacy through the lens of contract law. Privacy has also been approached as a basic or a constitutional right. *See* Orin S. Kerr, *The Case For The Third-Party Doctrine*, 107 MICH. L. REV. 561, 588 (2009). It is

consumer's computer to the Internet connection, to the ISP that provides that connection, and to the servers of online service and application providers.[42]

1. On the Desktop

Consumer information starts on the desktop. Everyone is aware of cookies, but anti-cookie browsing technology does not really protect consumer privacy. Anti-cookie technology, like the so-called "In Private" browsing mode,[43] and equivalents such as Google's "Incognito,"[44] have been an important selling point for pure free-market advocates. The claim is that the existence of such options demonstrates that the market in consumer information is both functional and respectful of consumer choices regarding privacy.[45] Yet

---

certainly true that consumers are being tracked everywhere, that this information ends up in unanticipated corporate and government hands without any of the constraints of the Constitution, and that this state of affairs is corrosive to free societies. *Id.* But this Article is about contract law, not constitutional law.

42. *See* Solove & Hoofnagle, *supra* note 14, at 359 ("Increasingly, the government is relying on data-broker companies to supply personal data for intelligence and law enforcement purposes. As a result, the government is navigating around the protections of the Privacy Act of 1974 . . . .").

43. *See* Edward C. Baig, *Microsoft's Internet Explorer 8 Lets You Browse in Private*, USA TODAY, Aug. 28, 2008, http://www.usatoday.com/tech/columnist/edwardbaig/2008-08-27-Internet-explorer-8_N.htm ("With 'InPrivate' browsing turned on, all traces of the sites you visit are removed from the Web history. No Web cookies . . . are left behind after you close a session."). *But see* Nick Wingfield, *Microsoft Quashed Effort to Boost Online Privacy*, WALL ST. J., Aug. 2, 2010, http://online.wsj.com/article/SB10001424052748703467304575383530439838568.html ("Explorer [requires] the consumer to turn on the feature that blocks tracking by websites, called InPrivate Filtering. It wasn't activated automatically. What's more, even if consumers turn the feature on, Microsoft designed the browser so InPrivate Filtering doesn't stay on permanently. Users must activate the privacy setting every time they start up the browser."); *What is InPrivate Browsing*, MICROSOFT, http://windows.microsoft.com/en-US/windows-vista/What-is-InPrivate-Browsing (last visited Dec. 22, 2011) ("While you are surfing using InPrivate Browsing, Internet Explorer stores some information—such as cookies and temporary Internet files—so that the webpages you visit will work correctly. However, at the end of your InPrivate Browsing session, this information is discarded.").

44. *See* Jennifer Valentino-Devries, *How to Avoid Prying Eyes*, WALL ST. J., July 30, 2010, http://online.wsj.com/article/SB10001424052748703467304575383203092034876.html ("All major browsers offer a 'private browsing' mode to limit cookies. Chrome calls it 'Incognito.' Internet Explorer calls it 'InPrivate Browsing,' . . . . Private browsing doesn't block cookies. It deletes cookies each time you close the browser or turn off private browsing . . . .").

45. *See* Wingfield, *supra* note 43 ("Mr. Cullen, Microsoft's chief Privacy strategist, says the input of outsiders helped Microsoft strike a balance between privacy and advertising interests. The browser, he says, 'was a better product than when it came off the drawing-room floor of the Internet Explorer group.'"). *But see* Jay P. Kesan & Rajiv C. Shah, *Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics*, 82 NOTRE DAME. L. REV. 583, 601-02 (2006) ("People do not change defaults when they are uninformed that another choice exists. If a person does not know about the possibility of changing an option *or the ramifications of each choice*, then a default setting is equivalent to a fixed setting." (emphasis added)).

such options cause consumers to erroneously believe that they are not being tracked.[46] Pure free-market advocates claim that corporations have every bit as much of an interest in selling privacy-enhancing products to consumers as they do in marketing surveillance products to advertisers.[47] This analysis is incomplete—the companies that effectively defend privacy often rely on open-source code rather than private products. Corporate "privacy tools" more often turn out to be channels for the consumer to permit the corporation to use her data in new ways.[48] It is therefore unsurprising that emerging corporate tools are neither simple, nor usable, nor truly effective.[49]

A closer look at current technology may help to illustrate why it is so difficult for consumers to engage in privacy self-help with currently available anti-surveillance products. To access a website, a user requests a URL—the string of characters in the address field that identifies and locates the website.[50] The website can compose a unique URL on the fly, which acts as a server-side digital footprint that tracks the user's activity. The URL can change depending on what the user clicks on, such as a banner advertisement or hyperlink to a related topic. Therefore, someone who has access to the user's viewing history, such as an ISP,[51] can track her movements by

---

46. *See* Wayne R. Barnes, *Rethinking Spyware: Questioning the Proprietary of Contractual Consent to Online Surveillance*, 39 U.C. DAVIS L. REV. 1545, 1551 (2006) ("Eventually, advertisers sought to overcome the domain-specific limitations of cookies and instead develop a means by which they could follow consumers wherever they went on the Internet. Thus, the concept of spyware was born."); Kesan & Shah, *supra* note 45.

47. *See Consumers are Key to Privacy Protection*, PCWORLD (June 29, 2001, 10:00 AM), http://www.pcworld.com/article/54183/consumers_are_key_to_privacy_protection.html (noting the pro-Free Market insights of some commentators, who equate the concept of "privacy" to that of "happiness").

48. *See* Barnes, *supra* note 46; *see also Symantec Insight*, SYMANTEC, http://www.symantec.com/business/theme.jsp?themeid=insight (last visited Oct. 12, 2011) ("Symantec Insight uses reputation security technology . . . to identify new threats as they are created. Based on advanced data mining techniques, Insight seeks out changing encryption and mutating code. Insight separates files at risk from those that are safe, for faster and more accurate malware detection.").

49. *See* Richmond, *supra* note 27 ("To remove tracking programs and keep them out, it is better to enlist the help of specialized software."). The article then cites several programs designed by privacy-focused companies other than Google, Microsoft, or Apple. *Id.*; *see also* Valentino-Devries, *supra* note 44 ("Ironically, these opt-out systems work by installing a cookie on your computer. That cookie tells ad networks to stop sending targeted ads to your computer. Because these systems rely on a cookie to work, you'll need to opt out all over again any time you delete cookies from your machine.").

50. *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1287 (2004) ("A URL is a pointer—it points to the location of particular information on the Internet. . . . [I]t indicates where something is located. . . . URLs can reveal the specific information that people are viewing on the Web. URLs can also contain search terms.").

51. *See* Matthew J. Tokson, *The Content/Envelope Distinction In Internet Law*, 50 WM. & MARY L. R. 2105, 2114 (2009) ("Unlike traditional letters, emails and web surfing

following the changing URLs.[52] There is no need to put code on a consumer's computer in order to know what URL the user wants to see or where the user has been.[53] Although cookies are invasive, they are on the user's computer where the user has some control over them. In contrast, modern tracking techniques are often located outside of the user's technological control.

Moreover, the technology to remove cookies is at least as invasive as the cookies themselves were.[54] Norton/Symantec is the top antivirus and spyware protection program in the country for individual users.[55] Ironically, their products come dangerously close to resembling spyware. Norton must be invasive because it can no longer rely on a standard antivirus model, in which protected computers merely download known virus profiles.[56] Certain attack methods, such as the Zeus attack kit,[57] can create one-off, custom-bred viruses on a per computer or per attack basis.[58] Therefore, since an

communications are often copied in transit by Internet Service Providers (ISPs) and are (in theory) easily accessed by ISP employees.").

52. *See* Solove, *supra* note 50.

53. *Id.*; Tokson, *supra* note 51.

54. They have to be: in order to remove cookies such as new advanced versions like "super cookies" or "zombie cookies," they must be able to identify the source and provenance of a piece of code. *See* Christopher Drew & Verne G. Kopytoff, *Deploying New Tools to Stop the Hackers*, N.Y. TIMES, June 17, 2011, http://www.nytimes.com/2011/06/18/technology/18security.html; *see also infra* note 103 (discussing "zombie cookies"). Thus, for example, when Norton/Symantec scans a document, it actually makes a copy of that document, compares the document to similar or identical documents that have appeared on other Norton/Symantec users' computers, and then determines whether those other users have become "sick" or have remained healthy. *See* Drew & Kopytoff, *supra*. The best anti-botnet software is itself therefore a botnet. *See id.*

55. *See* Ashlee Vance, *For Symantec and McAfee, 'Arms Race' for Security*, N.Y. TIMES, July 5, 2009, http://www.nytimes.com/2009/07/06/technology/business-computing/06virus.html ("In the consumer market, Symantec holds an even larger lead, with 52 percent share and $1.8 billion in revenue last year, compared with 18 percent of the market and $624 million in revenue for McAfee. A host of smaller players like Trend Micro, CA and Kaspersky Lab round out the field.").

56. *See* Drew & Kopytoff, *supra* note 54 ("Symantec's strategy is to rate software based on a number of factors including the file's age and source. The company also checks data it collects from users about the kind of software they have on their computers. Software used by 100,000 people is more likely to be good, while a file that no one else has is more likely to be bad.").

57. *See* Riva Richmond, *New Menace in the War Against Online Crime*, N.Y. TIMES, July 13, 2010, http://gadgetwise.blogs.nytimes.com/2010/07/13/new-menace-in-the-war-against-cyber-crime ("In the battle against online criminals, a new front has emerged involving Zeus, a data-stealing Trojan horse that infects Windows PCs . . . . Stopping the new Zeus attack can be tricky.").

58. *See* Peter Coogan, *Zeus, King of the Underground Crimeware Toolkits*, SYMANTEC, http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits (last updated Feb. 22, 2010).

antivirus can only defend against what it has seen before, the past antivirus approach is now largely obsolete.

In response, Norton/Symantec leveraged its large customer base into a counter-botnet.[59] That is, Norton customers together form a network that reports suspicious programs to Norton.[60] Norton can then heavily supplement its blacklist model (stopping viruses that appear on a list of antivirus definitions) and its whitelist model (only allowing access to websites that are known to be clean) with a new approach.[61] This approach, termed reputational-based security,[62] is a more effective counter to viruses. As part of this reputational process, the major antivirus programs not only record where their customers go when they surf the Internet, but also download and scan documents from their customers' computers.[63] Thus, antivirus programs can be almost as bad as the threats they protect against, since they automatically obtain customers' web-surfing history and confidential documents for offsite analysis.[64] Much of this snooping and copying is not transparent to users. Many Symantec users would be startled to learn that their virus-protection program was downloading and scanning all of their confidential information.[65]

Furthermore, due to overreaching corporate contracts,[66] corporations have become emboldened to conduct searches of their users' equipment as part of the installed program.[67] For example, a video game creator might install deep-level invasive software that scans the user's hard drive and looks for unauthorized third-party programs.[68] Or, as in another recent scenario, a smartphone carrier might install spyware that captures encrypted URL requests, SMS message text, and email text, all under the auspices of an End User License Agreement (EULA) that authorizes the carrier to monitor

---

59. *See* Drew & Kopytoff, *supra* note 54.

60. *See id.*

61. *See id.*

62. *See Symantec Insight*, *supra* note 48.

63. *See id.*

64. *See* Drew & Kopytoff, *supra* note 54.

65. *See id.*

66. *See* Robert A. Hillman & Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. REV. 429, 441 (2002) ("Courts have difficulty distinguishing between terms that create a reasonable arrangement of risks and terms that constitute exploitation of consumers. . . . [C]ourts typically frame the issue as a dispute between a single consumer and a business, rather than as an aggregate policy that affects the vast majority of consumers and businesses that transact with each other contentedly.").

67. *See* MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 936 (9th Cir. 2010).

68. *Id.* at 936 ("Blizzard launched Warden, a technology that it developed to prevent its players who use unauthorized third-party software, including bots, from connecting to [the computer game World of Warcraft's] servers.").

"usage information" to improve service.[69] This little-known invasive behavior is made possible via corporate contracts; the EULAs both enable and facilitate this "on the computer" malware consumer surveillance.[70] They do not, however, reflect the consumer's meaningful or informed consent to be surveilled.[71]

Illegitimate surveillance programs also pose a significant privacy risk. Encryption, anti-traffic analysis programs, and other precautions are rendered useless if the data-gatherer can directly access the data-receiving computer.[72] For example, a hacker can circumvent hard-to-penetrate encryption by installing a keylogger onto the user's hard drive that logs each keystroke the user enters,[73] or through "socially-engineered" attacks.[74] One of the most popular and effective socially-engineered-attack methods involves learning about a particular person's interests and sending her a tailored email.[75] Once the user clicks on a malicious link within the email, the

69. *See* Sherr & Troianovski, *supra* note 40. Another concern is where there is no applicable policy. *See* Thurm & Kane, *supra* note 5 ("Many apps don't offer even a basic form of consumer protection: written privacy policies. Forty-five of the 101 apps didn't provide privacy policies on their websites . . . .").

70. *See* Barnes, *supra* note 46, at 1547 ("Millions of people likely have spyware on their computers . . . . [T]hey may have 'agreed' to its installation by clicking their assent to a license agreement that came with another program that they downloaded. . . . [T]he spyware application may be performing . . . surveillance of every movement these consumers make on the Internet.").

71. *See* Solove & Hoofnagle, *supra* note 14, at 369 ("Many data transfers and uses by companies occur without the meaningful informed consent of consumers. . . . There must be a way to ensure that consumers can exercise *meaningful* informed consent about the uses and dissemination of their personal information." (emphasis added)); *see also* Mortensen v. Bresnan Commc'n, No. CV 10-13-BLG-RFC, 2010 U.S. Dist LEXIS 131419, at *12 (D. Mont. Dec. 13, 2010) (dismissing a class action allegation based on the Electronic Communications Privacy Act as defendant adequately notified plaintiff through its privacy disclosure and OnLine Subscriber Agreement that it would collect and use plaintiff's browsing behavior and through plaintiff's use of the internet service, consent was given or acquiesced to).

72. *See* Tom Zeller Jr., *Protecting Yourself from Keylogging Thieves*, N.Y. TIMES, Feb. 27, 2006, https://www.nytimes.com/2006/02/27/technology/27hackside.html ("[E]ven with [protective] measures in place, malicious code—including a keylogger—can sometimes find its way onto your computer. . . . 'With keyloggers, you've literally got someone sitting over your shoulder watching everything that you do' . . . .").

73. *See* Randall Stross, *A Strong Password Isn't the Strongest Security*, N.Y. TIMES, Sept. 4, 2010, http://www.nytimes.com/2010/09/05/business/05digi.html ("Keylogging software, which is deposited on a PC by a virus, records all keystrokes—including the strongest passwords you can concoct—and then sends it surreptitiously to a remote.").

74. *See* Sarah Granger, *Social Engineering Fundamentals, Part I: Hacker Tactics*, SYMANTEC, http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics (last updated Nov. 3, 2010) ("[H]ackers may obtain information on-line [sic] by pretending to be the network administrator, sending e-mail through the network and asking for a user's password. This type of social engineering attack doesn't generally work, because users are generally more aware of hackers when online, but it is something of which to take note.").

75. *Id.* ("E-mail can also be used for more direct means of gaining access to a system. . . . A good example of this was an AOL hack[:] . . . the hacker called AOL's tech support and spoke with the support person for an hour. . . . [and] mentioned that his car was for sale cheaply. The

hacker gains access to the user's system.[76] Eventually the data from an installed keylogger will reveal the user's password, at which point the hacker can know everything that the user knows.[77]

Online contracts between consumers and corporations permit corporations to routinely install spying networks on consumers' computers. But, a dangerous zone for corporations lies just beyond the scope of those contracts. When corporations exceed their contractual grant, they are, like hackers, trespassers at best and criminals at worst.[78]

A corporate-drafted contract is the sole difference between a corporation and a hacker. Thus far, this fact has not made a notable difference, since courts have permitted corporations the sole and exclusive right to draft and enforce contract terms in the mass-market consumer context.[79] However, this legal framework cannot last. Courts ought to recognize that consumers also have the right to set legal limits, and courts should enforce those limits even though they may be set forth in documents different from corporate-drafted EULAs or Terms of Service. In short, just as a user must follow the Terms of Use she agrees to upon accessing a corporation's website, a corporation should be equally bound to follow the individual's pre-set Terms of Use governing her private information.[80]

2. Over the Wire

The second basic threat to a consumer's private information is that a third party might intercept the message in transit, effectively intercepting it "over the wire." Although deep-packet inspection can reveal much about what is inside a communication,[81] analysts posit

---

tech supporter was interested, so the hacker sent an e-mail attachment 'with a picture of the car.' Instead of a car photo, the mail executed a backdoor exploit that opened a connection out from AOL through the firewall."); *see* Drew & Kopytoff, *supra* note 54 ("Unlike past blitzes of spam with clunky sales pitches, today's attacks often rely on a familiar face and are extremely difficult to stop. In a practice known as spear phishing, hackers send e-mails that seem to come from co-workers or friends and include attachments that can release malware to steal passwords and other sensitive data.").

