Missouri Law Review

Volume 80
Issue 3 *Summer 2015*

Article 7

Summer 2015

Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent

Nancy S. Kim

D. A. Telman

Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent

Nancy S. Kim[*]

D. A. Jeremy Telman[**]

ABSTRACT

Although the government's data-mining program relied heavily on information and technology that the government received from private companies, relatively little of the public outrage generated by Edward Snowden's revelations was directed at those private companies. We argue that the mystique of the Internet giants and the myth of contractual consent combine to mute criticisms that otherwise might be directed at the real data-mining masterminds. As a result, consumers are deemed to have consented to the use of their private information in ways that they would not agree to had they known the purposes to which their information would be put and the entities – including the federal government – with whom their information would be shared. We also call into question the distinction between governmental actors and private actors in this realm, as the Internet giants increasingly exploit contractual mechanisms to operate with quasi-governmental powers in their relations with consumers. As regulators and policymakers focus on how to better protect consumer data, we propose that solutions that rely upon consumer permission adopt a more exacting and limited concept of the consent required before private entities may collect or make use of consumer's information where such uses touch upon privacy interests.

[*] Professor of Law and ProFlowers Distinguished Professor of Internet Studies, California Western School of Law.

[**] Professor of Law, Valparaiso University Law School. We thank Elizabeth Littlejohn and Alyssa Spartz for their research assistance and Karen Koelemeyer for her editorial assistance.

TABLE OF CONTENTS

INTRODUCTION

In 2013, Edward Snowden, a contractor working for the National Security Agency ("NSA"), shared with journalists from the Manchester *Guardian* information revealing that the NSA was engaged in a massive data-mining operation that enabled the NSA to eavesdrop on the telephonic and electronic communications of U.S. citizens and residents.[1] On June 5, 2013, *Guardian* reporter Glenn Greenwald published the first[2] of a long series of articles (and now also a book)[3] in which he revealed that the NSA was collecting the phone records of millions of Verizon customers daily.[4] That same day,

---

1. *See* GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE 20–32 (2014) (detailing the author's initial contacts with Snowden and the nature of the Snowden revelations).

2. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

3. GREENWALD, *supra* note 1.

4. The swift response to this "revelation" is somewhat mysterious, as *The New York Times* reported on precisely this sort of government surveillance through the telecommunications providers back in 2005. James Risen & Eric Lichtbau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html?_r=0. Glenn Greenwald, the journalist who broke the Snowden revelations, published a best-selling book in 2006 detailing the NSA's warrantless wiretapping program that the Bush Administration launched in 2001. GLENN GREENWALD, HOW WOULD A PATRIOT ACT? DEFENDING AMERICAN VALUES FROM A PRESIDENT RUN AMOK (2006). *See also* David S. Kris, *On the Bulk Collection of Tangible Things*, 7 J. NAT'L SEC. L. & POL'Y 209, 210–11 (2014) (observing that the bulk collection of telephone metadata disclosed by Edward Snowden had occurred previously and was the cause of litigation, but the U.S. government had never confirmed that such collection took place). The American Civil Liberties Union ("ACLU") filed a number of lawsuits challenging the practice, and Congress eventually granted immunity to the telecommunications companies for their role in such surveillance. *See In re* NSA Telecommc'ns Records Litig., 483 F. Supp. 2d 934, 937 (N.D. Cal. 2007) (recounting allegations that Verizon Communications, Inc. disclosed telephone records to the NSA in violation of California residential customers' privacy rights); Al-Haramain Islamic Found. v. Bush, 451 F. Supp. 2d 1215, 1218 (D. Or. 2006) (detailing allegations that the NSA engaged in electronic surveillance of communications between plaintiff's directors and third parties in violation of FISA), *rev'd*, 507 F.3d 1190 (9th Cir. 2007); Terkel v. AT&T Corp., 441 F. Supp. 2d 899, 901 (N.D. Ill. 2006) (recounting allegations that AT&T provided to the NSA records of telephone calls of its customers in violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2702(a)(3) (2000 & Supp. IV 2005)); Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 978 (N.D. Cal. 2006) (recounting plaintiffs' allegations that AT&T collaborated with the NSA in an illegal and massive warrantless surveillance program); ACLU v. NSA, 438 F. Supp. 2d 754, 758 (E.D. Mich. 2006) (summarizing plaintiffs' constitutional and statutory challenges to the NSA's terrorist surveillance program), *vacated*, 493 F.3d 644 (6th Cir. 2007).

Greenwald reported on the NSA's PRISM program, through which it gained access to data collected by technology companies including Google, Facebook, Apple, Microsoft, YouTube, and other U.S. Internet service and telephone communications providers.[5] According to the *Guardian*, the PRISM program went beyond mere data mining. It gave the NSA direct access to these companies' systems, so that it could access "email, video and voice chat, videos, photos, voice-over-IP – Skype, for example – chats, file transfers, social networking details, and more."[6]

The media were quick to respond. Edward Snowden became a household name, and debates rage over whether he is a hero or a traitor.[7] Condem-

---

Congress responded by amending the Foreign Intelligence Surveillance Act to immunize telecommunications companies from liabilities that might arise from their participation in government-authorized surveillance of their customers:

> [N]o action, claim, or proceeding shall lie or be maintained in any court, and no penalty, sanction, or other form of remedy or relief shall be imposed by any court or any other body, against any person for the alleged provision to an element of the intelligence community of any information (including records or other information pertaining to a customer), facilities, or any other form of assistance, during the period of time beginning on September 11, 2001, and ending on the date that is the effective date of this Act, in connection with any alleged classified communications intelligence activity that the Attorney General or a designee of the Attorney General certifies, in a manner consistent with the protection of State secrets, is, was, would be, or would have been intended to protect the United States from a terrorist attack. This section shall apply to all actions, claims, or proceedings pending on or after the effective date of this Act.

H.R. 3321, 110th Cong. § 5(a) (2007); Federal Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008).

5. Glenn Greenwald & Ewan MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN (June 7, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

6. *Id*. *See also* Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J. L. & PUB. POL'Y 117, 124 (2015) (finding that certain government data collection programs exceeded the government's authority to engage in such collection under the Constitution's Fourth Amendment); Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations,* 37 HARV. J. L. & PUB. POL'Y 757, 760 (2014) (highlighting statutory and constitutional infirmities in the NSA's data collection operations and calling for a legislative response); David S. Kris, *On the Bulk Collection of Tangible Things*, 7 J. NAT'L SEC. L. & POL'Y 209, 213–23 (describing the operations of NSA surveillance programs the existence of which the government has confirmed).

7. *See, e.g.*, G. Michael Fenner, *Edward Snowden: Hero or Traitor*, NEB. LAWYER 13, 21 (Nov./Dec. 2014) (concluding that it is too soon to tell whether Snowden is a hero, a traitor, or both); Mary-Rose Papandrea, *Leaker Traitor Whistleblower Spy: National Security Leaks and the First Amendment*, 94 B.U. L. REV. 449, 454 (2014) (contending that government employees who leak secret information are entitled to First Amendment protections so long as they are neither traitors nor spies);

nation of the NSA's PRISM program was nearly universal.[8] But while a wave of outrage was directed at the government agency, the private companies that provided the government with their customers' information largely escaped criticism or condemnation.[9] This is striking because if the NSA act-

---

Katy Steinmetz, *The Edward Snowden Name Game: Whistle-Blower, Traitor, Leaker*, TIME (July 10, 2013), http://newsfeed.time.com/2013/07/10/the-edward-snowden-name-game-whistle-blower-traitor-leaker/ (citing a Quinnipiac poll in which 55% said they consider Snowden a "whistleblower," 34% consider him a traitor, and 11% could not choose between the two). Unsurprisingly, U.S. Director of National Intelligence James Clapper denounced Snowden's conduct as "reprehensible," while Glenn Greenwald argued that people who leak classified information to journalists are "heroes." Glenn Greenwald, *On Whistleblowers and Government Threats of Investigation*, THE GUARDIAN (June 7, 2013), http://www.theguardian.com/commentisfree/2013/jun/07/whistleblowers-and-leak-investigations.

8. *See* Timothy B. Lee, *Here's Everything We've Learned About How the NSA's Secret Programs Work*, WASH. POST (June 25, 2013), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/25/heres-everything-weve-learned-about-how-the-nsas-secret-programs-work/ (stating that PRISM is "a system for expediting the delivery of private information *after* company lawyers have scrutinized a government request"); *Massive NSA Phone Data-Mining Operation Revealed*, ACLU (June 5, 2013), https://www.aclu.org/national-security-technology-and-liberty/massive-nsa-phone-data-mining-operation-revealed (ACLU criticizes NSA's PRISM Program); Charles Savage, Edward Wyatt & Peter Baker, *U.S. Confirms That It Gathers Online Data Overseas*, N.Y. TIMES (June 6, 2013), http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?pagewanted=all&_r=0 (summarizing criticism of the NSA's PRISM Program); Christopher Zara, *Jim Sensenbrenner, Republican Author of Patriot Act, Says NSA PRISM Surveillance Goes Too Far*, INT'L BUS. TIMES (June 9, 2013), http://www.ibtimes.com/jim-sensenbrenner-republican-author-patriot-act-says-nsa-prism-surveillance-goes-too-far-1297697 (explaining that the author of the Patriot Act continues to criticize NSA's PRISM Program); *but see* Brett Logiurato, *The NSA's PRISM Program Is Shockingly Uncontroversial with the American Public*, BUS. INSIDER (June 17, 2013), http://www.businessinsider.com/prism-surveillance-poll-nsa-obama-approval-2013-6 (characterizing a recent poll as suggesting that the American response to the PRISM program was a "collective shrug").