76. *See* Drew & Kopytoff, *supra* note 54.

77. *See* Stross, *supra* note 73.

78. 18 U.S.C. § 1030 (2008).

79. *See* discussion *infra* Part II.A.

80. *See* discussion *infra* Part II.B.

81. *See* Kevin Werbach, *Breaking the Ice: Rethinking Telecommunications Law for the Digital Age*, 4 J. TELECOMM. & HIGH TECH. L. 59, 92 (2005) ("[I]t [is] technically challenging to classify traffic flows while they are actually moving across the network. . . . [D]eep packet inspection promises to overcome some of these limitations. . . . A service provider could use deep packet inspection to distinguish . . . traffic . . . and either block it or reduce its available bandwidth." (footnote omitted)).

that current commercially available encryption can withstand even military attempts to decrypt. Until some significant advance in computing—quantum computing, for example—changes the nature of decryption, current encryption is fairly secure.[82]

Despite this, many online companies refuse to use even basic secure encryption. Most websites are simply hypertext transfer protocol (http), not hypertext transfer protocol secure (https).[83] Some companies argue that making a website https is too expensive; however, companies that have made the switch have not found the costs prohibitive.[84] Indeed, even small companies have switched to secure connections. Ixquick, a small company that runs a privacy-oriented search engine, already encrypts all search requests.[85] The problem has become one of entrenchment: for most websites, by default the unencrypted http site comes up automatically. And unless consumers access a website through a search engine, they often request an unencrypted version by typing http instead of https in the address.[86] Encryption should be the default; instead, we find that by default the Internet architecture permits third parties to capture consumer data.

As with on-the-desktop problems, there are some technological solutions that consumers can use to improve their over-the-wire security. But, these solutions do not work well or comprehensively. Users can fix some over-the-wire problems through a simple add-on,

---

82. *See Secure Sockets Layer (SSL): How It Works*, SYMANTEC, http://www.verisign.com/ssl/ssl-information-center/how-ssl-security-works (last visited Feb. 17, 2012) ("Web servers and Web browsers rely on the Secure Sockets Layer (SSL) protocol to create a uniquely encrypted channel for private communications over the public Internet. . . . At current computing speeds, a hacker with the time, tools, and motivation to attack using brute force would require a trillion years to break [in] . . . .").

83. *See* Kate Murphy, *New Hacking Tools Pose Bigger Threats to Wi-Fi Users*, N.Y. TIMES, Feb. 16, 2011, http://www.nytimes.com/2011/02/17/technology/personaltech/17basics.html (discussing that not all websites have https and the few that do make it difficult to use).

84. *Id.* ("Gmail made end-to-end encryption its default mode in January 2010."); *see also* Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. TELECOMM. & HIGH TECH. L. 359, 378 (2010) ("Google's decision to adopt encryption by default for its Gmail service remains a minority practice in the cloud computing industry. Users of Facebook, MySpace, Yahoo and Microsoft are still vulnerable to the same data theft and account hijacking attacks. While Google improved the security defaults for its Gmail service in response to high-profile criticism from the security community, the other major Web 2.0 firms have shown little interest in deploying encryption technologies, and thus continue to deliver their users' private data over insecure connections. The problem, it seems, is industry wide.").

85. *See Ixquick Protects Your Privacy!*, IXQUICK, https://www.ixquick.com/eng/protect-privacy.html (last visited Dec. 17, 2011) (discussing the search engines comparison to other search engines and how it does not save your IP address); *see also Privacy*, DUCKDUCKGO, https://www.duckduckgo.com/privacy.html (last visited Feb. 16, 2012) ("DuckDuckGo does not collect or share personal information. That is our privacy policy in a nutshell.").

86. *See* Kesan & Shah, *supra* note 45, at 601.

such as HTTPS Everywhere—created by the Electronic Frontier Foundation in conjunction with the Tor Project.[87] HTTPS Everywhere requests an https-secured connection wherever one is available.[88] The add-on changes the default setting from an unencrypted connection to an encrypted one. But add-ons can only *request* an encrypted connection. If the corporation does not offer secure connections, the add-on can do little other than alert the user.

The actors who pose the greatest threat for interception over the wire are actually not hackers, but the legitimate entities that provide Internet access services.[89] Indeed, in many cases the threat is from employers, who function as ISPs.[90] Employers may use this function to intrude further into the personal lives of their employees.[91] A recent Supreme Court case, for example, gave employers broad access to text messages on an employee's personal cell phone.[92] Because employers control the wires and may not have their employees' best interests at heart, this can lead to serious privacy implications.

An ISP's power over data as it crosses the wire is so efficient and effective that in many authoritarian countries ISPs provide the means of state control.[93] Although almost every website is accessible in Saudi Arabia, the state logs the majority of web contact.[94] China takes a different approach: using what it is able to detect through over-the-wire and packet inspection technologies to censor what

87. *See* Murphy, *supra* note 83 ("[T]he Electronic Frontier Foundation in collaboration with the Tor Project, another group concerned with Internet privacy, released in June an add-on to the browser Firefox, called Https Everywhere.").

88. *See id.* ("The extension . . . makes 'https' the stubbornly unchangeable default on all sites that support it.").

89. *See* Werbach, *supra* note 81, at 92-93.

90. *See* Jill Yung, *Big Brother is Watching: How Employee Monitoring in 2004 Brought Orwell's* 1984 *to Life and What the Law Should do About it*, 36 SETON HALL L. REV. 163, 165 (2005) ("The alarm bells went off when . . . Internet tracking software debuted in workplaces. Still, these practices, limited somewhat by a need to show business-relatedness, have largely found acceptance in some form." (footnote omitted)).

91. *Id.* at 165 n.8 ("GPS is a prime example of 'technology [that enables] employers to gather enormous amounts of data about employees, often far beyond what is necessary to satisfy safety or productivity concerns.'" (alteration in original)).

92. *See* City of Ont. v. Quon, 130 S. Ct. 2619, 2632-33 (2010); *see also* Louise L. Hill, *Gone but Not Forgotten: When Privacy, Policy and Privilege Collide*, 9 NW. J. TECH. & INTELL. PROP. 565, 586 (2011) ("The Supreme Court determined that the City's search of Quon's text messages was reasonable. 'Although as a general matter, warrantless searches "are *per se* unreasonable under the Fourth Amendment,"' there is an exception for 'the "special needs" of the workplace.'").

93. *See* Dawn C. Nunziato, *How (Not) to Censor: Procedural First Amendment Values and Internet Censorship Worldwide*, 42 GEO. J. INT'L L. 1123, 1124-26 (2011).

94. *Id.* at 1150-52.

citizens see.[95] Even in the United States, ISPs retain broad over-the-wire control. Apple's iPhone tracked users wherever they went, and then stored that data unencrypted on the device.[96] Google engages in comparable efforts with Android.[97] Most smartphones in the United States recently carried the Carrier IQ software,[98] which intercepted user communications and secure data requests, and sent the information to the user's ISP.[99] Security over the wire, in the form of secure encrypted communications, thus is not technology that only special people use or need to keep their extraordinary secrets. Instead, it is something that should be standard on every connection and for every device.[100]

For purposes of the present analysis, the secured connection issue provides a useful data point. For secured connections, the consumer can set the terms on which data will be transmitted and the corporation must acquiesce or refuse the connection. This basic principle should be extended to other methods of communication through which a consumer wishes to make her data available. A

---

95. *Id.* at 1148; *see also* Christopher Rhoads & Loretta Chao, *Iran's Web Spying Aided by Western Technology*, WALL ST. J., June 22, 2009, http://online.wsj.com/article/SB124562668777335653.html ("China's vaunted 'Great Firewall,' which is widely considered the most advanced and extensive Internet censoring in the world, is believed also to involve deep packet inspection.").

96. *See* Julia Angwin & Jennifer Valentino-Devries, *Apple, Google Collect User Data*, WALL ST. J., Apr. 22, 2011, http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html; *see also Apple Q&A On Location Data*, APPLE (Apr. 27, 2011), http://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html ("Sometime in the next few weeks Apple will release a free iOS software update that: reduces the size of the crowd-sourced Wi-Fi hotspot and cell tower database cached on the iPhone, ceases backing up this cache, and deletes this cache entirely when Location Services is turned off. In the next major iOS software release the cache will also be encrypted on the iPhone.").

97. *See* Angwin & Valentino-Devries, *supra* note 96; *see also In re* Google Android Consumer Privacy Litig., 802 F. Supp. 2d 1372, 1373 (J.P.M.L. 2011) ("Plaintiffs contend, inter alia, that Google engaged in improper business practices and violated users' privacy by using and sharing plaintiffs' data without authorization.").

98. *See* Marguerite Reardon, *Sprint Updates Phones To Eliminate Carrier IQ*, CNET (Jan. 17, 2012), http://news.cnet.com/8301-30686_3-57360436-266/sprint-updates-phones-to-eliminate-carrier-iq.

99. *See* Sherr & Troianovski, *supra* note 40 ("Some wireless carriers, including Sprint Nextel Corp., AT&T Inc. and T-Mobile USA, ask some of their phone manufacturers to put Carrier IQ on their devices. Each said they use the technology to monitor their networks and improve service.").

100. Moreover, the ban on researching encryption technologies embodied in the Digital Millennium Copyright Act has put the United States ten years behind the competition for secure data on handheld devices. *See* Vicky Ku, Note, *A Critique of the Digital Millenium Copyright Act's Exemption on Encryption Research: Is the Exemption Too Narrow?*, 7 YALE J.L. & TECH. 465, 478 (2005) ("To have your adversary acknowledge that defending a lawsuit based on violations of the DMCA would create a chilling effect on research, is a pretty strong suggestion that it is true."); *see also* Joseph P. Liu, *The DMCA and the Regulation of Scientific Research*, 18 BERKELEY TECH. L.J. 501, 535-36 (2003).

handshake protocol request[101] is a request for technical rules that the computer must follow to connect. Corporations should honor a handshake protocol request not to be tracked on precisely the same grounds as a handshake protocol requesting a secured connection.

3. Online Service Providers

It may seem obvious that this Article would focus on the data collected by online websites, mobile application providers, and vendors of consumer data. Permitting users a meaningful, unitary opt-out choice to avoid corporate surveillance is, after all, the goal of this Article. But the technology by which third parties gather and aggregate this data is simple and startling enough to merit attention.

Cookies have advanced technologically.[102] Zombie cookies[103] now resurrect themselves after the user deletes them; how can a court see that as anything but a violation of the user's clearly-stated preference?[104] Google Ads display banner advertisements across a large swath of the Internet.[105] These advertisements, which sit on a different server than the main website accessed, redirect the user when clicked and retain the IP address of the computer that viewed the advertisement.[106] By simple aggregation, Google Ads can track a

---

101. *See* Michael Kende, *The Digital Handshake: Connecting Internet Backbones*, 11 COMMLAW CONSPECTUS 45, 45 (2003) ("The Internet is not a monolithic, uniform network; rather, it is a network of networks . . . . In order to provide end users with universal connectivity, Internet backbones must interconnect . . . . Interconnection agreements between Internet backbone providers are reached through commercial negotiations in a 'handshake' environment.").

102. *See* Ashkan Soltani et al., *Flash Cookies and Privacy* 2 (Aug. 10, 2009) (unpublished manuscript), *available at* http://ssrn.com/abstract=1446862 ("We found that top 100 websites are using Flash cookies to 'respawn,' or recreate deleted HTTP cookies. This means that privacy-sensitive consumers who 'toss' their HTTP cookies to prevent tracking or remain anonymous are still being uniquely identified online by advertising companies." (footnote omitted)).

103. *Id.* Zombie cookies are literally http code that cannot be deleted without significant efforts. *What are Zombie Cookies? How do I Delete Them?* GEEKMATICS (May 6, 2011), http://www.geekmatics.com/posts/320.

104. *See* Complaint at 2-3, Valdez v. Quantcast Corp., No. CV10-05484 (C.D. Cal. July 23, 2010), *available at* http://online.wsj.com/public/resources/documents/cookielawsuit073010.pdf (filing suit because of violations of privacy from cookies that recreate themselves after deletion); *see also* Jennifer Valentino-DeVries, *Lawsuit Tackles Files that 'Re-Spawn' Tracking Cookies*, WALL ST. J., July 30, 2010, http://blogs.wsj.com/digits/2010/07/30/lawsuit-tackles-files-that-re-spawn-tracking-cookies ("'The story is not about cookies,' said Scott Kamber, a privacy lawyer involved in the suit. 'The story is about tracking you without consent. The fact that it has a benign name like "cookies" has nothing to do with it.' He said the cookies found . . . '*deliberately circumvent controls you set on your computer*.'" (emphasis added)).

105. *See* Claire Cain Miller, *Google Campaign to Build Up its Display Ads*, N.Y. TIMES, Sept. 21, 2010, http://www.nytimes.com/2010/09/22/business/media/22adco.html.

106. *See Privacy Policy*, N.Y. TIMES, http://www.nytimes.com/content/help/rights/privacy/policy/privacy-policy.html (last updated Dec. 5, 2011) ("The New York Times logs Internet

user across the Internet through all the banner advertisements she views as she surfs.[107] Compounding the problem, some ISPs do not shift the IP addresses they allocate to users, or, if they do, they maintain meticulous multi-year records regarding which IP address was tied to which user.[108] For example, Sprint assigns mobile telephone users a single, static IP address for their data connection.[109] Any website operator or advertisement server that encounters the user's IP address, or other assigned static ID number, can be certain that it is interacting with the same person as last time, and can also identify the user as the same person who used that IP address on other websites.[110]

Advertisers and online service providers have found ways to aggregate information gathered from IP address tracking, thereby achieving total surveillance of the consumer from logon to logout.[111] More significantly, contract law blindly assumes that the user agreed to comprehensive and perniciously intrusive surveillance merely by virtue of terms of use that do not even appear on the visited website.[112]

Protocol (IP) addresses . . . . We use this information in an aggregate fashion to track access to our Web sites and mobile applications. . . . The New York Times . . . also transmits non-personally identifiable Web site usage information about visitors to the servers of a reputable third party for the purpose of targeting our Internet banner advertisements on other sites. To do this, we use Web Beacons in conjunction with cookies . . . .").

107. Google now tracks users across any services of Google they use. *See Preview: Privacy Policy*, GOOGLE, https://www.google.com/intl/en/policies/privacy/preview (last updated Mar. 1, 2012) ("We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users."). This new privacy policy went live on March 1, 2012, and consolidated the different privacy policies for each product and service Google offers. *Id.*

108. *See* Dep't of Justice, *Retention Periods of Major Cellular Service Providers*, WIRED, http://www.wired.com/images_blogs/threatlevel/2011/09/retentionpolicy.pdf (last visited Feb. 29, 2012) (outlining data gathered by the Computer Crime and Intellectual Property Section, U.S. Department of Justice); *see also* Klinefelter, *supra* note 24, at 2 ("Sites also regularly collect the date and time that a researcher from a particular IP address visits their site. Some websites may retain user information indefinitely." (footnote omitted)).

109. *See* Christopher Soghoian, *An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government*, 12 MINN. J. L. SCI. & TECH. 191, 210 (2011) ("Sprint Nextel assigns each Internet-connected wireless handset a static IP address and logs the allocation of these addresses for a twenty-four month period. The company also logs the URL of each webpage viewed by its customers . . . ." (footnote omitted)).

110. *Id.* at 210-11; *see* Thurm & Kane, *supra* note 5 ("Among all apps tested, the most widely shared detail was the unique ID number assigned to every phone."); *see also* Rubinstein et al., *supra* note 5, at 272 (noting that "[r]ecent privacy concerns now center on web services—and especially search engines"); *Advertising and Privacy*, *supra* note 14.

111. *See* Soghoian, *supra* note 109, at 211 ("[A] Sprint Nextel customer can later be tracked down based on an anonymous comment left on a blog or a peer-to-peer (P2P) file downloaded over the company's cellular network, while customers of T-Mobile and Cricket can freely engage in a variety of online activities without any risk of later discovery.").

112. *Id.* at 192-94.

A user generally has only one ISP, but online service providers are far more numerous. As aggressive or intrusive as ISP contracts with consumers may be, they are still limited in number, and therefore plausibly manageable for the consumer. If it is improbable that consumers will be able to manage their privacy in one corporate-drafted ISP contract, then it is absolutely impossible that they will be able to do so across thousands of different online service provider contracts. The current system places almost all privacy transaction costs on consumers' shoulders.[113] Consumers are set up to fail, because to protect their privacy, they must digest, update, and maintain enough legal information to stump a supercomputer. There is a simpler alternative. Courts could enforce the consumer's one-time, unitary expressed preference in the form of a do-not-track flag.