9. *See* Marc A. Thiessen, *Leaks, Not the NSA Programs, Deserve Condemnation*, WASH. POST (June 10, 2013), http://www.washingtonpost.com/opinions/marc-thiessen-leaks-not-the-nsa-programs-deserve-condemnation/2013/06/10/e91d09ac-d1c9-11e2-a73e-826d299ff459_story.html (stating that critics focused on the NSA program rather than the implications of Snowden's leaks); *see also* Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (showing the backlash against the NSA for mining data collected by Yahoo and Google); *Worldwide Reaction to NSA/PRISM Surveillance – An Overview*, INFOSECURITY MAG. (June 12, 2013), http://www.infosecurity-magazine.com/news/worldwide-reaction-to-nsaprism-surveillance-an/ (revealing that the reaction to Snowden's leaks tended to be

ed illegally, it was able to do so only because the Internet giants were already engaged in data mining. Major telecommunications and Internet-based businesses regularly engage in highly invasive data mining, and they do so largely without negative consequences, even though their conduct is what makes NSA data mining possible.[10] That is, the U.S. government lacks the surveillance *savoir faire* of these private businesses.[11] Private businesses harvest their customers' data all the time with impunity.

This Article explores the reasons why people are generally tolerant of private surveillance and argues that such surveillance is, if anything, more violative of privacy and personal autonomy than is government surveillance. We use the term "Internet giants" to refer to those technology companies that dominate the online environment, such as Google, Facebook, Yahoo, and Microsoft. We argue that, due to their size and market dominance, these companies exercise quasi-governmental authority and monopoly power that makes consumer consent to data collection meaningless.

In Part II, we discuss and reject three reasons often given for the lack of outrage at private surveillance. First, the courts generally support the notion

---

negative toward the NSA, rather than any other involved entities). There is some evidence that the private companies that cooperated with the NSA did face a backlash in the form of lost international business. *See* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 121–22 (2015) (reporting that U.S. cloud computing providers suffered a backlash in 2013 and may have lost between $22 and $35 billion in revenues over three years as companies switched to Swiss or other countries perceived as neutrals); Laura K. Donohue, *High Technology Consumer Privacy and US National Security*, BUS. L. REV. (forthcoming 2015), http://scholarship.law.georgetown.edu/facpub/1457, at 4–6 (detailing revenues lost by U.S. companies as a result of their association with NSA data mining); Susan Ariel Aaronson & Rob Maxim, *Data Protection and Digital Trade in the Wake of the NSA Revelations*, 48 INTERECONS. 281 (2013) (contending that Snowden's revelations "have threatened U.S. leadership of the Internet, as well as American market share").

10. The first top-secret document that Snowden leaked was an order from the Foreign Intelligence Surveillance Court allowing the NSA to subpoena metadata from Verizon. *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc., No. BR:13-80 (FISC, Apr. 13, 2013), http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order. The second was a forty-one-slide PowerPoint presentation outlining the PRISM program. Greenwald & MacAskill, *supra* note 5. The government would not have had access to any of this information if the private companies were not collecting and maintaining it for their own purposes. *Id.* As the NSA PowerPoint presentation notes, government access to metadata "is 100% dependent on ISP provisioning." *Id.*

11. *See* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (describing the NSA's need to have private companies grant access to their databases).

that people who use technology, including telephone and Internet service, agree to the Terms of Service ("TOS") that the providers of those services furnish. The Internet giants disclose in those TOS that they engage in data mining, or at least that they have the right to do so. As a result, the argument goes, nobody should be outraged that the Internet giants engage in mining the data provided by the customers because the customers have consented to such use.

Second, government data mining is more threatening than private data mining because the government has the power to detain, interrogate, arrest, and even, in certain circumstances, target individuals, including U.S. citizens, for killing.[12] Private businesses data mine simply so that they can send consumers advertisements and offers that will most likely interest them.

Third, and relatedly, some argue that data mining by private companies do not harm consumers. Private companies provide the public with useful products, and they use metadata to enhance those products and to deliver those products more efficiently to the consumers who desire them.

In Part II, we argue that consumers have not given meaningful consent to private companies' data mining. We discuss survey data that indicates that consumers would not willingly choose to sacrifice their privacy in exchange for targeted advertising. Finally, we discuss the ways in which private data mining harms ordinary consumers.

In Part III, we go a bit further and argue that data mining by the Internet giants is, if anything, more objectionable than government data mining. The Internet giants use data mining to shape and control the environment in which consumers use their products and services. They do so without either transparency or the sort of regulation and oversight to which government entities are subject. In addition, specialized legislation immunizes them from the sorts of liability to which natural persons are exposed. Companies use data mining to shape the lives of natural persons in myriad ways, ranging from terms and conditions of employment and the approval of individual credit to the cultural transformations of the reasonable expectation of privacy and control over intellectual property. In so doing, the Internet giants undermine any meaningful distinction between private and governmental data mining. Private companies use data mining to override political consensus that has been achieved through democratic processes and to dictate to We the People, the conditions of our existences. Corporate power allows private actors to undertake governmental functions without being subject to democratic controls,

12. For arguments defending the legality of lethal drone strikes against U.S. citizens, see Alberto R. Gonzales, *Drones: The Power to Kill*, 82 GEO. WASH. L. REV. 1, 4 (2013) (recommending procedures to protect the rights of American citizens while also placing on a firmer legal footing the President's power to order drone strikes against U.S. citizens and finding that the targeted killing of U.S. citizen Anwar Al-Aulaqi appears to have been justified); Marshall Thompson, *The Legality of Armed Drone Strikes against U.S. Citizens within the United States*, 2013 BYU L. REV. 153, 155 (contending that a drone strike against a U.S. citizen within the United States would be permissible under the law of armed conflict in certain circumstances).

and data mining is both a product of, and a tool to facilitate, this corporate usurpation of democracy.

In Part IV, we return to our focus on the thin concept of consent as it applies to contract formation. While conceding the market efficiencies that flow from form contracting generally, we contend that a more robust concept of consent ought to be applicable in the context of data mining that infringes on personal privacy. Before corporations can harvest consumer data, they must disclose the purposes for which they will use that data, and consumers must specifically and expressly consent to those uses. We believe that effective communication of data collection practices is possible only when the process by which companies elicit consumer consent affects the consumer experience. We argue that the process of consent should be disruptive, not the seamless, nearly frictionless process that it is now. There must be a moment when consumers are conscious of the fact that, by purchasing a product or services, they are agreeing to have their data collected in ways that are clearly identified and for purposes that are spelled out and to which they agree with specificity.

Our aim here is not to condone government overreaching. Rather, we intend to show that private data mining is just as objectionable and harmful to individual rights as is governmental data mining. Moreover, because corporate actors are now empowered to use their technological advantages to manipulate and dictate the terms on which they interact with the public, they govern us in ways that can mimic and even supersede governance through democratic processes. From this perspective, the distinction between private and public data mining becomes less significant. The government relies on private companies to provide it with the metadata it needs for its data-mining projects, and private companies engage in data-mining practices about which we should be every bit as suspicious as we are about NSA data mining.

I. CONSUMERS, CONSENT, AND DATA MINING

In this Part, we address three common arguments for why people do not object to data mining by private companies. The most formidable argument is that consumers consent to data mining, among other things, when they agree to the TOS of the Internet giants and other private enterprises prior to making use of services provided by them. Moreover, the argument goes, consumers actually want companies to mine their data because the companies use consumers' data to provide useful goods and services. In the alternative, the Internet giants contend, private data mining does no harm.

We disagree with all three arguments. First, we draw on the wealth of recent scholarship demonstrating that consumers have not consented in any meaningful way to the TOS that the law deems them to have accepted either through use of services or through the meaningless click that is purported to constitute consent to non-negotiable terms. Most significantly, we contend that, while contractual consent may suffice to bind consumers to ordinary

commercial terms, privacy is different,[13] and the contractual concept of consent is insufficiently robust to be used as a vehicle for stripping citizens of their zone of privacy.

Second, we summarize survey data that suggests that consumers actually do not want to sacrifice their privacy in exchange for the services that the Internet giants provide, such as targeted advertising. Finally, because private companies do not fully disclose the nature of the data mining in which they engage or the purposes for which they use metadata, consumers really have no idea of the extent of the harms caused by private data mining.

A. What We Talk About When We Talk About Consent

Companies routinely claim that users consent to extensive data collection practices by agreeing to the companies' TOS.[14] Facebook, a corporate giant with its hand perennially caught in the privacy cookie jar,[15] recently found itself embroiled in yet another public controversy when researchers published a study revealing that Facebook had manipulated its users' news feeds in order to evaluate whether doing so affected the nature of users' posts and presumably their moods.[16] The company's response was that users consented to this type of study by agreeing to its TOS.[17]

Google similarly used the rhetoric of consent to justify its practice of scanning Gmail users' emails. Plaintiffs in a class action lawsuit against Google[18] argued that the Internet giant's practice of scanning users' emails

---

13. There are other important rights that may be affected by adhesive contracts, but, in this Article, we focus primarily on privacy rights.

14. In making these claims, these companies are playing into the tendency of judges and even consumers to blame themselves for failing to read terms. *See* Eric A. Zacks, *Contracting Blame,* 15 U. PA. J. BUS. L. 169, 171 (2012) ("We have a tendency to blame the victim in retrospect, and the contract preparers 'assist' us in doing so by presenting contracts that reinforce the other party's blameworthiness.").

15. *See* Victor Luckerson, *7 Controversial Ways Facebook Has Used Your Data*, TIME (Feb. 4, 2014), http://time.com/4695/7-controversial-ways-facebook-has-used-your-data/ (outlining the various ways Facebook's privacy settings affect user data); *see also* Vindu Goel & Edward Wyatt, *Facebook Privacy Change Is Subject of F.T.C. Inquiry*, N.Y. TIMES (Sept. 11, 2013), http://www.nytimes.com/2013/09/12/technology/personaltech/ftc-looking-into-facebook-privacy-policy.html (describing the broad privacy settings for Facebook users and the implications of accepting those terms).

16. Vindu Goel, *Facebook Tinkers with Users' Emotions in News Feed Experiment, Stirring Outcry,* N.Y. TIMES (June 29, 2014), http://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html.

17. *Id.* ("The company says users consent to this kind of manipulation when they agree to its terms of service."); *cf.* SCHNEIER, *supra* note 9, at 47 ("The overwhelming bulk of surveillance is corporate, and it occurs because we ostensibly agree to it.").

18. *In re* Google Inc. Gmail Litig., No. 5:13-MD-02430-LHK (N.D. Cal. Sept. 26, 2013).

violated the federal Wiretap Act, as amended by the Electronic Communications Privacy Act.[19] The Wiretap Act prohibits the interception of "wire, oral or electronic communications" without "prior consent" to the interception.[20]

Google first claimed that plaintiffs – who used Google's Gmail service – consented to the terms of its online TOS[21] and Privacy Policy which "essentially stated throughout the class period that Google could use information from users to '[p]rovide, maintain, protect, and improve [its] services (including advertising services) and develop new services.'"[22] Google then argued that the plaintiffs' claims under the Wiretap Act failed because they had expressly consented to the terms in its TOS and Privacy Policy and, thus, to the scanning.[23]

However, users generally do not know that by clicking on an icon or hyperlink they are entering into a legally binding agreement. Numerous testimonies from consumers indicate that they often do not recall clicking on a link.[24] Few consumers actually read even part of the terms, and fewer still, *all* of the terms in a TOS or privacy policy. One study found that "only one or two of every 1,000 retail software shoppers access the license agreement and that most of those who do access it read no more than a small portion."[25] Another study of retail software sales purchasers found that 1.4% of 222 test subjects reported reading end-user license agreements ("EULAs") often, although a greater percentage (24.8%) reported reading parts of the agreement

19. 18 U.S.C. § 2511(1) (2012).

20. *Id*.

21. We use "TOS" to refer to both "terms of service" and "terms of use."

22. Defendant Google's Motion to Dismiss Plaintiffs' Consolidated Individual and Class Action Complaint: Memorandum of Points and Authorities in Support Thereof, *In re* Google Inc. Gmail Litig., No. 5:13-MD-02430-LHK (N.D. Cal. June 13, 2013), 2013 WL 3297861, at 4 (alterations in original) (citations omitted).

23. *See id.* at 23, lines 10–12 and 23–24, and at 24, lines 20–22 ("Under federal law, the consent of a single party to a communication is [a] complete defense to any liability and so the consent of the Gmail user alone is sufficient to bar a claim. . . . Because the Gmail Plaintiffs are bound to Google's TOS and/or Privacy Policy, they have expressly consented to the scanning disclosed in these terms. . . . Because the Gmail Plaintiffs are bound to these terms as a condition of using Gmail, they cannot pursue a claim under ECPA, which precluded liability based on a single party's consent.").

24. *See* Vernon v. Qwest Commc'ns Int'l, Inc., 857 F. Supp. 2d 1135, 1147 (D. Colo. 2012) (noting that plaintiff was unable to recall receiving a welcome letter or clicking accept), *aff'd*, 925 F. Supp. 2d 1185 (D. Colo. 2013); Fusha v. Delta Airlines, No. RDB–10–2571, 2011 WL 3849657 (D. Md. Aug. 30, 2011) (finding that plaintiff could not recall clicking on "Accept" hyperlink).

25. Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts,* 43 J. LEGAL STUD. 1, 1 (2014).

or browsing its contents. Of those surveyed, 66.2% reported rarely reading or browsing EULAs, and 7.7% reported never having noticed or read them.[26]

In a widely circulated story, Game Station, a computer game retailer, included in its online contract the right to claim the "souls" of 7500 of its online customers. Very few nullified the soul-claiming clause, even though they could have done so by clicking a box to opt-out, which would also have rewarded them with a £5 voucher. Given the number of people who did so, Game Station believes as many as 88% of people do not read the terms.[27]

No one reads all of the terms every time that they enter into an online agreement. Online terms are too long, they are often hyperlinked to other web pages containing more terms, the terms are dynamic and frequently updated, and they are ubiquitous.[28] It is simply impossible for consumers to give informed consent to all of the online contracts into which they enter. No human being has the cognitive capacity or the time to read through every digital contract that he or she encounters.[29]

It is not the adhesive nature of online terms that makes consent impossible. While paper mass consumer contracts may also be one-sided and non-negotiable, they are not inherently unreadable for the simple reason that they are tangible. The cost of printing constrains the magnitude of terms and a business's desire to update them. By contrast, online contracts balloon to comic lengths, as illustrated by the iTunes TOS which, when printed in eight-point font, extend to thirty-two pages of text elaborating the terms of a ninety-nine cent transaction.[30] These terms are frequently updated.[31] But the problems associated with online contracting now extend to paper contracts as well because paper contracts now frequently incorporate online terms by reference.

---

26. Nathaniel S. Good, Jens Grossklags, Deirdre K. Mulligan, & Joseph A. Konstan, *Noticing Notice: A Large-Scale Experiment on the Timing of Software License Agreements*, paper presented to the Conference on Human Factors in Computing Systems, Apr. 28–May 3, 2007, San Jose, CA, http://people.ischool.berkeley.edu/~jensg/research/paper/Grossklags07-CHI-noticing_notice.pdf (last visited July 17, 2015).

27. *7,500 Online Shoppers Unknowingly Sold Their Souls*, FOXNEWS (Apr. 15, 2010), http://www.foxnews.com/tech/2010/04/15/online-shoppers-unknowingly-sold-souls/. We believe Game Station's estimate is too high given the available studies and the existing cases. *See generally* NANCY S. KIM, WRAP CONTRACTS: FOUNDATIONS AND RAMIFICATIONS 85–86, 128–29 (2013) (citing examples of consumer failure to notice terms and possible explanations).

28. *See* KIM, *supra* note 27, at 54–69.

29. *See* OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 27 (2014) ("Reading all the privacy disclosures we received in 2008 would take each of us seventy-six work days, for a national total of over fifty billion hours – an opportunity cost greater than the GDP of Florida.").

30. *Id*. at 24, Plate 1 (after page 134).

31. KIM, *supra* note 27, at 65–67.

The notion that users actually consent to online contracts is widely mocked in popular culture,[32] yet the common law remains unchanged. Courts continue to conclude that a click constitutes a "manifestation of assent," despite all evidence to the contrary. Consumers acquiesce because they have no other meaningful choice. The ubiquity of wrap contracts[33] means that, in order to participate in modern life, consumers must act in a way that courts construe as consent.[34] According to a recent column in *The New York Times*, one-third of the top websites require users to agree to some form of limitation on their legal rights – usually mandatory arbitration provisions and class-action waivers.[35] This might suggest that consumers have the ability to shop around for the best terms. However, as indicated above, consumers have neither the time nor the information that would enable them to do so. In any case, given recent Supreme Court jurisprudence favoring such provisions,[36] it will not take long for other websites to catch up in the race to the bottom.

Even if the sheer scope of online terms did not undermine the argument that users consent to terms, there is an additional problem. Companies employ broadly-worded language and appeal to users' optimism bias. For ex-

---

32. *South Park: Human CentiPad* (Comedy Central television broadcast Apr. 27, 2011); *Last Week Tonight with John Oliver* (HBO television broadcast June 1, 2014), https://www.youtube.com/watch?v=fpbOEoRrHyU; *Saturday Night Live: The People's Court* (NBC television broadcast Aug. 11, 1986).

33. By "wrap contract," we refer to a unilaterally imposed set of terms that the drafter regards as legally binding. *See* KIM, *supra* note 27, at 2–3. Wrap contracts, encompassing shrinkwraps, clickwraps and browsewraps, are presented to non-drafting parties in ways that have developed since the 1980s and generally do not involve the use of a pen. *See id.*

34. After hearing about Facebook's news feed manipulation study, many users responded with a shrug, not because they approved of the study, but because they have accepted that they have no choice, that "user participation has come to equal user consent, a social contract governed by massive terms-of-service agreements that few users fully read or understand." Matt Pearce, *Facebook Experiment Becomes a Debate Over Power and Consent*, L.A. TIMES (July 3, 2014, 5:52 PM), http://www.latimes.com/nation/nationnow/la-na-nn-facebook-study-20140703-story.html#page=1.

35. Jeremy B. Merrill, *One-Third of Top Websites Restrict Customers' Right to Sue*, N.Y. TIMES (Oct. 23, 2014), http://www.nytimes.com/2014/10/23/upshot/one-third-of-top-websites-restrict-customers-right-to-sue.html?abt=0002&abg=1&_r=2.