Thus, this Article does not contest the enforceability of online, automated, and standardized contracts, but rather asserts that consumers should have the same power to benefit from such contracts as do corporations. Many scholars already argue that courts should neither enforce these contracts of extra adhesion beyond standard terms that consumers expect,[114] nor permit widespread consumer surveillance.[115] Judges, however, lack any principled rationale to apply different reasoning to consumer-proffered contracts than they do to corporate-proffered contracts.[116]

Therefore, if Google's terms-of-use agreement, residing somewhere on a Google server, is binding upon any user who views a Google Ad, then *a fortiori* a consumer's terms-of-data-use contract

---

113. *See* Julia Angwin & Geoffrey A. Fowler, *Microsoft, Facebook Offer New Approaches to Boost Web Privacy*, WALL ST. J., Feb. 26, 2011, http://online.wsj.com/article/SB10001424052748704692904576166820102959428.html ("Facebook consolidated many of its settings into a control panel designed to make it easier for users to adjust when and how their information was shared with other users and third parties."); Geoffrey A. Fowler, *Facebook Security Flaw Exposed User Accounts*, WALL ST. J., May 11, 2011, http://online.wsj.com/article/SB10001424052748703730804576315682856383872.html (discussing Facebook's complex ecosystem of apps and their data flows). This is only one of many examples illustrating the corporate default setting to full tracking of consumers' information. *See also* Kesan & Shah, *supra* note 45; discussion *infra* note 120.

114. *See, e.g.*, Wayne R. Barnes, *Toward a Fairer Model of Consumer Assent to Standard Form Contracts: In Defense of Restatement Subsection 211(3)*, 82 WASH. L. REV. 227, 272 (2007) (discussing Restatement (Second) of Contracts § 211(3) as a way to protect consumers against questionable terms in form contracts).

115. *See* Kirsch, *supra* note 3, at 54-65 (suggesting that the upcoming revision of the European Union's Data Protection Directive should require advertisers to use and respect a do-not-track mechanism for consumers to meaningfully consent, or not, to online tracking for use in behavioral advertising); Steindel, *supra* note 3, at 483-88 (discussing the problem of online tracking for consumers and offering that federal legislation should implement a do-not-track browser option to protect consumers).

116. *See* sources cited *supra* note 6.

should be binding upon a corporation that must interact directly with that consumer's computer. Online corporate contracts perhaps should not be so easily enforceable. But, if they are so strong in corporate hands, they should be equally strong in the hands of consumers.

B. The Failure of Consumers' Self-Help Solutions

Industry advocates claim that consumers should engage in technological self-help, known commonly as Privacy Enhancing Technology (PETs), as a means for constraining corporate overreaching.[117] But why should law not also be available to help consumers end the privacy arms race? Corporations receive the aid of the law to constrain technological arms races and stop bad actors,[118] but the law relegates consumers to self-help in order to protect their data. It makes little sense that while multinational corporations cannot keep their data secure without the enforcement of strong laws, the law expects consumers to do precisely that. The double standard is startling.

Law is well positioned to intervene in precisely this sort of case, where the technological arms race to defend a legal interest would cost both sides more than the cost of legal enforcement. Arms races are expensive, and when they do not have payoffs in the form of increased competition, law often steps in and stops the race.[119] That is, at least, the theory. To test whether it is true, however, one must inquire whether the law is as conducive to stopping arms races that are hurting consumers as it is to stopping arms races that are harming multinational corporations.

Courts should enforce a consumer's expressed preference for privacy instead of leaving consumers to be responsible for buying and using products that defend consumer privacy, or worse, responsible for reading and comprehending thousands of pages of EULAs and perennially shifting privacy policies. The opposing and ostensibly

---

117. *See* LESSIG, *supra* note 30, at 228 (discussing Privacy Enhancing Technologies (PETs)); *see also* Angwin & Fowler, *supra* note 113 ("A Microsoft spokeswoman said the company's proposed do-not-track feature is part of a suite of privacy tools that the company hopes can gain broad industry support. . . . Facebook consolidated many of its settings into a control panel designed to make it easier for users to adjust when and how their information was shared with other users and third parties."); Jonathan Mayer, *Tracking the Trackers: Self-Help Tools*, CENTER FOR INTERNET & SOC'Y (Sept. 13, 2011, 3:35 AM), http://cyberlaw.stanford.edu/node/6730 (discussing an empirical review of tracking, finding that "[m]ost desktop browsers currently do not support effective self-help tools" and "vary substantially in performance").

118. *See* Ben Sisario, *7 Charged as F.B.I. Closes a Top File-Sharing Site*, N.Y. TIMES, Jan. 19, 2012, http://www.nytimes.com/2012/01/20/technology/indictment-charges-megaupload-site-with-piracy.html; *see also* sources cited *supra* note 29.

119. *See* sources cited *supra* note 29.

free-market view argues that corporations are free to take what they want, but consumers must pay (in terms of time spent surveying varied and complex privacy policies or buying privacy-enhancing technologies) to make it stop.[120] That is neither a market nor free. A free market would involve legal protection for consumer interests, as expressed in contractual terms, that is at least equal to a corporation's ability to do likewise.

One predictable pushback is that leveling the playing field between consumer- and corporate-drafted contracts is only necessary if a consumer's other technological self-help options are inadequate. They plainly are—it is nearly impossible for a consumer to achieve even a low level of security.[121] First of all, every application has a different threat profile.[122] Since every application has to legitimately demand control over a significant amount of data and

120. In a Coasean transaction-free universe, this would not be a problem. The difficulty is that the transaction costs in online contracting are backwards: it is cheaper for users to express their preference not to be tracked once, in a single, unitary do-not-track option in their browser, than for users to read and navigate thousands of privacy policies on thousands of sites. *See* LESSIG, *supra* note 30; *see also* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J. L. & POL'Y FOR INFO. SOC'Y 543, 544-50 (2008-09) ("Studies show privacy policies are hard to read, read infrequently, and do not support rational decision making. . . . Privacy policies should help reduce information asymmetries because companies share information with their customers. However, researchers also note that if the cost for reading privacy policies is too high, people are unlikely to read policies."); Jeff Sovern, *The Coase Theorem and the Power to Increase Transaction Costs*, 40 MCGEORGE L. REV. 935, 943 (2009) [hereinafter *Coase and Transaction Costs*] ("The ability of financial institutions to inflate consumer transaction costs is not unique. . . . Online sellers sometimes hide unattractive terms in privacy notices."); Jeff Sovern, *Toward a New Model of Consumer Protection: The Problem of Inflated Transaction Costs*, 47 WM. & MARY L. REV. 1635, 1637 (2006) [hereinafter *Consumer Protection*] ("In many circumstances, businesses benefit by increasing consumer transaction costs to the detriment of consumers. Indeed some practices are profitable largely because they inflate consumer transaction costs. Accordingly, firms increase consumer transaction costs because doing so enriches them.").

121. *See* Valentino-Devries, *supra* note 44 ("Ironically, these opt-out systems work by installing a cookie on your computer. That cookie tells ad networks to stop sending targeted ads to your computer. Because these systems rely on a cookie to work, you'll need to opt out all over again any time you delete cookies from your machine."); *see also* Michael Riley & Sara Forden, *Hacking of DuPont, J&J, GE Were Google-Type Attacks That Weren't Disclosed*, BLOOMBERG (Mar. 8, 2011, 5:01 PM), http://www.bloomberg.com/news/2011-03-08/hacking-of-dupont-j-j-ge-were-google-type-attacks-that-weren-t-disclosed.html ("'You can't buy enough security to match the threat today,' said Anup Ghosh, chief executive officer of the cyber security firm Invincea Inc. . . . '[W]e continue to find malware from early 2009 . . .' one HBGary investigator wrote . . . ."). These two comments are in the context of hackers and large corporations and government entities. *See* Riley & Forden, *supra*. The example is clear—these large corporations can scarcely protect themselves. *See id*.

122. *See* Drew & Kopytoff, *supra* note 54 ("Companies like Symantec, the giant Internet security firm, are introducing services that assess the 'reputation' of software, weighing factors like how old it is and how widely it is used to decide if it is safe."); *see also* Fowler, *supra* note 113 ("'Facebook's complex ecosystem—with thousands of independent apps and complex data flows to and from apps—is a problem of its own creation,' said Ben Edelman, an assistant professor at Harvard Business School.").

computer-processing power in order to function, the human user cannot vet every decision each application makes.[123]

Second, even consumers who responsibly use antivirus and anti-intrusion programs, and who fairly regularly dispose of junk information by using cleaning programs, remain at significant risk. Grey-market companies still rely on the complexity of computer use and disposal of information to gather information about the user.[124] Similarly, security over the wire, like basic encryption, can be prohibitive to obtain because most websites and browsers do not accept or allow encrypted connections.[125] Even the most basic safeguards, therefore, such as requesting an encrypted connection, are often simply not available to the consumer.[126]

Moreover, encrypted connections do not provide complete protection. Encrypted connections can be analyzed by the type of traffic. For example, deep-packet inspection technology currently permits ISPs to differentiate Internet traffic—telephony, movies, music, and so on—and charge separate prices for different kinds of traffic.[127] Further, governments have circumvented strong encryption by using software that hacks a user's computer and intercepts communications before it becomes encrypted.[128] Thus, the

123. *See* Barnes, *supra* note 114, at 253-59.

124. *See* Thurm & Kane, *supra* note 5.

125. *See* Klinefelter, *supra* note 24, at 15 ("While some research websites such as LexisNexis, Westlaw, and Google Search allow for . . . encrypted communication, a number of websites that attorneys use . . . do not . . . . For example, twenty-seven state bar associations provide access to the legal research service Casemaker as a benefit of membership, but this service does not offer encrypted access." (footnote omitted)); *see also* Murphy, *supra* note 83 ("[W]hile the password you initially enter on Web sites like Facebook, Twitter, Flickr, Amazon, eBay and The New York Times is encrypted, the Web browser's cookie, a bit of code that that identifies your computer, your settings on the site or other private information, is often not encrypted.").

126. *See* sources cited *supra* note 125.

127. *See* Klinefelter, *supra* note 24, at 14 n.62 (discussing how deep-packet inspection of the contents of Internet communications gives service providers the option to prioritize or create tiered pricing by type of communication in order to address the challenges to the capacities of Internet infrastructure); *see also* Saul Hansell, *The Economics of Snooping on Internet Traffic*, N.Y. TIMES, Mar. 25, 2009, http://bits.blogs.nytimes.com/2009/03/25/the-economics-of-snooping-on-internet-traffic ("There are a lot of other things deep packet inspection can do that are perceived as rather creepy. It is great for spies and secret police, who want to know when people read or write about certain topics. It can identify people who send copyrighted files and block people from using certain programs, like BitTorrent. Advertisements can be shown based on what sites Internet users visit.").

128. *See* Steve Stecklow et al., *Mideast Uses Western Tools to Battle the Skype Rebellion*, WALL ST. J., June 1, 2011, http://online.wsj.com/article/SB10001424052702304520804576345970862420038.html ("In recent years, a handful of small European companies . . . have developed tools to eavesdrop on Skype. . . . Most of the tools are programs that must be installed on a person's computer. Often they are distributed via infected email attachments . . . . The software doesn't decode Skype's encryption, but instead captures audio streams . . . on the computer.").

technological arms race continues, and individual consumers are largely the losers.

These are just the problems of encryption—the difficulties involved in protecting what is inside one's own communications. Another serious concern is *with whom* one is communicating. Democracy activists in authoritarian regimes particularly care about protecting the identity of parties with whom they communicate.[129] Unsurprisingly, there are far fewer resources available to protect individuals who want to keep this information private than there are available to help governments.[130]

The only current, but imperfect, solution to traffic analysis[131] is a proxy. A proxy is a computer that acts as an untraceable post office box for an Internet user.[132] A traffic analyst can track the communication back to the proxy, but not to the person who was using it.[133] Yet there are several problems with using proxies to prevent unwanted traffic analysis. First, proxies sometimes retain data logs of their users' activities.[134] If they do, all of the problems engendered by corporate retention of consumer data still arise.[135] In addition, proxies that retain user activity logs are one-stop shops for government

---

129. *Id.* ("[Y]oung dissidents in Egypt were organizing an election-monitoring project last fall, they discussed their plans over Skype . . . believing it to be secure. But someone else was listening in—Egypt's security service. An internal memo . . . boasted it had intercepted one conversation in which an activist stressed the importance of using Skype 'because it cannot be penetrated online by any security device.'").

130. *Id.* ("A cottage industry of U.S. and other companies is now designing and selling tools that can be used to block or eavesdrop on Skype conversations. . . . To enter the Chinese market in 2004, Skype agreed to a unique arrangement in which a special version of its software there filters users' text chats and blocks politically sensitive keywords."); *see also* 47 U.S.C. § 1002 (2006); Rubinstein et al., *supra* note 5, at 281 ("Congress enacted CALEA to preserve the ability of law enforcement officials to conduct electronic surveillance involving digital telephony. This law requires telecommunications carriers and manufacturers of telecommunications equipment to design their equipment, facilities, and services to ensure that a required level of surveillance capabilities will be built in.").

131. That is, tools employed by service providers, recipient websites, bad actors, or others to determine to which websites a user is connected. *See generally* Adam Candeub & Daniel John McCartney, *Network Transparency: Seeing the Neutral Network*, 8 NW. J. TECH. & INTELL. PROP. 228, 228-30 (2010) (discussing the problems faced by the Internet and the fundamental need for traffic analysis, ensuring effective communications but screening for unwanted content).

132. *See* Joel Michael Schwarz, *'A Case of Identity': A Gaping Hole in the Chain of Evidence of Cyber-Crime*, 9 B.U. J. SCI. & TECH. L. 92, 95 (2003) ("[T]he proxy server often functions as a security gate and firewall between the internal network and the public Internet. To accomplish this, a proxy server substitutes its own IP address for the IP addresses of its subordinate computers behind the firewall, thus preserving their anonymity by masking their IP addresses from anyone outside on the Internet." (footnote omitted)).

133. *Id.*

134. *Id.* at 95-96 ("[A]t the time traffic passes into and out of the proxy server/firewall, the proxy server often captures the source and destination IP addresses, thereby giving rise to a virtual footprint.").

135. *See supra* text accompanying notes 9-14.

entities that wish to record user traffic.[136] Since the traffic is communicated to a third party, courts generally do not require a warrant.[137] While handing a letter to a US postal service worker, a government employee, does not permit the government to open it,[138] courts have persisted in allowing governments to review users' activity logs.[139] But, the present inquiry views privacy through the lens of contract law and does not make constitutional analyses and arguments, however numerous and important they may be.[140]

The second problem is that proxies do not prevent traffic analysis because the tools for traffic analysis are advancing. Social networks are mappable and trackable.[141] A person's social network

---

136. *See* Schwarz*, supra* note 132, at 98-100 (detailing the use of virtual "footprints" and the use of proxy servers as they stored data in *United States v. Hoke*, the first major online securities fraud cases).

137. *See In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), No. 1:11-DM-3, 2011 WL 5508991, at *17 (E.D. Va. Nov. 10, 2011) ("Even if Petitioners had a reasonable expectation of privacy in IP address information collected by Twitter, Petitioners voluntarily relinquished any reasonable expectation of privacy under the third-party doctrine. To access Twitter, Petitioners had to disclose their IP addresses to third parties."); *see also* United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."). *But see* United States v. Warshak, 631 F.3d 266, 274 (6th Cir. 2010) ("[Plaintiff] enjoyed a reasonable expectation of privacy in his emails vis-à-vis . . . his Internet Service Provider. Thus, government agents violated his Fourth Amendment rights by compelling [his ISP] to turn over the emails without first obtaining a warrant based on probable cause." (citation omitted)). The court made this holding based upon the analogy of emails and the Internet to the US postal system. *Id.* at 286.

138. *See Warshak*, 631 F.3d at 286 ("[T]he police may not storm the post office and intercept a letter . . . .").

139. *Compare Miller*, 425 U.S. at 443 (detailing the role of a recipient of information and the loss of Fourth Amendment protections), *with Warshak*, 631 F.3d at 288 (distinguishing from an intended recipient and finding the ISP in the case was an intermediary). If we accept that an email is analogous to a letter or a phone call, it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment. *See generally Warshak*, 631 F.3d at 286. An ISP is the intermediary through which emails must pass in order for email communication to be possible. Mike Masnick, *Appeal Court Says Emails are Protected by the 4th Amendment*, TECHDIRT (Dec. 14, 2010, 3:09 PM), http://www.techdirt.com/articles/20101214/12144812273/appeals-court-says-emails-are-protected-4th-amendment.shtml.

140. *See, e.g.*, Kerr, *supra* note 41, at 563, 563 n.5 ("The third-party doctrine is the Fourth Amendment rule scholars love to hate. It is the Lochner of search and seizure law, widely criticized as profoundly misguided. . . . A list of every article or book that has criticized the doctrine would make this the world's longest law review footnote.").