36. *See e.g.*, Am. Express Co. v. It. Colors Rest., 133 S. Ct. 2304 (2013) (upholding arbitration clause and class-action waiver in the face of a claim that the waiver invalidated plaintiff's access to meaningful redress under a federal anti-trust statute); AT&T Mobility v. Concepcion, 131 S. Ct. 1740 (2011) (upholding a class action waiver notwithstanding plaintiffs' claims that the waiver made the arbitration agreement unconscionable in that it deprived plaintiffs of a meaningful remedy); Rent-a-Ctr. v. Jackson, 561 U.S. 63 (2010) (permitting the arbitrator to decide the issue of whether a clause delegating decisions to the arbitrator was unconscionable); Stolt-Nielsen S.A. v. AnimalFeeds Int'l Corp., 559 U.S. 662 (2010) (finding that arbitrators exceeded their power when they construed an arbitration clause that was silent on class arbitration to permit class arbitration).

ample, the language in Facebook's TOS, which ostensibly justified its news-feed-manipulation study, stated:

> We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, [our partners], the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use. For example, in addition to helping people see and find things that you do and share, we may use the information we receive about you:
>
> - as part of our efforts to keep Facebook [products, services, and integrations] safe and secure;
> - [to protect Facebook's or others' rights or property];
> - to provide you with location features and services, like telling you and your friends when something is going on nearby;
> - to measure or understand the effectiveness of ads you and others see, [including to deliver relevant ads to you];
> - to make suggestions to you and other users on Facebook, such as: suggesting that your friend use our contact importer because you found friends using it, suggesting that another user add you as a friend because the user imported the same email address as you did, or suggesting that your friend tag you in a picture they have uploaded with you in it; [and
> - for internal operations, including troubleshooting, data analysis, testing, research and service improvement].
>
> Granting us permission to use your information not only allows us to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information we receive about you in new ways.[37]

If a user were that rare creature who actually attempted to wade through Facebook's terms, it is likely that he or she would have interpreted this provision to mean that Facebook would exploit user information only to improve

37. The language in brackets was added after the manipulation study was conducted. *See* Kashmir Hill, *Facebook Added 'Research' to User Agreement 4 Months After Emotion Manipulation Study*, FORBES (June 30, 2014), http://www.forbes.com/sites/%20kashmirhill/2014/06/30/facebook-only-got-permission-to-do-research-on-users-after-emotion-manipulation-study/.

its advertising, not that it would experiment on its users by manipulating their feeds.

Similarly, Google has pointed to broad language in its terms to justify email scanning. In *In re Google*, *Inc. Gmail Litigation*,[38] Plaintiffs, while conceding that they had provided legal assent, argued that they did not consent to email scanning, as the language did not specifically refer to it.[39]

Companies may also use wrap contracts in an informal manner to shape public opinion and to gain acceptance for dubious business practices. Companies may justify a dubious practice with easily obtainable contractual consent. A contract legitimizes a new and dubious business practice, such as data collection or experimenting on users, and the constructed consent shifts the blame for the practice from the company to the user. Tess Wilkinson Ryan found that "consumer choice is a very salient feature of how we understand transactional harm,"[40] and that, unless prompted to consider alternative explanations such as firm misbehavior, "subjects in these studies understood transactional harms as products of consumer consent."[41] Similarly, Eric Zacks argues that a contract can "encourage individuals to feel shame, to blame themselves," which may deter them from challenging a contract's enforceability.[42] In other words, the contract serves as a powerful legitimizing tool for companies and may convince consumers, ex-post formation, to shift responsibility away from the companies engaging in dubious practices and toward users for failing to read and understand terms to which they "consented."

Internet-based companies also use shaming and blaming to shape public opinion and normalize dubious practices. Typically, they downplay or belittle negative public reaction as the result of naiveté, irrational conservatism, or ignorance of the way technical matters work, and they may characterize criticisms as harmful to innovation. Executive officers of Sun Microsystems, Facebook, and Google have all issued variations on the theme that privacy is of concern only for old fogies with something to hide.[43] On OkCupid's company blog, one of the founders of the dating website proudly confessed to

38. *See In re* Google, Inc. Gmail Litig., No. 5:13-MD-02430-LHK, 2014 WL 1102660 (N.D. Cal. Mar. 18, 2014).

39. *Id.*

40. Tess Wilkinson-Ryan, *A Psychological Account of Consent to Fine Print*, 99 IOWA L. REV. 1745, 1781 (2014).

41. *Id.* at 1782.

42. Eric A. Zacks, *Shame, Regret and Contract Design,* 97 MARQ. L. REV. 695, 698 (2014).

43. Helen A.S. Popkin, *Privacy Is Dead on Facebook. Get Over It*, NBC News (Jan. 13, 2010, 8:56 AM), http://www.nbcnews.com/id/34825225/ns/technology_and_science-tech_and_gadgets/t/privacy-dead-facebook-get-over-it/#.U-O_GWNYN19. *See also* Bobbie Johnson, *Privacy No Longer a Social Norm, says Facebook Founder*, THE GUARDIAN (Jan. 10, 2010), http://www.theguardian.com/technology/2010/jan/11/facebook-privacy.

experimenting on its users and even subtly mocked those who would be surprised by such a disclosure, calling it "how websites work."[44]

Cognitive psychologists, scholars, and other researchers who study decision making have provided a multitude of other reasons why consumers may click "agree" to terms without actually agreeing to them.[45] Consumers, in the face of ubiquitous, non-negotiable terms, may succumb to a kind of learned helplessness. Believing that they are unable to negotiate terms, they do not even try to do so.[46] They may be subject to the herd effect, thinking that there is no harm in accepting wrap contract terms because everyone else is doing it. Optimism and overconfidence bias may make it easy for them to convince themselves that they will never be subject to harmful terms or that they will be able to appeal to the company to escape their enforcement.[47]

In sum, courts apply a standard that is too easily met when the question is whether a consumer has consented to a contract. They may well be right to do so in some situations, given the transactional efficiencies thereby achieved. But courts should not restrict consumers' privacy and other foundational rights based on this anemic, non-specific, contractual consent.

B. Do Consumers Really Want Data Mining?

The yawning gap between true consent and judicially-constructed consent does not bother those who believe that wrap contract terms are harmless, as consumers would have agreed to them anyway, or that they are intended merely to stave off the claims of opportunistic consumers.[48] Marketers claim that consumers want more tailored ads. The Digital Advertising Alliance claimed that the "more Internet users learn about the protections and choices available to them, the more comfortable they become with online interest-

44. Christian Rudder, *We Experiment on Human Beings!*, OKTRENDS (July 28, 2014), http://blog.okcupid.com/index.php/we-experiment-on-human-beings/.

45. *See generally* Wilkinson-Ryan, *supra* note 40 (unpacking beliefs, preferences, assumptions, and biases that constitute our assessments of assent to boilerplate).

46. *See* Amy J. Schmitz, *Pizza-Box Contracts: True Tales of Consumer Contracting Culture,* 45 WAKE FOREST L. REV. 863, 888 (2010).

47. DANIEL KAHNEMAN & AMOS TVERSKY, *Conflict Resolution: A Cognitive Perspective*, *in* CHOICE, VALUES AND FRAMES 473 (2000).

48. *See* Lucian A. Bebchuk & Richard A. Posner, *One-Sided Contracts in Competitive Consumer Markets*, 104 MICH. L. REV. 827, 828 (2006) (discussing how one-sided terms give companies protection against opportunistic consumers). For more general defenses of the adequacy of constructive consent in most circumstances, *see* Randy E. Barnett, *Contract Is Not Promise; Contract Is Consent*, 45 SUFFOLK U. L. REV. 647 (2012); Randy E. Barnett, *Consenting to Form Contracts*, 71 FORDHAM L. REV. 627 (2002).

based advertising."[49] Yet, that statement, based upon a poll conducted on behalf of the Alliance, is misleading – the poll results indicate a public resigned to the advertising model of the Internet but concerned about the information collected by marketers.[50] We are skeptical that hordes of consumers affirmatively want better-targeted advertisements, and we believe fewer still would want it if they understood the extent of the data collection required to create targeted advertisements.

We are not the only skeptics. Jack Marshall writes, "[W]hile some consumers see benefit in tailored ads, most don't want their information to be used to tailor them." He discussed a survey conducted by the market research company, Gfk, which found that of 1000 people surveyed, 49% agreed, "Advertising that is tailored to my needs is helpful because I can find the right products and services more quickly." Yet, the same survey found that only 35% agreed that "I use free services online and on smartphones/tablets and don't mind if my data is potentially also used for advertising purposes."[51]

A survey conducted in 2013 by Consumer Action, a non-profit consumer rights organization, supports such skepticism. It found that 49% of all respondents falsely believe that online tracking is unlawful.[52] Furthermore, 69% of respondents would not be willing to allow companies to track, collect,

---

49. *Poll: Internet Users Recognize the Importance of Online Advertising and the Value of Self-Regulation*, DIGITAL ADVER. ALLIANCE (Nov. 5, 2013), http://www.aboutads.info/news.

50. For example, in response to the question – "Which, if any, of the following scenarios would make you more comfortable than you currently are with a company using information about your Web surfing interests to show you relevant ads?" – 27% of 1004 adults polled responded, "If all Web pages displaying these ads included a simple, easy-to-use opt-out option that lets me choose not to have my data used for advertising," 16.3% responded, "If companies providing ads based on my interests were forbidden from collecting or using any sensitive financial or medical information," and 8.0% responded, "If companies providing ads based on my interests were required to participate in an enforcement program that could publicly sanction them if they did not meet their obligations." *Public Opinion Poll*, ZOGBY ANALYTICS (Oct. 2013), http://www.aboutads.info/ZogbyDAAOct13PollResults.pdf. The responses do not indicate that respondents preferred self-regulation to government regulation. *See id.*

51. *See* Jack Marshall, *Do Consumers Really Want Targeted Ads?*, WALL ST. J. (Apr. 17, 2014, 12:30 AM), http://blogs.wsj.com/cmo/2014/04/17/do-consumers-really-want-targeted-ads/. Marshall also cited another study conducted by Qriously, where only 48% of 4000 mobile device users responded that they preferred "targeted" ads over "non-targeted" ones. *Id.* (The question posed to the users was that given that ads "support your apps, which do you prefer?").