141. *See* Nate Anderson, *How One Man Tracked Down Anonymous—And Paid a Heavy Price*, ARS TECHNICA (Feb. 10, 2011, 3:31 AM), http://www.wired.com/threatlevel/2011/02/anonymous/all/1 ("Aaron Barr [the CEO of security firm HBGary Federal] believed he had penetrated Anonymous . . . [the] loose hacker collective . . . . But matching their online identities to real-world names and locations proved daunting . . . . Barr . . . used social media data and subterfuge to map those names to three real people, two in California and one in New York.").

and online contacts are serviceable digital fingerprints.[142] The final problem is that protections from online service providers are negligible or impracticable.[143] Each site has its own hidden and obscure "privacy policy,"[144] which is in fact the terms under which the corporation will expropriate the users' data.[145] These privacy policies are take-it-or-leave-it propositions that are generally applicable; one size fits all members who access a site.[146]

A consumer who wishes to protect her privacy through self-help must use encryption on her computer and must read and judge thousands of pages of EULAs for the programs she installs.[147] She must use a browser that permits her to refuse cookies. She must request secure connections wherever possible.[148] She must use traffic analysis avoidance software, such as the TOR Onion Router, which bounces traffic all over the world before it exits from an anonymized node.[149] She must use AdBlock Plus or some similar add-on to prevent banner advertisements from reporting her online traffic.[150] If she

142. *Id.*

143. *In re* Facebook Privacy Litig., 791 F. Supp. 2d 705, 714 n.8 (N.D. Cal. 2011) ("[H]olding that a defendant was not liable under the Stored Communications Act for disclosing personal information of which it was the intended recipient, even if the defendant was 'contractually bound by its privacy policy not to disclose . . . information' and could be held liable for breach of contract for doing so." (citing *In re* Am. Airlines, Inc., Privacy Litig., 370 F. Supp. 2d 552, 560-61 (N.D. Tex. 2005)).

144. *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, 4 (2005) ("[D]espite the proliferation of privacy policies online, consumers' privacy interests may in fact be no better protected today than they were ten years ago. . . . [T]here may be little incentive for online businesses to adopt and adhere to strong privacy policies. It is the appearance of privacy that seems to matter most."); *see also* Thurm & Kane, *supra* note 5 ("An examination of 101 popular smartphone 'apps' . . . . reveal[s] the intrusive effort by online-tracking companies to gather personal data . . . . Forty-five of the 101 apps didn't provide privacy policies on their websites . . . .").

145. *See* In re *Facebook Privacy Litig.*, 791 F. Supp. 2d at 714; Julia Angwin & Tom McGinty, *Sites Feed Personal Details to New Tracking Industry*, WALL ST. J., July 30, 2010, http://online.wsj.com/article/SB10001424052748703977004575393173432219064.html ("Dictionary.com . . . installed 168 tracking tools that didn't let users decline to be tracked, and 121 tools that, according to their privacy statements, don't rule out collecting financial or health data.").

146. *See, e.g.*, Comb v. PayPal, Inc., 218 F. Supp. 2d 1165, 1169 (N.D. Cal. 2002) (describing the user agreement of PayPal).

147. *See* Vance, *supra* note 55 (discussing the different antivirus companies); *see also McAfee Consumer Products End User License Agreement*, MCAFEE, http://home.mcafee.com/root/aboutus.aspx?id=eula (last visited Dec. 28, 2011); *Product License Agreements*, SYMANTEC, http://www.symantec.com/about/profile/policies/eulas (last visited Dec. 28, 2011) (linking to the numerous different products for consumer use and their license agreements).

148. *See* Stecklow et al., *supra* note 128; *see also* Soghoian, *supra* note 84.

149. *See* Paul Ohm, *Good Enough Privacy*, 2008 U. CHI. LEGAL F. 1, 44 (2008).

150. *See Getting Started with Adblock Plus*, ABLOCK PLUS, http://adblockplus.org/en/getting_started (last visited Dec. 18, 2011) (describing Adblock Plus as a program that blocks advertisements on websites and can be modified with filters based on geographic location or

carries a cellular phone, she faces the same difficulties with the added problem that the mobile device tracks her everywhere she travels in real space.[151] And even if she finds applications that block, delete, or redirect this information, recent scientific studies show that third parties can still track her.[152]

Instead of permitting this unreasonable situation to persist, the law should permit a consumer to select a simple one-time browser option that expresses her unwillingness to be tracked.[153] Courts could enforce that simple term the way they have been enforcing corporate contracts for years—favorably.

II. OUTLINING ONLINE CONTRACTING LAW

This Part discusses some trends in online contracting law, and isolates the impulses and analyses that have caused courts to systematically enforce corporate terms against consumers,[154] while denying consumers the right to proffer their own terms against

---

privacy preferences). *But see Allowing Acceptable Ads in Adblock Plus*, ADBLOCK PLUS, http://adblockplus.org/en/acceptable-ads (last visited Dec. 17, 2011) (discussing the switch to a changeable default setting where non-intrusive advertisements will be allowed where before they were not).

151. *See* Julia Angwin & Scott Thurm, *Judges Weigh Phone Tacking*, WALL ST. J., Nov. 9, 2011, http://online.wsj.com/article/SB10001424052970203733504577024092345458210.html ("The use of cellphone tracking by authorities is among the most common types of electronic surveillance, exceeding wiretaps and the use of GPS tracking, according to a survey of local, state and federal authorities by *The Wall Street Journal*."); *see also* Valentino-Devries, *supra* note 44 (detailing the steps that users can take to avoid being tracked online, such as browser setting changes and the different programs a user can download and manage).

152. *See* Pedro G. Lean et al., *Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising*, CARNEGIE MELLON U. CYLAB (Oct. 31, 2011), http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11017.pdf ("We present results of a 45-participant laboratory study investigating the usability of tools to limit online behavioral advertising (OBA). . . . None of the nine tools we tested empowered study participants to *effectively* control tracking and behavioral advertising according to their personal preferences." (emphasis added)); Valentino-Devries, *supra* note 44 ("If you opt out, you won't be shown ads tied to your browsing behavior from the member networks. But you'll still see ads, which may be placed based on criteria such as your location.").

153. *See* Nick Wingfield & Julia Angwin, *Microsoft Adds Do-Not-Track Tool to Browser*, WALL ST. J., Mar. 15, 2011, http://online.wsj.com/article/SB10001424052748703363904576200981919667762.html (discussing Microsoft's implementation of a Do-Not-Track feature); *Mozilla: Do Not Track*, MOZILLA, http://dnt.mozilla.org (last visited Oct. 3, 2011) (noting that Mozilla Firefox includes a Do Not Track option); *see also Allowing Acceptable Ads in Adblock Plus*, *supra* note 150 ("In particular, we want to require that user's privacy is respected (mandatory Do Not Track support). However, we are not yet in a position to enforce that requirement.").

154. *See* Hartzog, *supra* note 3, at 1635-36 ("Courts rarely look to the privacy settings or other elements of a website where users specify their privacy preferences because these settings and elements are typically not considered part of any contract or promise to the user."); Knapp, *supra* note 6 (discussing how dominance of the drafter has become typical in contract law).

corporations.[155] Even well-meaning courts cannot build contracts that protect consumer privacy using only corporate-drafted terms.[156]

Before beginning the legal discussion, a statement of limitations is appropriate. There is an extensive and developed literature on the various rules of contract formation, and the rules' moral and economic ramifications.[157] This Article does not replicate that research, rather, this Article mentions several example rules, laws, and cases for what they fail to accomplish: they do not generally operate to permit consumers to offer and enforce their own online contract terms.[158] The rules mentioned are regularly used to construe only the corporation's contractual terms.[159] Courts only enforce the consumers' preferences to the extent that the corporate contract embodies them: either actually (rare except for the price and quantity terms)[160] or impliedly (by courts seeking to construe corporate contract terms in a pro-consumer fashion).[161] This preference for corporate-drafted terms does not appear within the legal rules

155. *See* Marotta-Wurgler, *supra* note 21 (addressing the lack of consumer choice in accepting boilerplate language in standard form contracts).

156. *See* Mark E. Budnitz, *The Development of Consumer Protection Law, the Institutionalization of Consumerism, and Future Prospects and Perils*, 26 GA. ST. U. L. REV. 1147, 1169-70 (2010) ("One key element is the courts' effective elimination of the concept of agreement. There is no 'meeting of the minds' . . . . [C]ontracts are presented on a take-it-or-leave-it basis. In many situations, courts enforce contracts and changes in contract terms as long as the company notified the consumer . . . . Notice has replaced agreement as a crucial element of contract formation." (footnotes omitted)); *see also* Larry A. DiMatteo & Bruce Louis Rich, *A Consent Theory of Unconscionability: An Empirical Study of Law In Action*, 33 FLA. ST. U. L. REV. 1067, 1072 (2006) ("[T]he common law doctrine of unconscionability has proved difficult to define and has been rarely invoked undoubtedly because, other than in exceptional cases, it has been largely viewed as grossly interfering with the freedom of contract." (internal quotation marks omitted)); Hillman & Rachlinski, *supra* note 66; Knapp, *supra* note 6; Lemley, *supra* note 6.

157. *See, e.g.*, Budnitz, *supra* note 156; Giesela Rühl, *The Battle of the Forms: Comparative and Economic Observations*, 24 U. PA. J. INT'L ECON. L. 189 (2003); Amelia Rawls, Note, *Contract Formation in an Internet Age*, 10 COLUM. SCI. & TECH. L. REV. 200 (2009).

158. *See* Knapp, *supra* note 6.

159. *See id.*; *see also* Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 29-30 (2d Cir. 2002) ("[A] consumer's clicking on a download button does not communicate assent to contractual terms if the offer did not make clear to the consumer that clicking on the download button would signify assent to those terms . . . ."); Fisher v. MediSense, Inc., No. 95-1004-PFK, 1995 WL 396613, at *6 (D. Kan. June 29, 1995) ("Undue influence is not proven, nor is a contract unconscionable, merely because a corporation drafts a contract.").

160. *See, e.g.*, Cole v. Sandel Med. Indus., LLC, 413 F. App'x 683, 686-87 (5th Cir. 2011) ("[I]t is clear that no contract was created between Cole and Sandel when she submitted her idea via the online submission form. . . . The agreement left open what price, if any, would be paid to Cole. Accordingly, the online submission form is not an enforceable agreement to compensate Cole for her idea.").

161. *See, e.g.*, *Specht*, 306 F.3d at 29-30; *see* Knapp, *supra* note 6.

themselves, but rather in how those rules are actually applied.[162] This opens the door for this Article's argument: courts should bind corporations to consumer-expressed preferences in exactly the same way that courts have bound consumers to corporate-drafted contract terms.

A. Corporate and Consumer Contracts under Online Contracting Regimes

For online service transactions, courts use regular, common-law rules for contracting—often drawn from the *Restatement of Contracts*.[163] The application of Restatement rules often favors corporations under the "mirror image"[164] or common-law "last shot" rule,[165] since the corporation is able to structure the transaction in such a way as to benefit itself.[166] The Restatement contains some useful provisions for limiting corporate contractual overreaching—unconscionability,[167] for example—by finding that a consumer is not bound by what she has not understood to be part of

---

162. *See Fisher*, 1995 WL 396613, at *6 ("Undue influence is not proven, nor is a contract unconscionable, merely because a corporation drafts a contract."); *see also* DiMatteo & Rich, *supra* note 156; Hartzog, *supra* note 3, at 1635-36.

163. *See e.g.*, Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1099 (9th Cir. 2009) ("Barnes also refers in her complaint and in her briefs to Yahoo's 'promise' to remove the indecent profiles and her reliance thereon to her detriment. We construe such references to allege a cause of action under section 90 of the Restatement (Second) of Contracts (1981).").

164. RESTATEMENT (SECOND) OF CONTRACTS § 59 (1981).

165. *See* Rich Prods. Corp. v. Kemutec, Inc., 66 F. Supp. 2d 937, 959 (E.D. Wis. 1999) ("'[T]he terms of the party who sent the last form, typically the seller, would become the terms of the parties contract. This result was known as the "last shot rule."' Recognizing the growing impracticality of such rules in the modern economy, the drafters of the UCC 'change[d] the common law in an attempt to conform contract law to modern day business transactions.'" (citations omitted)), *aff'd*, 241 F.3d 915 (7th Cir. 2001).

166. *See* O'Quin v. Verizon Wireless, 256 F. Supp. 2d 512, 516 (M.D. La. 2003); i.Lan Sys., Inc. v. Netscout Serv. Level Corp., 183 F. Supp. 2d 328, 336-38 (D. Mass. 2002); *see also* Barnes, *supra* note 114, at 239 ("[S]tandard form contracts signed by consumers pose problems that are not present in traditional, heavily negotiated agreements between merchants. These problems include the difference in bargaining strength between the parties to the contract, the adhesive nature of the terms, and the problem of terms not being read by consumers." (footnote omitted)); *Barnes*, *supra* note 114, at 240 ("The consumer has no real choice in the matter of whether the terms will be part of the contract or not, and the forms are all one-sided and designed to benefit the drafting enterprise. The consumer is essentially put at the mercy of the form-drafting business." (footnote omitted)); Rühl, *supra* note 157, at 212-13 ("[I]t becomes obvious that the last-shot rule, despite or because it provides a clear and strict rule . . . . encourages an extensive exchange of standard forms because both [companies] know that the other party's standard terms will control the complete transaction if the other party manages to make the last offer.").

167. RESTATEMENT (SECOND) OF CONTRACTS § 208; *see also* David Horton, *Unconscionability Wars*, 106 NW. U. L. REV. COLLOQUY 13, 13 (2011) ("The unconscionability doctrine has emerged as the primary check on drafter overreaching.").

the contract.[168] But unconscionability is fairly strongly circumscribed,[169] especially after the Supreme Court's recent decision in *AT&T Mobility LLC v. Concepcion*.[170]

Since software is often sold off the shelves in boxes, some courts have applied Uniform Commercial Code (UCC) Article 2 to e-commercial sales of software, even when the goods in question are in fact licenses to use software products.[171] And, of course, many online transactions are simply sales of real goods over the Internet. Thus, for cases involving sales of goods online, or retail sales of software, courts often use UCC Article 2, which covers sales of goods. UCC 2-207, the famed battle of the forms provision, resolves competing terms in the parties' offer and acceptance.[172]

UCC 2-207 offers a range of possible interpretations that generate rules for contract formation. These interpretive rules in turn determine which of a competing set of contract terms the court will deem operative.[173] As between businesses, some cases resolve

---

168. *See* Williams v. Walker-Thomas Furniture Co., 350 F.2d 445, 449-50 (D.C. Cir. 1965); *see also* Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 29-30 (2d Cir. 2002).

169. *See* DiMatteo & Rich, *supra* note 156, at 1068-72.

170. AT&T Mobility LLC v. Concepcion, 131 S. Ct. 1740, 1753 (2011) (holding that California's rule classifying most collective-arbitration waivers in consumer contracts as unconscionable was pre-empted by the Federal Arbitration Act (FAA) and the FAA's goal of enforcing arbitration clauses). AT&T had an arbitration clause in its mobile phone contract that waived class action suits by consumers. The Concepcions, consumers who purchased the AT&T plan in order to get the free phone, filed suit against AT&T alleging that AT&T fraudulently charged them tax on the phone, because AT&T had stated in its advertisement that consumers would get a free phone with the purchase of a plan. Under prior California precedent, waiver of class arbitration in consumer contracts of adhesion was unconscionable in certain circumstances and therefore unenforceable. In addition, the FAA did not preempt California's state law prohibition of class action waivers in arbitration agreements. Discover Bank v. Super. Ct., 113 P.3d 1100 (Cal. 2005), *abrogated by* AT&T Mobility LLC v. Concepcion, 131 S. Ct. 1740 (2011); *see also* Horton, *supra* note 167, at 14 ("Justice Thomas implies that *nobody* can apply unconscionability to arbitration clauses. . . . Because Justice Thomas provided the swing vote in *Concepcion,* and invited parties to address the link between §§ 2 and 4 in the future, he ensured that unconscionability's viability will become a flashpoint in the arbitration wars." (footnotes omitted)).

171. Recursion Software, Inc. v. Interactive Intelligence, Inc., 425 F. Supp. 2d 756, 786 n.17 (N.D. Tex. 2006).

172. *See* IFC Credit Corp. v. United Bus. & Indus. Fed. Credit Union, 512 F.3d 989, 992 (7th Cir. 2008) ("Terms in form contracts are routinely enforced under the UCC, unless a 'battle of the forms' occurs . . . or the term would be unconscionable . . . .").

173. *See* PCS Nitrogen Fertilizer, LP v. Christy Refractories, LLC, 225 F.3d 974, 977 (8th Cir. 2000) ("Applying Article 2 of the . . . (UCC), the district court held that, because . . . acceptance was expressly conditional upon . . . assent to additional terms . . . no contract was formed under UCC § 2–207(1). The district court alternatively determined that, even if . . . customer acknowledgment was a valid acceptance under § 2–207(1), the provisions of § 2–207(2) prevented incorporation of . . . added terms because the[re] . . . was a material alteration of the contract. Finally, the district court held that the additional arbitration terms could not qualify as a supplemental term under § 2–207(3) given the parties' limited course of dealing." (footnote omitted) (citations omitted)).

differing terms in the offer and acceptance by merging non-conflicting unimportant terms under 2-207(2).[174] Other cases apply a judicial gloss through the so-called "knockout rule" to eliminate differing terms and fill any resulting gaps with commercial default rules.[175] As between a merchant and non-merchant, UCC 2-207(2), at least technically, creates a "first shot rule," which courts occasionally interpret to favor consumers—who make the "first shot" by initiating a purchase.[176] More often, UCC 2-207(2) operates to favor corporations as firing the "first shot",[177] since the corporate EULA or Terms of Use are the first website terms that the user encounters.[178]

The real problem, though, lies not with whether courts enforce corporate terms as the "first shot," or enforce corporate terms as the "last shot." The issue is that a significant number of courts are applying a de facto "only shot" rule.[179] That is, by not recognizing or

---

174. *See, e.g.*, Aceros Prefabricados, S.A. v. TradeArbed, Inc., 282 F.3d 92, 100 (2d Cir. 2002) ("'[T]he burden of proving the materiality of the alteration must fall on the party that opposes inclusion.' This is so because the UCC presumes that between merchants additional terms will be included in a contract. Thus, 'if neither party introduced any evidence, the [proposed additional term] would, by the plain language of § 2-207(2), become part of the contract.'" (alteration in original) (citations omitted)).

175. *See, e.g.*, SCM Grp., USA, Inc. v. Custom Designs & Mfg. Co., 89 F. App'x 779, 780 (3d Cir. 2004) ("[T]he Pennsylvania Superior Court has issued an opinion in which it holds that the 'knockout rule' applies to contracts governed by Article 2 of the U.C.C. . . . As such, we hold that neither the original terms nor the handwritten changes, which were obviously 'different' and not simply 'additional' terms, control the issue of acceptance. Instead, we look to the U.C.C. to supply the default terms of acceptance." (citation omitted)).

176. *See* Klocek v. Gateway, Inc., 104 F. Supp. 2d 1332, 1340 (D. Kan. 2000) ("In typical consumer transactions, the purchaser is the offeror, and the vendor is the offeree."); DeFontes v. Dell, Inc., 984 A.2d 1061, 1067 (R.I. 2009) ("The U.C.C. creates the assumption that, unless circumstances unambiguously demonstrate otherwise, the buyer is the offeror and the seller is the offeree."); *see also* Rich Prods. Corp. v. Kemutec, Inc., 66 F. Supp. 2d 937, 956 (E.D. Wis. 1999) ("[T]he purchase order usually is the first document having the legal attributes of an offer." (alteration in original) (quoting Gulf States Utils. Co. v. NEI Peebles Elec. Prods., Inc., 819 F. Supp. 538, 549 (M.D. La. 1993) (internal quotation marks omitted))), *aff'd*, 241 F.3d 915 (7th Cir. 2001).

177. *DeFontes*, 984 A.2d at 1071 ("After reviewing the case law pertaining to so-called 'shrinkwrap' agreements, we are satisfied that the *ProCD* line of cases is better reasoned and more consistent with contemporary consumer transactions. It is simply unreasonable to expect a seller to apprise a consumer of every term and condition at the moment he or she makes a purchase. . . . We therefore *decline* to adopt the *minority view*, as urged by plaintiffs, that a contract is fully formed when a buyer orders a product and the seller accepts payment and either ships or promises to ship. Instead, formation occurs when the consumer accepts the full terms after receiving a reasonable opportunity to refuse them." (emphasis added)).

178. *See* MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 935 (9th Cir. 2010) ("Each WoW player must read and accept Blizzard's End User License Agreement ('EULA') and Terms of Use ('ToU') on multiple occasions. . . . The ToU pertains to the online service, so a player agrees to it both when creating an account and upon first connecting to the online service."), *amended by denial of reh'g*, No. 09-15932, 2011 WL 538748 (9th Cir. Feb. 17, 2011).

179. *See DeFontes*, 984 A.2d at 1071 ("[W]e are satisfied that the *ProCD* line of cases is better reasoned and more consistent with contemporary consumer transactions. . . . [F]ormation

enforcing consumer expressions of preference as true contractual terms, or by finding that the corporate version of the deal is the only version,[180] these courts avoid the transaction costs they believe consumer-proffered contracts would present.[181] Or, to the extent that a court is sympathetic to consumer concerns, courts continue to try to protect consumer interests by interpreting only the corporate contract terms.[182] In other words, whatever the test, the corporate terms govern.

This tilted architecture is built upon the line of cases including *ProCD, Inc. v. Zeidenberg*[183] and *Hill v. Gateway*.[184] These cases argue that the consumer simply had not offered any contractual terms that the court could consider—that, in essence, the corporation had fired the "only shot."[185] Other courts widely follow the approach taken in these two cases.[186] Courts hold that consumers have not offered their own terms, ostensibly because such terms were not in writing, and because any writing would be superseded by the following corporate contract that came with the shipped product.[187]

---

occurs when the consumer accepts the full terms after receiving a reasonable opportunity to refuse them.").

180. *Id.*

181. *Id.* ("It is simply unreasonable to expect a seller to apprise a consumer of every term and condition at the moment he or she makes a purchase.").

182. *See id.*; *see also* Barnes, *supra* note 114, at 239-40; Horton, *supra* note 167; Knapp, *supra* note 6.

183. ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1452 (7th Cir. 1996) ("Our case has only one form; UCC § 2-207 is irrelevant. . . . What then does the current version of the UCC have to say? We think that the place to start is § 2-204(1): . . . . A vendor, as master of the offer, may invite acceptance by conduct, and may propose limitations on the kind of conduct that constitutes acceptance. A buyer may accept by performing the acts the vendor proposes to treat as acceptance. And that is what happened.").

184. Hill v. Gateway 2000, Inc., 105 F.3d 1147, 1148-49 (7th Cir. 1997) (finding *ProCD* to be controlling, specifically the power to control the offer and set its terms). "Plaintiffs ask us to limit *ProCD* to software, but where's the sense in that? *ProCD* is about the law of contract, not the law of software." *Id.* at 1149.

185. *See id.* at 1148-49; *ProCD*, 86 F.3d at 1452 ("A vendor, as master of the offer, may invite acceptance by conduct, and may propose limitations on the kind of conduct that constitutes acceptance. A buyer may accept by performing the acts the vendor proposes to treat as acceptance."). *But see* Klocek v. Gateway, Inc., 104 F. Supp. 2d 1332, 1340 (D. Kan. 2000) ("[T]he Seventh Circuit provided no explanation for its conclusion that 'the vendor is the master of the offer.' . . . In typical consumer transactions, the purchaser is the offeror, and the vendor is the offeree." (citations omitted)). In *ProCD*, Judge Easterbrook looked to UCC § 2-204(1) and determined that contracts can be formed in a variety of ways, and having a splash screen was one of them. *ProCD*, 86 F.3d at 1452.

186. *DeFontes*, 984 A.2d at 1069-71 ("The defendants argue that *ProCD* represents the majority view and we have found considerable support for their contention.").

187. *See id.* at 1069 ("[A]dopting ProCD analysis but noting shrinkwrap agreement explicitly instructed consumers 'IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, PROMPTLY RETURN * * * TO THE PLACE OF PURCHASE AND YOUR

Moreover, in the *Hill* and *ProCD* approach, courts often go to significant lengths to reinterpret the moment of contract formation to ensure that the corporate drafter is the "offeror," and the consumer accepts the corporate-proffered terms.[188] In *Hill v. Gateway*, the court determined that the consumer did not offer, in the legal sense, to buy a computer when he called Gateway and ordered a computer.[189] That would have made the consumer's terms govern, since Gateway promptly accepted the offer by shipping the computer, as is permitted under UCC 2-206.[190] Indeed, under the "first shot" rule of 2-207(2), had the court deemed the Hills the offerors, all additional terms to the original agreement would be mere proposals for modification and not part of the contract. But the court deemed that the Hills were not the offerors, and also found that the parties did not form a contract even when the computer arrived with the contract enclosed.[191] Rather, the court found that the Hills, by not returning the computer, accepted Gateway's contract terms nearly a month afterward.[192] The idea that there was no contract as of the point of the initial telephone order is odd.[193] The parties had agreed on a sale and a price,[194] and would have had a cause of action if one party had not performed.[195] But courts continue to shuffle offer and acceptance until they come to the unfortunate result: the corporate contractual terms prevail.

PURCHASE PRICE WILL BE REFUNDED . . . ." (citing M.A. Mortenson Co. v. Timberline Software Corp., 998 P.2d 305, 308 (Wash. 2000))).

188. *See id.* at 1067-70. *But see Klocek*, 104 F. Supp. 2d at 1339 ("The Court is not persuaded that Kansas or Missouri courts would follow the Seventh Circuit reasoning in *Hill* and *ProCD*. In each case the Seventh Circuit concluded without support that UCC § 2-207 was irrelevant because the cases involved only one written form.").

189. *Gateway*, 105 F.3d at 1150 ("The question in *ProCD* was not whether terms were added to a contract after its formation, but how and when the contract was formed—in particular, whether a vendor may propose that a contract of sale be formed, not in the store (or over the phone) with the payment of money or a general 'send me the product,' but after the customer has had a chance to inspect both the item and the term. . . . At oral argument the Hills propounded still another distinction: the box containing ProCD's software displayed a notice that additional terms were within, while the box containing Gateway's computer did not. The difference is functional, not legal.").

190. *See* U.C.C. § 2-206(1)(b) (2003) ("[A]n order or other offer to buy goods for prompt or current shipment shall be construed as inviting acceptance either by a prompt promise to ship or by the prompt or current shipment of conforming or nonconforming goods . . . .").

191. *Gateway*, 105 F.3d at 1148-50.

192. *Id.* at 1150 ("By keeping the computer beyond 30 days, the Hills accepted Gateway's offer . . . .").

193. *See* U.C.C. § 2-206(1)(b).

194. *See id.* § 2-201 (establishing partial payment as grounds for satisfying the Statute of Frauds).

195. *See id.* § 2-206 (inviting acceptance of offer by any means, including shipping).

Despite this, consumers sometimes win contractual disputes with corporations.[196] But their victories only highlight the problem. Because courts only look at corporate-drafted terms even when they are attempting to protect consumer interests, consumer victories are one-shot, flash-in-the-pan victories that merely cause the corporation to rewrite its EULA or TOS to avoid the prior result in future cases.[197] Corporate victories such as *Concepcion*, however, are wide ranging and permanent. When a court validates and enforces a corporate term, like one barring class actions and requiring arbitration, other corporations include those terms in their contracts and then courts subsequently enforce those terms against more consumers.[198] In this way, consumer victories are limited to the individual case, while corporate victories redound to the benefit of all corporate drafters. Focusing on corporate-drafted contracts to protect consumer rights does not provide sufficient protection to consumers.

This one-way ratchet only works, however, because consumers cannot effectively contribute terms to their own online contracts. They are merely permitted to choose which corporate-drafted contract will bind them. When a consumer buys a product online, she selects the product, and then the seller hands her a set of inalterable terms and conditions. She may refuse to purchase, or may accept the terms. She may not, however, add or change the terms or conditions. There is no drop-down box for that.

Indeed, some courts may not enforce consumer-proffered terms even if offered in writing and in the form of a contract. As noted above, even if a court holds that a consumer had offered written contractual terms, it can easily alter which terms are considered definitive by changing who is the offeror and who is the acceptor in favor of the corporation.[199] Alternatively, a court may exclude consumer terms under the parol evidence rule (if the consumer's communication of terms took place prior to, or contemporaneously with, the transaction) or under anti-modification clause analysis (if the communication of terms came after whichever moment the court deems that the corporation's contract excluding modification became operative).[200] In this way, the law excludes the consumer from the

196. *See also* discussion *supra* note 185.

197. *See* Budnitz, *supra* note 156, at 1172; Knapp, *supra* note 6.

198. *See* Budnitz, *supra* note 156, at 1171-72; Knapp, *supra* note 6, at 117-18.

199. *See* DeFontes v. Dell, Inc., 984 A.2d 1061, 1069-71 (R.I. 2009); *see also* Budnitz, *supra* note 156, at 1172.

200. U.C.C. § 2-209(2).

contracting process if she communicates her terms before, during, or after the delivery of the corporate terms.[201]

A return to the basic contract principle that consumers may offer contract terms could resolve deep difficulties in the law of online contracting, and could have ramifications well beyond the original "do-not-track" context. A thought experiment may help define how the proposal of this Article departs from standard practice, and how much of a difference a bit of consumer contracting could make. After *Concepcion*, many believe that several forms of consumer class actions face significant additional legal hurdles.[202] Courts will hold that consumers gave up their right to go to court because of corporate-drafted and court-enforced arbitration clauses. Imagine, however, that a consumer includes a full retention-of-rights clause in her browser handshake protocol. That is, suppose that the consumer communicated to the corporation, at the moment of their first online interaction: "If you want to deal with me, you should know that I reserve all rights and remedies, and specifically reject any arbitration clause." If courts were to enforce such a contractual term, the non-trivial concerns raised by *Concepcion* would simply cease to exist.[203] Restoring power to the consumer to draft and offer contract terms would do much to ameliorate the problem of consumer powerlessness in online contracting.

Giving consumers power to proffer, and not merely accept automated contract terms online is not a radical proposal. It is easy to overlook that in the one place where corporations do permit consumers to communicate contractual preference—the quantity term in an online sales contract—the enforcement of that term is simply a matter of course. The consumer gets the number of items she ordered.

---

201. *See* Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L.J. 1283, 1307 n.121 (2005) ("For contract claims, cases [where] . . . consumer's act of breaking the shrinkwrap is deemed to be assent to the governing terms, form the foundation for courts' analysis. The trend among courts is to enforce such licenses, so long as the consumer has a right to reject the terms by returning the product."). "[C]ourts . . . have broadly construed license agreements in favor of licensors – even when it is questionable whether the licensee has manifested assent to particular notices provided by the licensor." *Id.* at 1306-07.

202. *See* Ashby Jones, *After AT&T Ruling, Should We Say Goodbye to Consumer Class Actions?*, WALL ST. J. L. BLOG (Apr. 27, 2011, 12:36 PM), http://blogs.wsj.com/law/2011/04/27/after-att-ruling-should-we-say-goodbye-to-consumer-class-actions (noting that class action suits are threatened by the result in *Concepcion*).

203. *See* Horton, *supra* note 167 ("The unconscionability doctrine has emerged as the primary check on drafter overreaching."); Knapp, *supra* note 6; *see also* Stephen E. Friedman, *A Pro-Congress Approach to Arbitration and Unconscionability*, 106 NW. U. L. REV. COLLOQUY 53, 54-57 (2011) ("This Essay . . . responds to some of Professor Horton's objections to my position. . . . *Concepcion* invites us to ask whether unconscionability really is within § 2 at all. That is, rather than put unconscionability into a tiny cage in which it can barely move, why not put it out of its misery altogether in the context of arbitration provisions . . . .").

Outside of the consumer context, courts routinely give legal effect to buyer-side machine-automated contract terms.[204] When a computer in a business-to-business transaction orders a product—for example in the extremely common practice of Electronic Data Interchange (EDI)—the buyer and seller have usually worked out the terms and conditions in advance as part of an overall EDI agreement.[205] Machines make the contracts, and the terms of the purchasing machine's contract are as binding upon the seller as the terms of the selling machine's contract are upon the buyer.[206]

Likewise, when one website wishes to exclude robots and scrapers from its service, the website posts a file called "robots.txt" that includes the restrictions on scraping.[207] These restrictions are readable by other people's scrapers and agents, and are quite binding: if the scraper continues despite the preferences expressed in the robots.txt file, courts have analogized the resulting server load to trespassing on someone's land without permission.[208] Thus, automated contracts are enforced. Buyer-side contracts are enforced. Buyer-side automated contracts are enforced. But *consumer* buyer-side automated contracts—such as a contractual do-not-track term included in a browser—are often either ignored or swept under the rug as not comprising part of the contract.

A critical question to answer is why courts disfavor consumer contract terms in the online context. First, courts may be crudely attempting to streamline online contracting, or at least to simplify their work in construing online contracts. Courts like corporate contracts. Corporations draft contracts in legal language, in a format that the court recognizes, and with strong mechanisms of acceptance, like clicking an "I Accept" button, or scrolling to the bottom of the legal document. Thus, in order to keep things simple, courts have turned to

---

204. *See* UNIF. COMPUTER INFO. TRANSACTIONS ACT § 107(a) (2002); *see also* Baney Corp. v. Agilysys NV, LLC, 773 F. Supp. 2d 593, 600 (D. Md. 2011) ("Maryland law governs interpretation of the contracts at issue in this case. The Uniform Computer Information Transactions Act ("UCITA") has been enacted by the Maryland legislature and both contracts are covered by its terms." (citations omitted)); KeyBank, Nat'l Ass'n v. Quality Payroll Sys., Inc., No. CV 06-3013(JS)(AKT), 2006 WL 1720461, at *4 (E.D.N.Y. June 22, 2006) ("[T]he Service Agreement for Electronic Fund Transfers dated July 11, 1998, and the Key Exchange Services Amendment Agreement dated December 10, 2004 (collectively the 'Agreements') clearly define the rights and duties of the parties.").