52. *Consumers to Online Advertisers: No Tracking for ANY Reason*, CONSUMER ACTION (June 18, 2013), http://www.consumer-action.org/press/articles/no_tracking_for_any_reason. *See also Consumer Action "Do Not Track" Survey Results*, CONSUMER ACTION (2013) [hereinafter *Survey Results*], http://www.consumer-action.org/downloads/english/Summary_DNT_survey.pdf.

and share data *with permission* in exchange for a free product or service.[53] Yet, most websites now track, collect, and share data without express permission or true consent. In response to the statement, "You see no harm in being tracked online if it results in your being shown more relevant ads," 55% "strongly disagree," and 19% "somewhat disagree."[54] A majority (76%) strongly believes that there "should be a way for people to limit when they are tracked online."[55] An overwhelming majority (87%) believes that "you should have the right to control what information is collected about you online."[56]

More telling are survey results conducted from 1999 to 2012 by the Annenberg School for Communication.[57] A survey conducted in 2003 found that:

> 59% of adults who use the [I]nternet at home know that websites collect information about them even if they don't register. They do not, however, understand that data flows behind their screens invisibly connect seemingly unrelated bits about them. When presented with a common version of the way sites track, extract, and share information to make money from advertising, 85% of adults who go online at home did not agree to accept it on even a valued site.[58]

Other surveys suggest that Americans are becoming increasingly concerned that companies are following their online movements. In a 2005 study, 81% disagreed with the statement that "what companies know about me won't hurt me," and 79% agreed that "I am nervous about websites having information about me."[59] In 2009, researchers found that 66% of adult Americans do not want marketers to tailor advertisements. This number was even greater – between 73% and 86% – when survey takers were informed of three common ways that marketers gather data to tailor ads.[60] In sum, the common refrain of marketers – that consumers *want* tailored ads – finds no

53. *Survey Results*, *supra* note 52.

54. *Id.*

55. *Id.* Of the other responses, 14% "somewhat agree"; 3% "somewhat disagree", 6% "strongly disagree" and 1% "don't know/no opinion." *Id.*

56. *Id.* Of the other responses, 8% "somewhat agree," 1% "somewhat disagree,"4% "strongly disagree," and 1% "don't know/no opinion." *Survey Results*, *supra* note 52.

57. Joseph Turow et al., *Americans, Marketers, and the Internet: 1999-2012*, UNIV. OF PA. – ANNENBERG SCH. FOR COMMC'N (2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2423753.

58. *Id.* at 1–2 (citing Joseph Turow, *Americans and Online Privacy: The System Is Broken* 3, *in* Turow et al., *supra* note 57 [hereinafter Turow, *Americans and Online Privacy*]); *see also* Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade,* 3 I/S: J. L. & POL'Y FOR THE INFO. SOC'Y 723, 732 (2008).

59. Turow et al., *supra* note 57.

60. *Id.*

support in studies of consumer preferences. Consumers may want more relevant ads instead of irrelevant ads, but they do not want to lose control over their personal data in order to receive them.

A recent survey conducted by the Pew Research Center found that 91% of adults surveyed "agree" or "strongly agree" that "consumers have lost control over how personal information is collected and used by companies," and that 80% of those who use social networking sites are "concerned about third parties like advertisers or businesses accessing the data they share" on these sites.[61]

In addition to being inaccurate, the claim that consumers like targeted advertising is misleading because consumers do not know the price they are paying for that service. Companies do not collect data on their users *solely* to serve them with more relevant ads. Some of these uses will eventually hurt at least some consumers, even those engaging in lawful behavior. Companies combine and aggregate data in ways that may surprise consumers, and the result may harm some consumers, even if the harm is unintentional.[62] Furthermore, the more companies gather and store information, the greater the likelihood that the information will be used by third parties – known and unknown to the primary website – in an unlawful or unethical manner.

Language employed by websites in their wrap contracts suggests that data collection benefits customers. For example, Twitter's Privacy Policy states that it uses customer information "to display ads about things you may have already shown interest in."[63] Twitter presents this information as an example of why it may share information with third parties, but the Privacy Policy does not limit Twitter's use of the data in any way. Facebook's data usage policy cited above claims that its data collection practices are intended "to provide you with location features and services, like telling you and your friends when something is going on nearby" and "to measure or understand the effectiveness of ads you and others see, including to deliver relevant ads to you."[64] But, as noted in the previous Part, the language is broadly worded, and the company's ability to use the data collected is not limited to these specific examples.

---

61. Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CENTER (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/. *See also* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 19–58 (2015) (explaining surprising ways that data is gathered and used and how it affects reputations).

62. *See generally* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact,* 104 CALIF. L. REV. (forthcoming 2016), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899. "Approached without care, data mining can reproduce existing patterns of discrimination, inherit the prejudice of prior decision-makers, or simply reflect the widespread biases that persist in society." *Id.* at 3.

63. *Privacy Policy*, TWITTER, https://twitter.com/privacy/ (last visited July 19, 2015).

64. *Id.*

The real effect of such policies is to grant the websites broad rights to use and share user information. The companies mislead consumers into believing that "targeted advertisements" are the *only* way the information can be used. Most consumers do not understand what companies can do with their data, and the language of corporate "privacy" policies only misleads them.[65] Many never suspect their data is being used for purposes other than to process orders or create more relevant advertisements. Or, at least they did not until Edward Snowden gave the public a peek into how much data companies collect about us and what they do with it.

C. Does Data Mining Hurt Consumers?

In her keynote address at the Computers Freedom and Privacy Conference, Commissioner Julie Brill of the Federal Trade Commission noted that Edward Snowden's revelations:

> [G]ave the world a crash course in just how much privacy we can expect if we participate at all in an increasingly online and mobile marketplace. . . . Americans are now more aware than ever of how much their personal data is free-floating in cyberspace, ripe for any data miner – government or otherwise – to collect, use, package and sell.[66]

Snowden's disclosures created headaches for the government. It also created headaches for the Internet giants that had lulled the public into believing that the data being collected was unidentifiable and limited to improving free services. As Brill explained:

> We send our digital information out into cyberspace and get back access to the magic of our wired lives. We sense this, but it took Snowden to make concrete what exactly the exchange means – that firms or governments or individuals, without our knowledge or consent, and often in surprising ways, may amass private information about us to

---

65. Turow, *Americans and Online Privacy*, *supra* note 58, at 33. Turow states:

> We found that despite their strong concerns about online privacy, most adults who use the [I]nternet at home misunderstand the purpose of a privacy policy. Just as important, our findings indicate that despite fairly wide awareness that websites collect information about them, adults who use the [I]nternet at home are fundamentally unaware of data flow: how organizations glean bits of knowledge about individuals online, interconnect those bits, link them to other sources of information, and share them with other organizations.

Id.

66. Julie Brill, Comm'r, Keynote Address at the 23rd Computers Freedom and Privacy Conference, Washington, D.C. (June 26, 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/reclaim-your-name/130626computersfreedom.pdf.

> use in a manner we don't expect or understand and to which we have not explicitly agreed.[67]

Corporations track and collect information about users online, and data brokers buy and sell that information to other companies. These companies use the information to make decisions affecting all areas of consumer life.

Companies have the ability to use surveillance for inappropriate discrimination and manipulation.[68] Companies may also start to use correlations to reach conclusions that are unfair or unsupportable.[69] For example, a company may find a correlation between the number of pets a person owns and the number of times that person has been in a car accident and conclude that pet owners are at a higher (or lower) risk. New banking start-up companies are using a variety of information from different sources to determine whether to make consumer loans, even though the validity of the correlations remains unproven.[70] One company even considers as relevant criteria the amount of time a potential borrower spends reading online terms and condi-

---

67. *Id*.

68. *See* SCHNEIER, *supra* note 9, at 109–16 (discussing "weblining," a twenty-first century version of redlining, and technology that helps vendors price discriminate based on consumers past practices, as well as manipulation through product placement and advertisements and the more over Facebook mood manipulation study); *see also* PASQUALE, *supra* note 61, at 25–42 (explaining how "runaway data" is used to make assumptions regarding users' health, income level, credit worthiness, race, sexual orientation and work habits).

69. After leading a review of Big Data and privacy requested by President Obama, John Podesta wrote that Big Data is making the economy work better and saves lives, yet it "raises serious questions," including the "potential for big data analytics to lead to discriminatory outcomes and to circumvent longstanding civil rights protections in housing, employment, credit, and the consumer marketplace." John Podesta, *Findings of the Big Data and Privacy Working Group Review,* THE WHITE HOUSE BLOG (May 1, 2014, 1:15 PM EDT) https://www.whitehouse.gov/blog/2014/05/01/findings-big-data-and-privacy-working-group-review. *See also Big Data: Seizing Opportunities, Preserving Values*, EXECUTIVE OFFICE OF THE PRESIDENT 7 (May 2014) [hereinafter *Big Data*], https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf; PASQUALE, *supra* note 61, at 38 ("Algorithms are not immune from the fundamental problem of discrimination, in which negative and baseless assumptions congeal into prejudice. . . . And they must often use data laced with all-too-human prejudice."); Amy J. Schmitz, *Secret Consumer Scores and Segmentation: Separating "Haves" From "Have-Nots"*, 2014 MICH. ST. L. REV. 1141, 1141 (2014) (noting that consumers have no way to challenge the accuracy of collected data as it usually falls outside the reach of the Fair Credit Reporting Act and that it may "foster discrimination and augment preexisting power imbalances among consumers").