205. *See Keybank*, 2006 WL 1720461, at *4.

206. *See* UNIF. COMPUTER INFO. TRANSACTIONS ACT § 107(a).

207. *See* Zittrain, *supra* note 24, at 100-03.

208. *See* eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000) ("eBay argues that BE's use was unauthorized and intentional. eBay is correct. BE does not dispute that it employed an automated computer program to connect with and search eBay's electronic database. . . . BE argues that it cannot trespass eBay's web site because the site is publicly accessible. BE's argument is unconvincing.").

corporate contracts as the sole expression of contractual preferences within an e-commercial case.[209] A consumer's preferences are rarely so cleanly stated. They might consist of statements made during the purchasing process, or even tacit understandings of the parties.

While in each individual case it may be simpler to enforce the corporate terms, the aggregate effect of this practice is to shift large transaction costs onto consumers. While a judge must read only one contract in a case, the result of the corporate-contract-focused interpretive approach is that privacy-minded consumers must read thousands of different online contracts drafted in extremely technical language.[210] And if, as this Article suggests, there is a way to create compact, streamlined consumer-offered contract terms—such as a "do-not-track" flag set in a browser—the court's judicial economy preference for corporate-drafted contracts should give way to a more even-handed approach.

Some contracts that the law calls "standardized" are in fact obfuscatory.[211] Other "standardized" contracts are truly standardized—that is, they convey more information to the user by virtue of the fact that they offer the standard deal.[212] For this latter kind of standardized contract, the consumer need not read the contract in every case, since she knows she is getting the standard deal. True standardization helps convey information.[213] What courts dislike are not true standard contracts, but precisely those contracts that are *not* standardized—that is, that contain some term or condition that would unfairly surprise the consumer.[214]

However, even courts that understand that standardized contracts can reduce information costs[215] have, not without irony,

---

209. *See* Barnes, *supra* note 114, at 245-46 ("Under the duty-to-read rule, if a consumer signs a form contract, the law has traditionally stated that it is reasonable for the merchant to conclude that the consumer has thereby given her assent to the deal.").

210. *See* Hartzog, *supra* note 3, at 1642 ("It has become a truism that virtually no one reads standard-form online agreements."); Nehf, *supra* note 144 ("[D]espite the proliferation of privacy policies online, consumers' privacy interests may in fact be no better protected today than they were ten years ago.").

211. *See* Joshua A.T. Fairfield, *The Search Interest in Contract*, 92 IOWA L. REV. 1237, 1273 (2007).

212. *Id.* at 1244.

213. *Cf.* Eric J. Feigin, Note, *Architecture of Consent: Internet Protocols and Their Legal Implications*, 56 STAN. L. REV. 901, 902 (2004) ("Higher-level protocols, such as those utilized in most web interactions, involve exchanges that should be considered express consent: the formation of a legally binding contract.").

214. *See* Joshua Fairfield, *The Cost of Consent: Optimal Standardization in the Law of Contract*, 58 EMORY L.J. 1401, 1450 (2009).

215. *See* Hill v. Gateway 2000, Inc., 105 F.3d 1147, 1149 (7th Cir. 1997) ("Writing provides benefits for both sides of commercial transactions. Customers as a group are better off

refused to take the last step of enforcing consumer-side standard terms. Automated contracts have been around for years,[216] and while courts continue wrestling with the problems raised by the mid-nineties automation of corporate-side contracting over the Internet, commerce has already moved on to new frontiers.[217] As noted above, one of the inalterable features of this new commercial landscape is that computers automatically offer and accept contracts.[218] Automated contracting is the backbone of modern commercial systems, from machine parts to groceries to vast swaths of financial markets.

Transaction costs would be at their lowest if both consumers and corporations could offer standard contracts automatically, whether through the consumer's web browser or the corporation's web server. Corporations benefit from legal enforcement of their web-server-proffered contracts. When a consumer purchases an item from Amazon.com, she does not interact with a live person. The machine is the agent or instrumentality of the corporate contractual counterparty.[219] In exactly the same fashion, consumers should benefit from legal enforcement of their web-browser-proffered contracts. It is neither complex nor costly for corporations to refuse to do business with customers who offer contractual terms the corporation does not wish to accept. Of course, what will likely happen is the opposite: the corporation will choose to do business with the consumer,[220] and in so doing, a court should deem that the

---

when vendors skip costly and ineffectual steps such as telephonic recitation, and use instead a simple approve-or-return device.").

216. *Cf.* Amelia H. Boss, *Electronic Data Interchange Agreements: Private Contracting Toward a Global Environment*, 13 NW. J. INT'L L. & BUS. 31, 31 (1992) ("With the growth in the use of electronic communications technologies to communicate important business and trade information, the size of the earth . . . is rapidly shrinking.").

217. *Id.* at 31-32 ("[T]he drafting . . . of several international codifications . . . . though progressive, ha[s] failed to keep pace with the quickly changing face of international business transactions.").

218. *Id.* at 33 ("Companies are increasingly resorting to electronic communications technologies like electronic data interchange (EDI) because of the increased speed of transmission, reduction in error in commercial exchanges of data, reduced need for paper documents, elimination of repetitive computer input, reduced inventory needs, faster response to business demand, reduced time to market products, and significant overall cost reductions.").

219. Of course, the programmer who set the machine up, or her superiors who told her what to code, are the real legal counterparties, but that does not matter for this analysis.

220. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 275-78 (2011) (discussing the rise in privacy concerns by consumers and the media, and the change in policies by corporations to address this demand); Doug Gross, *Apple: Apps Need 'Explicit Approval' Before Collecting User Contacts*, CNN, http://www.cnn.com/2012/02/15/tech/mobile/apple-user-contacts/index.html (last updated Feb. 22, 2012) ("Apple on Wednesday said it will start requiring mobile apps to get explicit permission from iPhone and iPad owners before the apps collect and store information about users' personal

corporation accepted the consumer's terms. The next Section explores the potential of deeming automated consumer-side terms enforceable.

B. A Better Direction: Consumer Online Contracts

Courts should apply the same rules to enforce consumer-offered online contract terms as they do to enforce corporate-offered terms. Consumer privacy preferences would, under this approach, be expressed as standardized, simple, machine-readable settings set in the web browser client. This solution is at least as good as, and likely far better than, the practice of corporations offering lengthy and obfuscatory contracts via their web servers. An enforceable do-not-track flag is a perfect place to start. It is an absolutely clear expression of the consumer's unwillingness to sell her private information, offered at the first and every subsequent point of contact between consumer and corporation. While comprehension costs to consumers of reading and keeping up with thousands of corporate contracts are very high, comprehension costs to corporations of complying with a simple and binary machine-readable flag are absolutely zero. Corporations can set their web servers to respond to the flag and respect the consumer's preference, or choose not do business with her, as the corporation chooses.

The proposal advanced here is not a vision of individuated, dickered, or particularized consumer contracting, but rather a vision of standardized, mass-market, consumer-proffered contract terms. This is an approach with a successful track record. For example, in the intellectual property context, consumers can use Creative Commons copyright licenses (CC licenses) for content that they create and upload to online sites.[221] CC licenses give content creators control of their work in the form of short, clear, and standardized license terms.[222] The result is a copyright system that is characterized by simplicity, low transaction costs, and equalization in legal power for

---

contacts. . . . The statement came after a week of revelations that popular social tools like Twitter and Path were doing just that . . . .").

221. *See About the Licenses*, CREATIVE COMMONS, http://creativecommons.org/licenses (last visited Aug. 15, 2011) [hereinafter CREATIVE COMMONS] (providing for a standard option set of contractual licenses that have revolutionized online exchanges). For example, an aspiring web developer may pick a Creative Commons (CC) license that allows others, including corporations, to use their work but only for non-commercial use and with attribution, or freely with only attribution required.

222. *See* Severine Dusollier, *Contract Options for Individual Artists: Master's Tools v. The Master's House: Creative Commons v. Copyright*, 29 COLUM. J.L. & ARTS 271, 272 (2006) (discussing the purpose of Creative Commons to address the over expansion of copyright and need to protect both future creators and users of copyrighted works).

consumers with corporations through simple contracts[223] that courts will enforce.[224] And to the extent that a consumer-proffered contract contains a non-standard or non-machine-readable surprise, courts can strike unconscionable terms from the contract on the same grounds and to the same extent that they do (or equally often do not) for unfairly surprising terms in corporate contracts. But in this case, there can be no surprise in a single check box indicating that a consumer does not wish to be tracked.

Indeed, there is every reason to believe that the contract terms that consumers offer will be simple and standardized. Consumers often merely expect the standard deal, which involves price, quantity, and standard quality. Consumers do not need or want most of the fine legal technicalities that corporations do; they desire only essential terms.

Underneath the basic inclination of consumers to add a breath of needed simplicity to legal transactions lies a deeper point. Consumer-side contracts can be crafted to be not only simple but also modular and standardized. A good model here again is the CC licenses.[225] CC users select pre-drafted standardized licenses that govern the use of their content through a simple menu of options.[226] The licenses respond to user desires and do not add needless boilerplate. Finally, the licenses are undoubtedly enforceable consumer contracts offered by and responsive to the needs of the individual rather than the corporation.[227]

Other scholars have proposed to use CC licensing as a broader solution to the problem of consumer data privacy.[228] This Article does not propose so broad an initiative here. Rather, it notes that browsers currently permit a user to express her preference to not be tracked.[229] This option is simple, binary, and machine-readable. There is no reason, other than willful ignorance, for a company to track a user who has made use of such a browser option. Certainly, the argument that consumer-proffered contracts will complicate online contracting

223. *See* Patricia Sánchez Abril, *Private Ordering: A Contractual Approach to Online Interpersonal Privacy*, 45 WAKE FOREST L. REV. 689, 720-21, n.224 (2010) ("The Creative Commons . . . licenses are legally enforceable in both contract and property.").

224. *Id.* at n.224.

225. *See* CREATIVE COMMONS, *supra* note 221.

226. *See id.*

227. *See* Dusollier, *supra* note 222 at 272.

228. *See* Patricia Sánchez Abril, *supra* note 223, at 720-23 (2010).

229. *See* Wingfield & Angwin, *supra* note 153; *see also* Ryan Singel, *Google Holds Out Against 'Do Not Track,'* CNN (Apr. 18, 2011), http://www.cnn.com/2011/TECH/web/04/18/google.chrome.wired/index.html; *Mozilla: Do Not Track*, *supra* note 153 (noting that Mozilla Firefox includes a Do-Not-Track option).

fails in the face of such a simple and standard expression of preference.

III. THE DO-NOT-TRACK OPTION

A. The FTC's Proposal

The Federal Trade Commission (FTC), sensing the inadequacies of the current legal framework, has voiced some support for a federally enforced do-not-track option.[230] The FTC has already had broad success with an analogous program: the Federal Do-Not-Call Registry.[231] This list helped to curb direct-call harassment by call centers because it permitted consumers to make a simple, one-time, enforceable election to not be contacted.[232]

Companies reliant on unchecked use of consumer information have broadly opposed the FTC's proposal of a do-not-track enforcement regime,[233] just as telemarketers resisted the Do-Not-Call list. [234] Whether these lobbying efforts will succeed remains an open question. It is certainly true that a FTC-mandated do-not-track option should not be run in the same fashion as the Do-Not-Call list.

The Federal Do-Not-Call list requires users to register their telephone numbers with the government.[235] The government then maintains this central registry and telemarketers must scrub their contact lists by comparison to the central database on a regular

---

230. *See* Edward Wyatt & Tanzina Vega, *F.T.C. Backs Plan to Honor Privacy of Online Users*, N.Y. TIMES, Dec. 1, 2010, http://www.nytimes.com/2010/12/02/business/media/02privacy.html.

231. *See* Nils Kongshaug, *Do-Not-Call List a Success . . . Even for Telemarketers*, ABC NEWS (Aug. 14, 2005), http://abcnews.go.com/WNT/Business/story?id=1037365.

232. *See Reporter Resources: The National Do Not Call Registry*, FED. TRADE COMMISSION, http://www.ftc.gov/opa/reporter/dnc.shtm (last visited October 2, 2011) [hereinafter *National DNC Registry*] (describing the role and certain limitations of the Do Not Call Registry).

233. *See* David Goldman, *FTC 'Do Not Track' Plan Would Cripple Some Web Giants*, CNNMONEY (Dec. 3, 2010, 10:03 AM), http://money.cnn.com/2010/12/02/technology/ftc_do_not_track/index.htm (identifying numerous industry leaders, for example Google, who are opposed to "do not track" because of unforeseen security problems and loss of advertising revenues). *But see* Casey Newton, *Google Agrees to Do-Not-Track Button*, S.F. CHRON., Feb. 24, 2012, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2012/02/23/BULK1NBLSQ.DTL&type=tech ("Google . . . became the latest Internet giant to support adding a do-not-track button to its web browser. No time frame was set for changing the Chrome browser to include a do-not-track feature . . . ."); Jennifer Valentino-Devries & Emily Steel, *White House to Push Privacy Bill*, WALL ST. J., Mar. 15, 2011, http://online.wsj.com/article/SB10001424052748704662604576202971768984598.html ("[A] group of about 30 online-advertising companies is preparing to break with most of the industry and support a proposal for a single do-not-track tool.").

234. *See Do-Not-Call Back on the Line*, CBS NEWS (Feb. 11, 2009, 8:36 PM), http://www.cbsnews.com/stories/2003/07/07/tech/main561876.shtml (describing industry efforts to stop the Do Not Call list).

235. *See National DNC Registry*, *supra* note 232.

basis.[236] A do-not-track option could not work in the same way, nor should it. The "telephone number" at issue could be one of two options, both of which present difficulties. The identifying number could be a special government-issued cookie that identified the user[237] or it could be the user's IP address.[238] The IP address option will not work, since most ISPs assign IP addresses on a dynamic basis, changing any given user's IP address regularly. And those ISPs that allocate static IP addresses, such as Sprint,[239] create enormous tracking problems for consumers.[240] The government cookie option raises even more concern, because in order to not be tracked by corporations, the user must reveal herself in a permanent fashion to the government.[241] One option is unworkable, the other unacceptable.

B. A Better Alternative: Do-Not-Track Browser-Level Options

The simple expedient of enforcing a browser-level do-not-track option would solve the above-mentioned problems. A do-not-track option in the browser does not rely on an IP address, since the user can express her preference not to be tracked no matter what Internet address she is using.[242] And it does not raise issues of government intrusion into privacy, since the government would not have to maintain a central database of special tracking cookies ostensibly used to tell corporations not to track consumers.[243]

---

236. *Id.*

237. *See Tracking the Trackers: Our Method*, WALL ST. J., July 31, 2010, http://online.wsj.com/article/SB10001424052748703977004575393121635952084.html ("HTML cookies are small text files, installed on a user's computer by a website, that assign the user's computer a unique identity and can track the user's movements on a site.").

238. *See* Keith Black, Note, *Technical Knockout: How Mixed Martial Arts Will Change Copyright Enforcement on the Web*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 739, 755 n.106 (2011) ("An IP address is a unique user-identification number that is automatically assigned to the user.").

239. *See supra* text accompanying note 109.

240. *See* Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6, 50 n.80 (2003) ("A dynamic IP address is analogous to a 'temporary phone number[,] for the duration of that Internet session or for some other specified amount of time. Once the user disconnects from the Internet, their [sic] dynamic IP address goes back into the IP address pool so it can be assigned to another user.'" (alterations in original)).

241. *See generally* GEORGE ORWELL, 1984 (Signet Classic 1977) (1949) (describing a fictional era in which the government watches and regulates one's every action).

242. *See, e.g.*, *Mozilla: Do Not Track*, *supra* note 153 (instructing users how to enable Do Not Track).

243. This is because the user and the website would handle the do-not-track option: the government would have no direct role. *Compare id.* (discussing how a user can enable Do Not Track in her browser), *with National DNC Registry*, *supra* note 232 (illustrating how the FTC operates its do-not-call registry by compiling and maintaining registered telephone numbers and reporting the numbers to telemarketing companies).

A simple and successful approach would be for the FTC to use its section 5 authority to stop unfair business practices.[244] This would require businesses to respect a consumer's expressed preference not to be tracked.[245] As is too often the case in politics, however, what should be done may not be done. And even if the FTC were to adopt do-not-track as an enforceable rule, the FTC has few resources available for direct enforcement.[246] An individual's ability to stop corporate surveillance therefore may depend on the availability of other enforceable rights, such as those proposed here.