70. Steve Lohr, *Banking Start-Ups Adopt New Tools for Lending,* N.Y. TIMES (Jan 18, 2015), http://www.nytimes.com/2015/01/19/technology/banking-start-ups-adopt-new-tools-for-lending.html?ref=technology (stating that the "technology is so new that the potential is unproved" and "raises questions, especially for regulators who enforce anti-discrimination laws").

tions and whether he or she uses proper capitalization.[71] While there are laws governing the use of some data in some areas, the ability for regulators to monitor and stop unlawful use is limited.[72]

Furthermore, companies can use "surrogates" to gain access to data to which they do not have access. For example, they may use a consumer's occupation as an indicator of income level.[73] Consumers may not know the reason why they were turned down for a job or denied a loan or insurance policy, and the reasons could be based on incorrect or outdated data. Furthermore, the statistical inferences might be discriminatory.[74] The New York Public Interest Research Group found that some auto insurers were charging higher rates to drivers with less education and nonprofessional, nonmanagerial jobs.[75] Already, at least one health care system is using credit card data to make predictions about patients' health – and to take steps to deter what they consider to be unhealthy behavior.[76] That company, which operates more than 900 care centers, purchases data from brokers who gather it from credit card purchases, store loyalty program transactions, and public records. The company then uses this data to identify "high-risk patients" who may then be contacted by doctors and nurses who can reach out and suggest changes to their behaviors.[77]

Data can also be used to help companies determine how much they can charge a particular customer or how much they can raise prices before an existing customer will leave for a competitor. Some argue that using data to set prices may hurt lower-income consumers because they tend to comparison shop less than wealthier consumers.[78] Facial recognition technology, combined with data gathered from social networking sites and public records, may help nightclub owners decide who gets in based upon how much they are

71. *Id.*

72. Brill, *supra* note 66 (noting that while there are rules in place governing the way data can be used, many companies are unaware of these rules and "it is difficult to reach all of those who may be" engaging in unlawful data use activity).

73. Andy Morrison, a consumer advocate at the New York Public Interest Research Group, believes that permissible questions such as occupation and education level are being used "as surrogates for income" in determining insurance premiums. Alina Tugend, *As Data About Drivers Proliferates, Auto Insurers Look to Adjust Rates,* N.Y. TIMES (Apr. 18, 2014), http://www.nytimes.com/2014/04/19/your-money/as-data-about-drivers-proliferates-auto-insurers-look-to-adjust-rates.html. California, however, does not permit the use of occupation or education level. *Id*.

74. *See* Podesta, *supra* note 69 (raising concern about the "potential for big data analytics to lead to discriminatory outcomes and to circumvent longstanding civil rights protections in housing, employment, credit, and the consumer marketplace").

75. Tugend, *supra* note 73.

76. Shannon Pettypiece & Jordan Robertson, *Hospitals are Mining Patients' Credit Card Data to Predict Who Will Get Sick,* BLOOMBERG BUSINESSWEEK (July 3, 2014), http://www.businessweek.com/articles/2014-07-03/hospitals-are-mining-patients-credit-card-data-to-predict-who-will-get-sick.

77. *Id.*

78. *Id.*

likely to spend or encourage retailers to engage in preferential treatment of certain customers.[79]

But data can also violate privacy in much more overt and irksome ways that might strike consumers as creepy or uncanny. For example, *The New York Times* reported in 2012 that Target was tracking shoppers and looking for clues that they were pregnant. The strategy was to target such women with advertising and to give Target a head start on other vendors seeking to lock in consumers developing new shopping patterns.[80] This strategy can have explosive unintended consequences when, for example, the pregnancy has not yet been disclosed to family members who are then alerted to the situation when they notice the targeted ads.

Data can also be used to help corporations better manipulate consumers. Their extensive dossier of consumer habits and preferences may enable companies to better understand and exploit consumers.[81] Ryan Calo argues that companies can use their intimate knowledge of the consumer to take advantage of consumers' cognitive biases and "trigger irrationality or vulnerability in consumers" that propel them to act in ways that may be harmful to their self-interest.[82] The information that companies glean can be used to "generate a fastidious record" of consumer transactions and "personalize every aspect of the interaction" with the marketplace.[83]

It is undoubtedly true that data can be harnessed in socially beneficial ways. Our purpose here is not to denounce "Big Data" or the use of data for research or policy purposes. Our argument is much more narrowly focused: the problem is exploitation of customer data by private companies to further their corporate interest in profit maximization without effective disclosure and true consent of consumers.

II. PRIVATE DATA MINING AS AN EXERCISE OF QUASI-GOVERNMENTAL POWER

The preceding Part explained how data mining by private entities is as intrusive and objectionable as data mining by government entities such as the NSA. In this Part, we contend that the Internet giants function as quasi-

79. *See* Natasha Singer, *When No One Is Just a Face in the Crowd*, N.Y. TIMES (Feb. 1, 2014), http://www.nytimes.com/2014/02/02/technology/when-no-one-is-just-a-face-in-the-crowd.html?_r=0 (reporting on how facial recognition technology offers the ability to "surreptitiously offer some customers better treatment").

80. *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0 ("[T]he key is to reach them earlier, before any other retailers know a baby is on the way.").

81. Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 999 (2014) ("[T]he digitization of commerce dramatically alters the capacity of firms to influence consumers at a personal level.").

82. *Id.*

83. *Id*. at 1002–03.

governmental agencies by implementing governance systems and rules to regulate the conduct of their users.[84] Yet, unlike the government, they are not subject to constitutional limitations or democratic controls.

Private companies can exercise their power over users in two ways: through the exercise of their property rights and through contract. Contract allows private companies to obtain rights they would not otherwise have through mere property ownership. Using contractual means, companies can establish and enforce their own laws, rules, and regulations, just as the government does.

The Internet giants are private entities that, as proprietors, may exercise certain rights over users. They expand those default proprietorship rights and obtain additional rights through their use of contracts. These contracts impose rules and regulations upon users, and allow companies to exercise legislative and administrative authority akin to that of the government. As Margaret Jane Radin has written,[85] private agreements have the ability to undo, for example, consumer protection legislation and the class action mechanism. The myth of consumer consent permits such companies to eliminate terms that might favor consumers in litigation against the Internet giants. The legislative role that private companies play by using these so-called contracts thus undermines many of the fruits of our democratic political process, resulting in what Radin called "democratic degradation."[86]

The Internet giants also enjoy the benefits of specialized legislation, such as Section 230 of the Communications Decency Act ("CDA"), which offers them immunities from certain tort liability similar to those enjoyed by the government, and the Foreign Intelligence Surveillance Act reforms that immunize them from breach of contract claims when they share information with the government in violation of privacy provisions in their agreements with customers.[87] As a result, these companies are subject to neither the burden of transparency nor the constitutional constraints imposed upon state actors; yet they often escape governmental regulation. They benefit from immunity from tort liability in a way that mimics governmental immunity. Unlike the government, however, they are not obligated to act in the public interest, and, unlike elected officials, they are not subject to democratic processes.

---

84. As David S. Evans notes, these governance systems may be socially beneficial. *See* David S. Evans, *Governing Bad Behavior By Users of Multi-Sided Platforms,* 27 BERKELEY TECH. L.J. 1201 (2012).

85. MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (2012).

86. *Id.* at 16.

87. *See* H.R. 3321, 110th Cong. § 5(a) (2007); Federal Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, §§ 702(h)(3), 703(e), 122 Stat. 2436 (2008) (providing that no action may be maintained in any court against a company sharing information with the government in connection with national security investigations).

Finally, we note that while private entities enjoy extraordinary powers as quasi-governmental agencies, they also simultaneously assert their rights as private persons. They are emboldened to do so more aggressively in the aftermath of recent Supreme Court decisions adopting an expansive interpretation of corporate personhood.[88]

A. Privatization of Laws, Rules, and Regulations

The networks of Internet giants are private, not public, which gives them the power to impose certain rules upon users. Their ownership of property – their property being their domain names, their networks, and their business models – grants them certain rights. These rights, in turn, operate as a de facto regulatory regime. As David Evans explains:

> Multi-sided platforms . . . develop governance systems to reduce . . . bad behavior and minimize negative externalities. . . . These platforms enforce such rules by exercising their property rights to exclude users from the platform. In some cases, the rules and penalties imposed by the platform are similar to, and in some cases close substitutes for, rules and penalties adopted by a public regulator.[89]

Internet giants create virtual spaces that consumers inhabit. When consumers do so, they enter a world in which private companies are both service providers and regulatory bodies that govern their own and their users' conduct.

These regulatory regimes often serve to create a certain community and to establish norms of acceptable conduct. Facebook, for example, has a Code of Conduct that specifies what behavior is prohibited on the site. Such governance systems provide for penalties and punishment for misbehavior, including banishment from the site. The companies have the right to impose certain rules as a condition to entry because they own the property of the website. Codes of Conduct are not unique to the online environment. A shopping center, for example, may prohibit certain animals, unruly behavior, or even some otherwise protected activities on the premises.[90] These rules

88. *See* Burwell v. Hobby Lobby Stores, Inc., 134 S. Ct. 2751, 2768–75 (2014) (interpreting the term "person" in the Religious Freedom Restoration Act as protecting the religious liberty interests of for-profit corporations); Citizens United v. FEC, 558 U.S. 310 (2010) (recognizing the free speech rights of corporate entities).

89. Evans, *supra* note 84, at 1204. A "multi-sided platform" brings together "two or more different types of users, who could benefit from getting together, find and interact with each other, and exchange value." *Id*. at 1203. Examples of multi-sided platforms include software platforms, search engines, and social networks. *Id.*

90. *See* Hudgens v. NLRB, 424 U.S. 507, 520–21 (1976) (upholding the right of a mall owner to prevent workers from advertising their labor strike); Lloyd Corp. v. Tanner, 407 U.S. 551, 570 (1972) (upholding the right of a mall owner to exclude Vietnam war protestors from its premises).

do not require consent, provided that the only penalty imposed for disobeying them is ejection from the premises. Notice provides a semblance of fairness and minimizes resistance to ejection, but notice is not required for ejection in most cases.[91] The right to eject someone from purely private property arises from the bundle of rights belonging to a property owner. But wrap contracts can also give rise to property rights.[92]

A contract legitimizes the reallocation of rights from one party to another. For example, a property owner has no right to extract money from a trespasser on its premises – it may only eject the trespasser.[93] Allowing the property owner to arbitrarily establish the fee for the trespass accords the property owner too much power. The owner may, however, charge money for entry. Notice provides the visitor with the opportunity to participate in the process – even if he does not set the fee for entry, he can reject the fee by refusing to pay it in exchange for entering the premises. But in order for the notice to rise to the level of contract, there needs to be consent. In other words, the user must have seen or should have seen the notice – what courts refer to as actual or constructive notice – regarding the fee before it can be enforced.[94]

The online environment is different from the physical one, however, in the way that it has expanded the role of the Code of Conduct. Online Codes of Conduct are much lengthier, encompass more activities, impose unexpected burdens, and extract rights that offline Codes of Conducts do not. Website Codes of Conduct typically impose rules or obligations that carry penalties other than ejection. In such cases, the website proprietors seek to exercise rights that they do not already possess or that are unallocated.[95] This is often the case where technology creates business opportunities in grey areas of the law. Businesses seek to use technological advances to their advantage.

Internet-based companies, more so than traditional physical-world corporations, have a reputation for risk-taking, moving quickly, and worrying about the consequences later. Facebook's motto, "Move fast and break

---

91. *See* Richard M. Hynes, *Posted: Notice and the Right to Exclude*, 45 ARIZ. ST. L.J. 949, 958 (2013) (observing that the default U.S. rule is that notice is satisfied so long as the boundaries of the property are posted).

92. *See* Loretto v. Teleprompter Manhattan CATV Corp., 458 U.S. 419, 433 (1982) (quoting Kaiser Aetna v. United States, 444 U.S. 164, 176 (1979)) (characterizing the right to exclude as "one of the most essential sticks in the bundle of rights that are commonly characterized as property").

93. KIM, *supra* note 27, at 135–36. We refer here only to the common law and not specific local legislation, which may differ.

94. *Id.* at 136–37.

95. For further discussion on the various functions of notice and consent with respect to particular rights, see *id.* at 93–109; Nancy S. Kim, *Boilerplate and Consent,* 17 GREEN BAG 2d 293, 301–05 (2014).

things," reflects this ethos.[96] Companies like Facebook and Google are proud of their "hacker culture,"[97] their willingness to take risks and fail,[98] and their desire to challenge the status quo. In this business environment, many associate risk-taking with innovation, and deliberateness and prudence are associated with stagnation and *true* failure. In a letter to investors before Facebook went public, Mark Zuckerberg wrote:

> Building great things means taking risks. This can be scary and prevents most companies from doing the bold things they should. However, in a world that's changing so quickly, you're guaranteed to fail if you don't take any risks. We have another saying: "The riskiest thing is to take no risks." We encourage everyone to make bold decisions, even if that means being wrong some of the time.[99]

Not surprisingly, these risk-taking, fast-moving young companies are eager to deploy new technologies that are not only novel, but also raise ethical, moral, or legal concerns.[100] Courts and legislatures, responsive by nature, are several steps behind, leaving businesses to operate in a legal gap without the benefit of case precedent or legislation to guide them. Operating in unchartered territory, Internet giants seek to minimize the risk to themselves of their risky behavior both by containing their liability through contract and by cultivating favorable public opinion.

In the gap created where technology moves ahead of the law, there are uncertainties regarding whether certain practices infringe upon the rights of others. Data-collection practices are the most glaring example. Businesses can use contracts to operate in this legal gap. Contracts permit companies to allocate unallocated rights and otherwise minimize their legal exposure. As discussed in Part II.A., however, it is doubtful that users actually consent to the data collection practices of these companies.

---

96. *See Mark Zuckerberg's Letter to Investors: 'The Hacker Way'*, WIRED (Feb. 1, 2012, 6:35 PM) http://www.wired.com/2012/02/zuck-letter/.

97. Mark Zuckerberg, the CEO and founder of Facebook, described the company as having cultivated a culture and management approach that he referred to as the "Hacker Way." *Id*. He described hacking as "building something quickly or testing the boundaries of what can be done." *Id*.

98. Google's chief social evangelist, Gopi Kallayil, lists as one of Google's rules of innovative culture, the ability to "fail well." Kathy Chin Leong, *Google Reveals Its 9 Principles of Innovation*, FAST CO., http://www.fastcompany.com/3021956/how-to-be-a-success-at-everything/googles-nine-principles-of-innovation (last visited July 3, 2015) ("There should be no stigma attached to failure. If you do not fail often, you are not trying hard enough.").

99. *Mark Zuckerberg's Letter to Investors: 'The Hacker Way'*, *supra* note 96.

100. It is important to point out that innovation is not the exclusive domain of young Internet companies. "Innovate or die" is a slogan that could apply to any business, and we view the association of Internet giants with a special type of bold, entrepreneurial risk taking as another example of the self-interested rhetoric that Internet giants employ to enhance their ability to evade regulation.

To a large extent, Internet giants have been successful at staving off regulation by lobbying for self-regulation,[101] although their efforts have been – unsurprisingly – a failure in protecting consumer privacy.[102] In a report, the Electronic Privacy Information Center, a non-profit research center, warned that "[s]elf-regulatory systems have served to stall Congress while anesthetizing the public to increasingly invasive business practices."[103]

But Internet giants do not merely evade regulation; they seek to own it, and in this way they take on governmental regulatory functions. To illustrate this, we return to the example of Facebook's experimentation on its users. As a general rule, an Institutional Review Board ("IRB") must approve any experimentation involving human subjects.[104] The federal government established IRBs through the 1974 National Research Act, which applies to any research institution that utilizes federal funding.[105] Because Facebook is a private company not reliant on federal assistance, no IRB approved its user study.[106]

---

101. For example, in response to pending "do-not-track" legislation in California, several technology companies, including Google and Facebook, sent a letter warning of dire consequences to Internet commerce and the economy of the state of California. Letter from California business to Alan Lowenthal, Cal. State Senator (Apr. 27, 2011), http://cdn.arstechnica.net/oppositionletter.pdf; *see also* Matthew Lasar, *Google, Facebook: "Do Not Track" Bill a Threat to California Economy*, ARSTECHNICA (May 6, 2011, 11:02 AM), http://arstechnica.com/tech-policy/2011/05/google-facebook-fight-california-do-not-track-law/. The California legislature recently approved a "do-not-track" disclosure law instead. *See* Vindu Goel, *California Urges Websites to Disclose Online Tracking,* N.Y. TIMES (May 21, 2014), http://bits.blogs.nytimes.com/2014/05/21/california-urges-websites-to-disclose-online-tracking/?_php=true&_type=blogs&_r=0.

102. *See* Chris Jay Hoofnagle, *Privacy Self Regulation: A Decade of Disappointment*, ELEC. PRIVACY INFO. CTR. (Mar. 4, 2005), https://epic.org/reports/ decadedisappoint.html (finding that technologies have become more intrusive and that the FTC should abandon its faith in self-regulation).

103. *Id.* at 15.

104. *See* National Research Act, Pub. L. No. 93-348, 88 Stat. 342, § 474(a) (1974) (calling for the establishment of IRBs "to review biomedical and behavioral research involving human subjects . . . in order to protect the rights of the human subjects of such research").

105. *See id*. (making the Act applicable only to institutions that seek a grant or contract from the federal government).

106. *Compare* Adrienne LaFrance*, Even the Editor of Facebook's Mood Study Thought It Was Creepy*, THE ATL. (June 28, 2014), http://www.theatlantic.com/technology/archive/2014/06/even-the-editor-of-facebooks-mood-study-thought-it-was-creepy/373649/ (suggesting that Cornell University had "pre-approved" the study because it was based on a pre-existing database), *with* Gail Sullivan, *Cornell Ethics Board Did Not Pre-Approve Facebook Mood Manipulation Study*, WASH. POST (July 1, 2014), http://www.washingtonpost.com/news/morning-mix/wp/2014/07/01/facebooks-emotional-manipulation-study-was-even-worse-than-you-thought/ (citing a Cornell statement that Cornell had not thought IRB review was required and thus did not review the Facebook study).

In undertaking its mood experiment, Facebook collaborated with two communications and information scientists at Cornell University.[107] Cornell decided that because the work of its researchers involved only data analysis and no actual interaction with human subjects, IRB review was not necessary.[108] The result was a public relations disaster for Facebook and, according to *The New York Times*, for the Cornell researchers, who were accused of engaging in "mind control."[109]

One might think that the solution ought to be some sort of government-mandated regulation, but as they have in the area of privacy, Facebook and other industry giants aim to "self-regulate," thereby co-opting the regulatory function.[110] They seek to establish the terms under which they will continue to experiment on their customers, resisting an outside ethical review process that they believe would impede their ability to innovate.[111] Cornell's Professor Jeffrey Hancock has said that he and the others involved in the Facebook emotions experiment "didn't realize that manipulating the news feed, even modestly, would make some people feel violated."[112] His response is undoubtedly sincere. Yet, this failure to anticipate the reactions of Facebook's users is a compelling reason to have unaffiliated third parties, with expertise in ethics, involved in the review process.