Furthermore, the FTC's section 5 authority is restricted to unfair business practices.[247] Courts have read this authority quite broadly.[248] Nevertheless, corporations will certainly assert that following the terms of their own privacy policies and terms of use does not constitute an unfair business practice.[249] From the corporation's perspective, the consumer has agreed to unlimited intrusion and untrammeled surveillance merely by using an online site or service. Changing the law's default preference for corporate contracts is important[250] because the FTC has traditionally been much more willing to step in on behalf of consumers when a company violates

---

244. *See* Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (2006) (granting the FTC the power to regulate unfair trade practices); *see also A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMMISSION, http://www.ftc.gov/ogc/brfovrvw.shtm (last updated July 2008) [hereinafter *FTC: A Brief Overview*] (describing the FTC's authority under section 5 of the FTCA).

245. *FTC: A Brief Overview*, *supra* note 244.

246. *See id.* ("[E]ven where the Commission determines through adjudication or rulemaking that a practice is unfair or deceptive, the Commission must still seek the aid of a court to obtain civil penalties or consumer redress for violations of its orders to cease and desist or trade regulation rules."); *see also* Bamberger & Mulligan, *supra* note 220.

247. *See* 15 U.S.C. § 45(a)(1) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.").

248. *See* FTC v. Cinderella Career & Finishing Sch., Inc., 404 F.2d 1308, 1311 (D.C. Cir. 1968) ("Congress, in 1914, enacted the Federal Trade Commission Act. The then broad purpose of the Act was to prevent unfair methods of competition in their inception. By the Wheeler-Lea amendment, Congress, in 1938, broadened section 5 of the Act and extended the authority of the Commission to eliminate unfair or deceptive acts or practices in commerce without regard to competition." (footnotes omitted) (citation omitted)).

249. *See* Claridge v. RockYou, Inc., 785 F. Supp. 2d 855, 862-865 (N.D. Cal. 2011) ("Unfair acts are those that 'offend[] an established public policy' or are 'immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers.' . . . [D]efendant . . . argued . . . plaintiff's contractual claims should be dismissed because the provisions of the privacy policy maintained by defendant expressly provide that no liability will result due to a third party's unauthorized access of defendant's computer system . . . ." (alteration in original)); *see also* Adam R. Bialek & Scott M. Smedresman, *Internet Risk Management: A Guide to Limiting Risk Through Web Site Terms and Proactive Enforcement*, 20 INTELL. PROP. & TECH. L.J. 1 (2008) (describing how privacy policies and terms of use statements can limit risks to companies that operate websites).

250. *See* Kesan & Shah, *supra* note 45.

contractual promises with consumers.[251] Since corporations rarely make enforceable promises regarding consumer privacy, FTC involvement in consumer privacy has been anemic.[252]

There is, however, a potential upside to this dynamic. If courts enforce consumer-offered automated standardized contract terms, then companies will indeed be violating the promises they have made to consumers if they violate a do-not-track term. If corporations violate an actual contractual promise regarding privacy, the FTC will have more opportunity to become legally involved. What was once a rarity may become commonplace; the FTC will actually protect consumers from corporate overreach.[253]

Indeed, the FTC does step in where corporate transactions violate actual contractual promises made to consumers regarding privacy. In *F.T.C. v. Toysmart.com, LLC*, the FTC stepped in to prevent the sale of consumer information as part of a bankruptcy proceeding, where the debtor entity had promised its consumers not to sell or share customer information.[254] *Toysmart.com* was, typical of modern pro-consumer contract cases, a mere flash in the pan. The industry standard clauses regarding resale of consumer information were promptly rewritten to permit *ad infinitum* resale of consumer information.[255] But again, it is worth noting that enforcing consumer-proffered contract terms will help to correct for the one-way ratchet that current online contracting trends have established. It is quite possible, therefore, that if courts permit robust consumer-proffered contracting, then the FTC will see violations of those contract terms as grounds to intervene under its section 5 authority to sanction unfair business practices.

---

251. *See e.g.*, FTC v. Toysmart.com, LLC, No. Civ.A. 00-CV11341RGS, 2000 WL 1523287 (D. Mass. Aug. 21, 2000) (alleging that Toysmart violated the terms of its privacy policy with consumers about disclosure of personal information and therefore engaged in deceptive acts or practices in violation of section 5 of the Federal Trade Commission Act); *see also* In re Gateway Learning Corp., 138 F.T.C. 443 (2004).

252. *See* Bamberger & Mulligan, *supra* note 220, at 302 ("[T]his turn to objective manifestations of privacy embodied in social norms has been used by the FTC to protect privacy where technological changes render traditional reliance on consent inoperative, or at least incomplete."). The article continues by discussing the problem of the FTC's roving enforcement and inconsistency on privacy concerns for consumers and how this has been significant. *Id.*

253. *Id.* at 314-15 ("Finally, as the privacy community reflects upon the key global instruments of data protection, our account underscores the importance of empirical inquiry and thick institutional engagement in considering contested issues of regulatory strategy, technological complexity, social and institutional networks, and the protection of individual and communal interests in the private sphere. If privacy is to be protected in an increasingly connected world, debates over its formal regulation must increasingly be informed by the ways that today's frameworks operate on the ground.").

254. *See id.*

255. *See* Richard A. Beckmann, Comment, *Privacy Policies And Empty Promises: Closing The "Toysmart Loophole,"* 62 U. PITT. L. REV. 765, 788 n.159-60.

Establishing a do-not-track option as a consumer-side contractual term that corporations must respect would, at a minimum, accomplish two things. First, it would return control over contractual relations to consumers.[256] Second, it would establish that companies are systematically breaking their contractual promises to consumers when they track those consumers despite an expressed preference against tracking. Such a systematic breach of relations between corporation and consumer would lay a more solid groundwork for FTC intervention. [257]

C. On Geese and Gander: Why Favor Corporate Interests?

This Section will argue that corporations and consumers should have equal power to offer enforceable contract terms. It will then provide several examples of other areas in the law where this kind of equalization has been successful. The most successful movements in Web 2.0[258] have turned the tables on corporations by relying on courts' basic intuitions of fairness.[259] The developed and powerful law of intellectual property that corporations built over the past two decades was put at consumers' fingertips through the CC licenses.[260] This Article promotes a similar proposal for data protection: that the developed law of online contracting, which until

256. *See* Hartzog, *supra* note 3, at 1638 ("Code-based negotiations for confidentiality can form implied-in-fact contracts or give rise to a claim for promissory estoppel.").

257. *See FTC: A Brief Overview*, *supra* note 244 (describing the FTC's authority to regulate unfair and deceptive trade practices). For an example of the FTC's willingness to intervene in consumer privacy cases where there is a violation of the contractual promises between corporation and consumer, see Press Release, FTC, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network: Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data (Mar. 30, 2011), *available at* http://www.ftc.gov/opa/2011/03/google.shtm ("The FTC complaint charges that Google violated its privacy policies . . . .").

258. *See* Matthew J. Wilson, *E-Elections: Time for Japan to Embrace Online Campaigning*, 2011 STAN. TECH. L. REV. 4, 1 ("Internet users spend significant time using 'Web 2.0' technologies and other World Wide Web tools (collectively 'Internet tools') that enable interactive information sharing, user-centered design, collaboration, and a compilation of collective intelligence.").

259. *E.g.*, Major v. McCallister, 302 S.W.3d 227, 232 (Mo. Ct. App. 2009) (Rahmeyer, J., concurring) ("[T]he same contract principles hold on the Internet. When the consumer is presented with a contract of adhesion containing lengthy provisions and hidden terms, I believe courts should consider whether the process of assent or terms of the contract are unconscionable.").

260. *See About*, CREATIVE COMMONS, http://creativecommons.org/about (last visited Oct. 8, 2011) ("[The creative commons system] give[s] everyone from individual creators to large companies and institutions a simple, standardized way to keep their copyright while allowing certain uses of their work—a 'some rights reserved' approach to copyright—which makes their creative, educational, and scientific content instantly more compatible with the full potential of the [I]nternet.").

now has served only corporate interests, be put to use by protecting consumers.[261]

The project falls apart, however, if courts are not willing to grant the same contract power to consumers that they do to corporations. They could refuse to do so through a range of options, as noted above.[262] For example, courts could deny the existence of the consumer-proffered terms, as in *Hill v. Gateway 2000, Inc*.[263] Under *Hill* and its progeny, courts acted as though consumers' preferences simply did not exist, or had no validity because they were not contained within the corporate document.[264]

Indeed, of all of the challenges to the current proposal, this is the most dangerous. When courts simply will not consider consumer preferences to be part of "the" contract between the parties because they are not expressed within the four corners of the corporate contract, these courts destroy any hope of consumers protecting their personal privacy.[265] This is an even more untoward extension of the preferences courts have already extended to corporations in the online contracting arena. Under modern contract case law, consumers may not offer contract terms or expect courts to enforce those terms. Furthermore, courts do not even consider consumer preferences unless they appear in the corporate contract.[266] Imagine the counterfactual: courts would ignore corporate contractual preferences unless they appeared in the consumer's data-use terms. If what were good for the consumer goose were good for the corporate gander, all corporate online contracts would have no effect, just as consumer terms are now ignored.

If courts are legally rigorous and have not lost their sense of fair play, then they will recognize consumer contractual terms and should reach some form of accommodation. That might mean cancelling the entire contract based on a lack of meeting of the minds.[267] More likely, it may be some form of "last shot" analysis that may continue to favor corporations as long as courts continue to treat

---

261. *See* LESSIG, *supra* note 30, at 228-30 (arguing for a contractual model to protect privacy).

262. *See supra* Part III.A-B.

263. Hill v. Gateway 2000, Inc., 105 F.3d 1147, 1149-50 (7th Cir. 1997) (explaining how there is no battle-of-the-forms situation when consumers purchase items with contracts attached, and that such contracts are binding on both sellers and purchasers).

264. *See id.* at 1148 ("Terms inside Gateway's box stand or fall together. If they constitute the parties' contract because the Hills had an opportunity to return the computer after reading them, then all must be enforced.").

265. *See* Knapp, *supra* note 6, at 102-04; *see also* Hartzog, *supra* note 3, at 1635-36.

266. *See, e.g.*, *Gateway*, 105 F.3d at 1149-50.

267. *See* RESTATEMENT (SECOND) OF CONTRACTS § 20 (1981) (citing cases in which an absence of a meeting of the minds led to unenforceability of a contract).

keeping the product as signifying assent—the last action. However, a "last shot" analysis can also favor the consumer by, for example, treating the corporation's acceptance of payment or failure to recall the product as actions that accept the consumer's terms.[268]

Ideally, courts should give effect to each party's preferences as expressed in automated machine-offered terms that are readable by the counterparty, insofar as they are not considered absolutely contrary to each other. And when they directly contradict—that is, when the corporation wishes to track an individual who has expressed the clear and simple wish not to be tracked—then the court should find that the parties have not reached a deal. No deal means no tracking, on pain of violation of hacking laws, or liability for cyber trespass, or other background default laws and rules.

The final vision here is one of computer-mediated automated contracting between consumer and corporation. Consumers would offer to sell their information based on standardized terms, represented by check boxes in their browsers. ISPs and online service providers would code their preferences for information purchases into their web servers. Computers would perform a match. If the match is exact, the contract contains the terms, both consumer check box and corporate-drafted, that both parties have agreed to. If the terms are such that the parties do not substantially agree, and they do not do business with each other (because the corporate server refuses the consumer's connection) then there is still no tracking problem. If the corporation accepts the consumer's connection with full understanding of the consumer's expressed privacy preference, then the corporation must respect that preference under two theories—either the corporation would be deemed to have accepted the consumer's preferences by accepting the communication, or the differences between the two would be so irreconcilable that any court would find there was effectively no contract. This would, of course, lead to a no-tracking result, since a result of no deal means the corporation did not secure the consumer's consent to tracking.

268. *Cf.* Diamond Fruit Growers, Inc. v. Krack Corp., 794 F.2d 1440, 1444 (9th Cir. 1986) (discussing how § 2-207 of the UCC was created in part to do away with the common law's "last shot" rule of contract formation). According to the "last shot" rule, "the offeree/counterofferor gets all of its terms simply because it fired the last shot in the exchange of forms." *Id.*

D. Is there a Remedy?

After *AT&T Mobility LLC v. Concepcion*,[269] there is one remaining caveat to the implementation of consumer do-not-track preferences as contract terms. Assuming the consumer prevails, what would the remedy be? Class actions in consumer mass-market contracting have decreased after *Concepcion*,[270] and privacy class actions have fared particularly poorly in the courts.[271] How does a theory of do-not-track as contract alter this dynamic?

Without offering a deep discourse on the availability of remedies in consumer e-commercial contracts, especially since courts render most remedies moribund by enforcing corporate-drafted limitations of remedies clauses, this Article offers some limited suggestions. First, the consumer often wants the ISP to take some action, such as taking down defamatory or embarrassing content, or in the case of a privacy-conscious consumer, requiring the corporation to delete the data.[272]

Specific performance—requiring a company to delete a consumer's data that it has extra-contractually gathered—seems a simple, straightforward, and reasonable remedy. Remedies at law (damages) do not solve the plaintiff's problem of data remaining outside her control. Thus, under the standard test for specific performance, damages are inadequate, and specific performance is not a particularly difficult remedy to obtain.[273] The UCC encourages liberal use of specific performance.[274] And outside of the UCC, the inadequacy of legal damages should lead courts to order Internet or

---

269. AT&T Mobility LLC v. Concepcion, 131 S. Ct. 1740, 1753 (2011) (upholding the Federal Arbitration Act against a judicial rule that would require class arbitration despite contractual waivers).

270. *See id.* at 1746 (holding that California's *Discover Bank* rule—which holds that class waivers are unconscionable when found in a contract of adhesion—is an obstacle to Congressional objectives in the FAA and therefore preempted); *see also* Jones, *supra* note 202 (noting how the *Concepcion* decision may threaten the viability of class-action suits in the future).

271. *See* Ian C. Ballon & Wendy Mantell, *Cloud Litigation: Suing Over Data Privacy and Behavioral Advertising*, CENTURY CITY LAW., Sept. 2011, *available at* http://centurycitybar.com/newslettertemplate/Sept11/article2.htm ("Courts have dismissed putative privacy class action suits where consent was inferred from a TOU agreement or a Privacy Policy.").

272. *See, e.g.*, Class Action Complaint at 28-29, White v. Clearspring Techs., Inc., No. 2:2010-cv-05948 (C.D. Cal. Dec. 6, 2010), ECF No. 27 (demanding, in part, relief in the form of deleting consumer data collected in the forms complained of).

273. *See* Steve Thel & Peter Siegelman, *You Do Have to Keep Your Promises: A Disgorgement Theory of Contract Remedies*, 52 WM. & MARY L. REV. 1181, 1205 (2011) ("It is commonly said that specific performance is available only when damages are 'inadequate.'").

274. *See* U.C.C. § 2-716 (2003) ("Specific performance may be decreed if the goods are unique or in other proper circumstances.").

online service providers that breach consumer's contractual conditions, to delete the data.

As noted above, consumer-offered contract terms may also have some impact on a particular method for legal adjudication of small harms—the class action. After *Concepcion*, it appears that Internet class actions face significant additional legal hurdles from the prevalence and enforcement of arbitration clauses that preclude class treatment.[275] But, for *Concepcion* to apply, the arbitration clause in the corporate contract must be the operative legal clause.[276] Courts will enforce corporate rights and remedies limitations only if they ignore consumer contractual language retaining all legal rights and remedies—specifically including the right to a court trial. If courts permit a consumer contracting approach, the consumer may include a no-arbitration clause alongside her do-not-track option. Once courts permit consumers to draft contracts rather than merely sign them, these consumers can better defend their legal rights.

E. Corporate Objections to the Do-Not-Track Proposal

Consumer machine-mediated contracting is as valid and enforceable as corporate machine-mediated contracting. Despite the simplicity and limited scope of the do-not-track proposal, it will certainly draw significant corporate objections. This Section seeks to anticipate and answer some of the likely objections.

First, corporations will claim that they lack notice of consumer-proffered contract terms. But courts have already rejected the argument that consumers lacked notice of the contents of corporate machine-mediated contracts.[277] If consumers have notice of corporate terms buried in prolix EULAs, corporations certainly would have notice of simple, machine-readable flags set in a consumer's browser.

---

275. *See* Jones, *supra* note 202 (noting that the *Concepcion* result threatens class action suits).

276. *See* AT&T Mobility LLC v. Concepcion, 131 S. Ct. 1740, 1742-43 (2011) ("Section 2's saving clause permits agreements to be invalidated by 'generally applicable contract defenses,' but not by defenses that apply only to arbitration or derive their meaning from the fact that an agreement to arbitrate is at issue.").

277. *See, e.g.*, Swift v. Zynga Game Network, Inc., No. C-09-5443 EDL, 2011 WL 3419499, at *7 (N.D. Cal. Aug. 4, 2011) ("Plaintiff's argument that she was not provided with sufficient notice of the contractual terms she was assenting to because of Zynga's modified clickwrap presentation, and therefore is not bound by any arbitration provision, fails in light of recent caselaw holding that clickwrap presentations providing a user with access to the terms of service and requiring a user to affirmatively accept the terms, even if the terms are not presented on the same page as the acceptance button, are sufficient.").

Corporations might also claim that they did not have any power to object to consumer-proffered contracts. Again, courts rejected the argument that consumers had no choice but to accede to the terms of corporate machine-mediated contracts.[278] Unless courts are willing to embrace a jurisprudence of pure corporate preference, corporations should be held to the same standards when they agree to consumer terms as consumers are when they agree to corporate terms. Only procedural unfairness leading to a substantively unconscionable result would permit the corporation to escape from its promises.[279] And it is quite hard—almost laughable—to imagine a corporation legitimately arguing that a consumer had so much market power that it forced the corporation to agree to substantively unfair terms. Moreover, the term at issue here—consumer privacy as expressed in a do-not-track flag—is not substantively unfair.

The strongest objection is that courts should enforce the corporation's version of the contract rather than the consumer's version. Some variation of the four corners or parol evidence doctrine may convince courts to continue ignoring consumers' contractual preferences.[280] But if courts follow black-letter contract law, the buyer is the master of the offer and the seller may agree to the buyer's terms or refuse the transaction.[281] Courts should not manipulate the moment of offer and counteroffer until the corporation's terms mysteriously come out as the enforced terms.[282]

A do-not-track option should be a core part of any data transaction. It is expressed up front in machine-readable format. The corporation knows what the deal is in crystal clear terms. So, as noted above, if the corporation does not wish to do business with customers who do not want to be tracked, it is free to refuse the connection at that first point of contact. Nothing could be simpler. When courts

278. *Id.*

279. *See* Rent-A-Ctr., W., Inc. v. Jackson, 130 S. Ct. 2772, 2780 (2010) ("As required to make out a claim of unconscionability under Nevada law, he contended that the Agreement was both procedurally and substantively unconscionable." (citation omitted)); Harrington v. Atl. Sounding Co., 602 F.3d 113, 118 (2d Cir. 2010), *cert. denied*, 131 S. Ct. 1054 (2011) ("The district court found that the facts of this case satisfied New Jersey's 'sliding scale' approach to unconscionability, under which 'a claim of unconscionability can succeed when one form of it, either procedural or substantive, is greatly exceeded, while the other form is only marginally exceeded.'").

280. *See, e.g.*, CAL. CIV. PROC. § 1856 (West 2011) (describing California's parol evidence rule).

281. *See* U.C.C. § 2-206(1) (2003); *see also* discussion *supra* note 185.

282. *See* DeFontes v. Dell, Inc., 984 A.2d 1061, 1069-71 (R.I. 2009); *see also* Budnitz, *supra* note 156.

attempt to complicate matters, it looks suspiciously like naked corporate preference.[283]

Another possible objection is that automated consumer contractual preferences more complicated than do-not-track will place an impermissible burden on corporations to read the contracts that they enter into with their consumers.[284] This burden did not particularly bother corporations when customers had to track hundreds of privacy policies from many different institutions.

But herein lies the larger point: to reduce information costs, both buyers and sellers online should be able to offer standard and automated contract terms with the full expectation that a court would enforce their terms. By way of contrast, the current system permits corporations to contract by computer and requires consumers to contract by hand. The current system permits corporations to "read" contracts by machine, but requires consumers to read contracts in person. The imbalance in transaction costs is colossal. Currently consumers must read thousands of different agreements to even begin protecting their privacy online. None do, and it is no wonder; the law has predetermined their failure. Information costs would be far lower if a consumer could express her preferences once and expect that corporations would respect those preferences. Information costs would be lower for corporations too, who would merely have to check the consumer's browser handshake protocol to see if the consumer had expressed a preference not to be tracked.

Corporate advocates are wrong when they claim that consumer-offered contract terms would raise information costs for corporations. The entire system at the moment revolves around consumers shouldering massive information costs. Corporations do not want to identify or respect their customers' privacy preferences; they instead intend to continue taking, aggregating, and reselling private consumer information. Corporations continue this behavior based on the theory that the consumer has "consented" to sale of her personal information, even though the corporation has been clearly and cleanly informed upon every instance of being contacted by the consumer that this consent is withheld.

This false consent model cannot be the future of online contracting. Among other things, consumers are becoming producers. This is the result of the Web 2.0 model combined with so-called

283. *See* Hillman & Rachlinski, *supra* note 66, at 440-41.

284. *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 76 ("The problems with P3P have now been widely reported. Technical experts have noted that the protocols are complex, difficult to implement, and unlikely to enable consumer to protect privacy. . . . Industry analysts have also found shortcomings in the P3P proposal." (footnote omitted)).

"prosumer" electronic equipment, which permits consumers to create professional grade products.[285] Consumers are already wearing two hats—consumer and professional. They are clearly able to draft, offer, and enforce contractual terms in their professional capacity. The current trend of denying consumers the right to offer contract terms in their consumer capacity simply cannot continue.

Another challenge to this Article's hypothesis is that some have already unsuccessfully attempted consumer-choice privacy models.[286] A discussion of prior efforts toward consumer privacy choice, notably the Platform for Privacy Preferences (P3P), can explain how the proposed solution is significantly different from those prior efforts.

The P3P, a consumer privacy system developed by the World Wide Web Consortium (W3C), attempted to simplify the interaction between websites and consumers by automating the consumer's "review" of a given site's privacy policy.[287] Websites could, if they wished, fill out a multiple-choice survey about their privacy policy, which was translated into a privacy policy that the consumer's web browser would read.[288] Provided they had P3P-enabled browsers, users then indicated their privacy preference, which was translated and compared with sites' privacy policies.[289] Despite being implemented in Internet Explorer 6 and Netscape 7,[290] P3P experienced very limited success even by those who worked vigorously to promote it.[291]

---

285. *See, e.g.*, Thomas K. Grose, *3D Comes To Web 2.0*, TIME, May 13, 2008, http://www.time.com/time/business/article/0,8599,1739765,00.html (French company Dassault Systèmes decided to put its high-quality modeling software into the hands of consumers . . . to 'democratize' its use . . . 3DVIA recently linked up with Facebook, where users can now make a 3D mashup.").

286. *Id.*

287. *See* Kim Rose Goldberg, Note, *Platform for Privacy Preferences ("P3P"): Finding Consumer Assent to Electronic Privacy Policies*, 14 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 255, 263 (2003) ("While the consumer merely selects his or her privacy settings, the P3P user-agent actually conducts the comparison between those settings and the P3P privacy policy.").

288. *Id.* at 260 ("Once the Web site provides its responses to the survey, those responses are then translated into a P3P privacy policy and placed on one of the Web site's servers where it is easily accessible by P3P user-agents.").

289. *Id.* at 261 ("When a consumer visits a P3P-enabled Web site, the second P3P component, called a P3P user-agent, accesses the P3P privacy policy, and compares the data-collection practices stated in that P3P privacy policy to the consumer's privacy settings.").

290. *See Platform for Privacy Preferences (P3P) Project*, W3C, http://www.w3.org/P3P/implementations.html (last updated May 28, 2007) (listing software implementing P3P).

291. *See generally* Ari Schwartz, *Looking Back at P3P: Lessons for the Future*, CENTER FOR DEMOCRACY & TECH. (Nov. 11, 2009), http://www.cdt.org/paper/looking-back-p3p-lessons-future.

One of the fatal flaws in P3P was its insufficiency as a stand-alone system for privacy protection.[292] The lack of mandatory enforcement—any legal backing for the preferences expressed in P3P—led to P3P's non-adoption and demise.[293] It is precisely for this reason that courts should enforce do-not-track as a contract term while the FTC works out whether or not it will formulate a rule.

P3P's complexity also contributed to its lack of adoption. P3P replicated the complexity of a corporate privacy policy on the consumer side. The consumer had to deal with a "dashboard" interface that presented multiple confusing options.[294] The infamously byzantine Facebook privacy controls are a modern example—controls clearly built to create serious transaction costs for privacy,[295] induce choice paralysis, and cause consumers to abandon their attempts to control private information. The complexity of approaches like P3P impacted corporations as well. As a result of complexity on the consumer side, there were too many options for webmasters, which ultimately made implementation less appealing.[296] An automated system for protecting privacy would need to address these issues of complexity and voluntary implementation.[297]

Do-not-track expresses a single, unitary, clear, machine-readable option that communicates at every instance of the user's contact with a corporation that she does not consent to her information being tracked. This is a distinction with a difference. The entire framework of online tracking is built on consent.[298] None of it makes sense if corporations ignore the clear and oft-repeated statement that a consumer does not give consent to tracking. Any effort to return control over private information to consumers must, in the first instance, take the form of an enforceable right to complete prohibition.

---

292. *See* William McGeveran, Note, *Programmed Privacy Promises: P3P and Web Privacy Law*, 76 N.Y.U. L. REV. 1812, 1854 (2001) (concluding that lawmakers should use P3P as the foundation of a privacy-protection regime, but that P3P itself is not enough to guarantee privacy).

293. *See* Schwartz, supra note 291.

294. *See* Rotenberg, *supra* note 284.

295. *See* Fowler, *supra* note 113 ("'Facebook's complex ecosystem—with thousands of independent apps and complex data flows to and from apps—is a problem of its own creation,' said Ben Edelman, an assistant professor at Harvard Business School.").

296. *See* Schwartz, *supra* note 291.

297. *Id.*

298. *See* Kende, *supra* note 101 ("The Internet is not a monolithic, uniform network; rather, it is a network of networks . . . . In order to provide end users with universal connectivity, Internet backbones must interconnect . . . agreements between Internet backbone providers are reached through commercial negotiations in a 'handshake' environment."); *see also* Feigin, *supra* note 213.

Industry advocates claim that consumers want more "nuanced" privacy settings.[299] This is quite wrong: consumers want simple, strong, and enforceable privacy settings.[300] The argument for "nuanced" consumer privacy settings is doublespeak for creating privacy settings complicated enough to induce choice paralysis, which is profitable to corporations. But even if one assumes that consumers want nuanced and complicated privacy settings, the analysis of this Article does not change. A nuanced privacy setting is not enforceable if a simple one is not. If consumers cannot say, simply, "I do not consent to any tracking in any form under any circumstances" and expect courts to enforce that statement, then we cannot begin to consider the enforcement or utility of more complicated statements of consumer preference.[301]

Courts must first enforce consumers' clearly, simply, and continuously communicated preferences of an absolute right to be let alone. Complex, nuanced statements of privacy preferences may only be considered once courts have established this basic right. This Author's sense is that consumers will never need that second step. Consumers will not seek these theoretically desirable nuanced or complicated privacy arrangements once courts enforce a simple, continuous, and clear expression not to be tracked, not least because consumers rightly distrust complicated privacy arrangements.[302] Corporations have so abused consumer trust in the information market that rejecting nuanced privacy arrangements seems both easily predictable and amply justified.

---

299. *See* Angwin & Fowler, *supra* note 113; *cf. Many Consumers Would Allow Online Tracking by Retailers and Service Providers if Discounts Applied, KPMG Survey Finds,* PR NEWSWIRE (Dec. 8, 2011), http://www.prnewswire.com/news-releases/many-consumers-would-allow-online-tracking-by-retailers-and-service-providers-if-discounts-applied-kpmg-survey-finds-135258183.html ("Some security reservations and usage preferences exist, but the increased adoption of digital business models provides a compelling argument for retailers, content providers and advertisers to conquer the digital divide. . . . In looking at mobile phones, only 28 percent said they would be willing to receive such advertising for a lower fee.")

300. *See* Schwartz & Solove, *supra* note 2, at 1815 n.1 (discussing the increase of US Internet users and how they are ready to limit online tracking for ads).

301. *See* Jonathan Feldman, *Carrier IQ: Mobile App Crap Must Stop*, INFO. WK. (Dec. 1, 2011, 9:45 AM), http://www.informationweek.com/news/security/mobile/232200532 ("The Carrier IQ situation is an insane breach of trust for enterprises. And unless phone makers copy the Apple model, where carriers can't pre-install app crap, it will happen again. . . . The whole model needs to change, or this incident will be repeated. Carriers currently control the phone, and work with third parties to build management software that they need. The third parties have no skin in the game in terms of the trust relationship with the enterprise. . . . Now contrast that to the simpler Apple model, where Apple delivers a phone with fundamental firmware, absent the app crap. Both Apple and the carriers have major skin in the game to preserve the trust of the enterprise. If carriers want to have management capabilities on the iPhone, they'll have to EXPLICITLY have permission from the enterprise.")

302. *See Coase and Transaction Costs*, *supra* note 120.

In assessing do-not-track's feasibility, P3P's failure serves as a useful blueprint going forward.[303] Do-not-track as contract addresses P3P's main limitations in two key ways. First, do-not-track is incredibly simple: there is only one option to select and follow. Second, do-not-track is enforceable under the law of contract in its own right, and may draw regulatory support from the FTC.[304] Conversely, corporate resistance to do-not-track rings hollow.[305] Corporate protestations lack credibility given the transaction costs and lack of notice currently imposed on consumers.[306] A corporation has the power to refuse the connection if the proffered terms are too complex or are not offered in machine-readable format. If terms beyond do-not-track are expressed in a consumer's automated contract with an online service provider, the service provider is free to terminate the connection. Corporations have successfully used this argument against their customers.[307] They should be held to their own standard.

303. *But see FTC Significant Steps*, *supra* note 4 ("FTC Commissioner Julie Brill spoke at the Online Trust Alliance (OTA) Forum today and noted . . . . '*I don't see this as a toggle switch-on or off*,' but rather 'a place where consumers can choose through a *dashboard mechanism* what they want . . . .' She further stated that the World Wide Web Consortium (W3C) Tracking Protection Working Group is working around issues like 'what does tracking mean' and other technical issues." (emphasis added)).

304. *See supra* Part III.A (discussing FTC backing of a do-not-track option).

305. *See also* discussion *supra* note 233.

306. *See* Juliet M. Moringiello, *Signals, Assent and Internet Contracting*, 57 RUTGERS L. REV. 1307, 1315-19 (2005) ("Electronic contracting stretches contract doctrine even further. . . . Today . . . courts apply the objective theory of contracts to terms delivered electronically without considering the differences between paper and electronic communications. . . . [I]t is difficult to find in their reported decisions a coherent framework for analyzing electronic agreements."); *see also* Lucian A. Bebchuk & Richard A. Posner, *One-Sided Contracts in Competitive Consumer Markets*, *in* BOILERPLATE: THE FOUNDATION OF MARKET CONTRACTS 3, 4 (Omri Ben-Shahar ed., 2007) ("The existence of a one-sided contract does not imply that the *transaction* will be one-sided but only that the seller will have *discretion* with respect to how to treat the consumer." (second emphasis added)); *Coase and Transaction Costs*, *supra* note 120; *Consumer Protection*, *supra* note 120.

307. *See* Specht v. Netscape Commc'ns Corp., 150 F. Supp. 2d 585, 594 (S.D.N.Y. 2001) ("Clicking on the notice links the user to a separate web page containing the full text of the license agreement, which allegedly binds any user of the information on the site. However, the user is not required to click on an icon expressing assent to the license, or even view its terms, before proceeding to use the information on the site."); *see also* Smallwood v. NCsoft Corp., 730 F. Supp. 2d 1213, 1227 (D. Haw. 2010) ("The Court finds the agreement here valid. Plaintiff had notice of the User Agreement, was required to affirmatively agree to it by clicking "I agree," and had an opportunity to cease playing Lineage II if he disagreed with it.").

IV. CONCLUSION

This Article advances a simple hypothesis: consumers should be able to effectively offer their own enforceable terms in online contracts. There is no reasoned ground in contract law or the economic weighing of transaction costs to prohibit consumers from doing so. Further, consumer-proffered automated contracts offer a potential solution to several long-standing and troubling conundrums in online contract law as it has drifted from its traditional common-law moorings.

The problem of online contracting is one of information poisoning: there is too much information. This is true for privacy policies, EULAs, and TOSs. Corporate-drafted contracts may look like the contracts that courts are accustomed to enforcing, but they are written in legalese that consumers are unlikely to understand. Further, enforcing corporate terms in individual consumer cases does not simplify analysis across cases. Each corporate privacy policy may seem simple, well drafted, and therefore the best document for a court to enforce. But each policy is different, and the number of online corporate privacy policies, EULAs, and TOSs is high.

To the extent that courts have tried to address the problem of online contracting, they have attempted to reinsert humans into the contracting equation by insisting that consumers read an ever-greater number of ever-longer contracts. Even courts that have identified information costs as the problem have determined, incorrectly, that the solution is more information. The problem of too much information cannot be solved by more information.

The answer is not more humans in electronic contracting, but more computers. Rather than resolving these enduring questions of consumer contracts by reemphasizing the human element of contracting, this Article proposes to permit consumers to offer enforceable contract terms via automated processes. Consumers should be able to set machine-readable contract terms in precisely the same manner that corporations do now. The law as it stands is deeply imbalanced because only corporations can conduct their contracting in an automated manner. Consumer-side automated contracting would put the power to determine contract terms—and thus privacy—back in individuals' hands.