B. Rights Deletion with a Click

Internet giants use wrap contracts to reorder or delete rights otherwise available to consumers. These rights may include substantive limitations on remedial rights, or they may involve procedural mechanisms, such as class action waivers, that render contractual remedies, and even statutory remedial schemes, unobtainable. They also include the deletion of other rights, such as

---

107. *See* Vindu Goel, *As Data Overflows Online, Researchers Grapple with Ethics*, N.Y. TIMES (Aug. 12, 2014) [hereinafter Goel, *As Data Overflows Online*], http://www.nytimes.com/2014/08/13/technology/the-boon-of-online-data-puts-social-science-in-a-quandary.html?ref=technology&_r=1 (stating that the Facebook emotion experiment was "designed and analyzed with help from Professor Hancock and another academic researcher, Jamie E. Guillory").

108. Sullivan, *supra* note 106 ("Cornell University's Institutional Review Board concluded that [Cornell researchers were] not directly engaged in human research and that no review by the Cornell Human Research Protection Program was required.").

109. *See* Goel, *As Data Overflows Online*, *supra* note 107 (quoting from one of the "hundreds of anguished and angry e-mails" Professor Hancock received).

110. *See id.* (describing the efforts of academics, such as Professor Hancock, and corporate entities, such as Microsoft Research, to develop their own ethical guidelines).

111. *See id.* (paraphrasing Professor Hancock as expressing the view that "[c]ompanies won't willingly participate in anything that limits their ability to innovate quickly").

112. *Id*.

speech, privacy, and intellectual property rights unrelated to a business's potential liability.

As Margaret Jane Radin has explained, businesses use form contracts to overrule legislation specifically designed to protect parties to form contracts, including consumers, small businesses, and employees.[113] Not all form contracts are alike.[114] Form contracting reduces transaction costs.[115] It can be useful for frequently repeated transactions or for repeat players who are familiar with the standard terms and who possess relatively equal bargaining power.[116] Such parties are always free to begin with a standard form agreement and to subject the form to revision through negotiation. Even where standard form agreements are not subject to revision, they are acceptable if they contain terms reasonable to both parties.

But in this Part, we are focused on the spectrum of contracts that Margaret Jane Radin calls "World B" contracts – that is, adhesive form contracts that courts may well enforce even though consumers have never given meaningful consent to their terms.[117] Radin contrasts World B contracts with "World A contracts that involve actual agreement on salient terms."[118] Radin has coined the term "mass-market boilerplate rights-deletion schemes" to describe the use of boilerplate contract language to divest recipients of their rights.[119]

1. Limiting Remedies and the Role of the Judiciary Through Boilerplate

Boilerplate documents protect their creators against liability. This is so even though the rights deleted in boilerplate agreements have been enacted

113. *See* RADIN, *supra* note 85, at 16 (introducing the concept of "democratic degradation," whereby contracts "delete rights that are granted through the democratic process" and substitute a system imposed by the business that drafts the form contract).

114. *See id*. at 33 (recognizing the distinction between standard form contracts and "mass-market boilerplate rights deletion schemes"). Even within boilerplate contracts, Radin provides a useful typology, including standardized adhesion contracts, offsite terms, shrink-wrap licenses, and rolling contracts. *Id*. at 10–11. *See also* KIM, *supra* note 27, at 53–62 (noting that while wrap contracts have a lot in common with other contracts of adhesion, their form raises peculiar difficulties).

115. *See, e.g.*, Nw. Nat'l Ins. Co. v. Donovan, 916 F.2d 372, 377 (7th Cir. 1990) (noting that form contracts reduce transactions costs); KIM, *supra* note 27, at 27 (noting that courts often uphold form contracts, even in the absence of clear indicia of assent because they regard form contracts as efficient and as facilitating transactions).

116. *See* Mark Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 465 (2006) (noting that standard form contracts can serve useful purposes in "mass-market, repeat-play settings").

117. *See* RADIN, *supra* note 85, at 8–9 (describing the "purported contracts" of World B).

118. *See id.* at 3.

119. *See id.* at 33.

through democratic political processes that one might think would trump such private legislation.

Theoretically, courts may strike down World B contracts as illusory or unconscionable.[120] That is cold comfort, however, in large part because of what Radin terms "democratic degradation."[121] Numerous legal mechanisms in World B transactions, such as forum selection clauses, arbitration clauses, class action waivers, disclaimers of consequential damages, and limitations of liability prevent such transactions from being subject to effective legal challenges.[122] These characteristics of World B contracts degrade democracy because they permit private actors to dictate contractual terms that undermine regulatory and remedial schemes that are the product of democratic processes. So, for example, the Supreme Court has allowed arbitration provisions, including class action waivers, to trump state legislation that prohibits such waivers with respect to claims arising under state law.[123]

In the recent *Italian Colors* case,[124] the Supreme Court granted American Express's motion to compel arbitration of plaintiffs' antitrust claims – despite the fact that plaintiffs would be unable to pursue their claims in arbitration on a class basis. The expense involved in bringing an antitrust claim effectively deprived plaintiffs of a meaningful remedy because they could not pursue their claims through a class action. As Justice Kagan summarized in her dissent:

> [I]f the arbitration clause is enforceable, Amex has insulated itself from antitrust liability – even if it has in fact violated the law. The monopolist gets to use its monopoly power to insist on a contract effectively depriving its victims of all legal recourse.
>
> And here is the nutshell version of today's opinion, admirably flaunted rather than camouflaged: Too darn bad.[125]

In Justice Kagan's view, the Supreme Court, by ruling in Amex's favor in this case, permits private legislation in the form of non-consensual, World

120. Steven W. Feldman, *Mutual Assent, Normative Degradation, and Mass Market Standard Form Contracts – A Two-Part Critique of Boilerplate: The Fine Print, Vanishing Rights and the Rule of Law (Part I)*, 62 CLEV. ST. L. REV. 373, 425–29 (2014) (reviewing case law on unconscionability and concluding that the doctrine "is frequently an effective tool to ready merchant overreaching on mass market boilerplate agreements").

121. RADIN, *supra* note 85, at 33–51.

122. *See id.* at 33–42 (describing the way in which "copycat boilerplate" effectively eliminates all consumer choice and forces all purchasers to forfeit rights won through democratic process).

123. *See* AT&T Mobility LLC v. Concepcion, 131 S. Ct. 1740 (2011).

124. Am. Express Co. v. It. Colors Rest., 133 S. Ct. 2304 (2013).

125. *Id*. at 2313 (Kagan, J., dissenting).

B, mass boilerplate, rights-deletion schemes, to trump federal antitrust legislation.

Similarly, Internet giants use contracts to insulate themselves from legal claims that derive from consumer protection legislation that was often decades in the making. Untold hours of toil in the realm of public policy advocacy are undone with the stroke of a pen, or more likely, with a reflexive and unreflective click on an "I agree" icon.

2. Deleting Rights Through Opaque Bargains and Monopoly Power

The previous Part explained how Internet giants use wrap contracts to delete consumers' rights to redress grievances. Businesses use these provisions to limit their potential liability and assess their risk exposure. There are other provisions, however, that have nothing to do with limiting a business's liability. Instead, these provisions claim rights in a way that lacks transparency and may substantially alter or diminish the value of the bargain for the consumer.[126] A company may, for example, use non-disparagement clauses to limit the user's right to speak.[127]

The distributive reach of Internet giants and the private nature of the Internet mean that business decisions made by them may have an indirect effect on basic social, economic, and even civil rights. Facebook, for example, dominates the marketplace in the area of social networking. Given the way social networks operate, being banished from Facebook means being shut out of the biggest online community in the world. Google is the dominant search engine, which means that its decision to remove content or even change its algorithm affects one's ability to attract readers to the content one displays on

126. Nancy Kim has referred to this type of provision as a "crook" provision elsewhere. *See* KIM, *supra* note 27, at 44–52.

127. One reportedly threatened to charge a $250 penalty if a customer even threatened to complain or seek a credit card chargeback. Chris Morran, *Online Retailer Will Fine You $250 if You Even Threaten to Complain About Purchase,* CONSUMERIST (Aug. 27, 2014), http://consumerist.com/2014/08/27/online-retailer-will-fine-you-250-if-you-even-threaten-to-complain-about-purchase/. This apparently was no empty threat. *Id.* One consumer sued the company, Accessory Outlet, after it charged her the $250 penalty. *Id.* She requested a chargeback from her credit card company for a product that she claimed was not shipped. *Id.* Accessory Outlet allegedly told her that the claim would be sent to a collections agency where it would "put a negative mark" on her credit and result in "calls to your home and or/work." *Id.* She alleged that the company also threatened that she would be charged for additional fees for any correspondence that the company had with plaintiff's card issuer. *Id.* The California legislature recently passed a law prohibiting non-disparagement clauses in consumer contracts. CAL. CIVIL CODE § 1670.8 (West 2015) (effective Jan. 1, 2015).

a website.[128] As a practical matter, the content might as well not be there if it cannot be found through Google's search function.

The business practices of Internet giants set online standards, restrict or delete consumers' rights, establish business norms, and dictate behavior that shapes and affects the lives of citizens. As the next Part explains, the power of Internet giants to control society is, in some ways, even greater than that of the government.

C. Governmental Power Without Accountability

Despite the enormous power wielded by Internet giants, their status as private actors frees them from the constraints that limit state actors. While Snowden's disclosures prompted a fierce public outcry that continues to reverberate, the outcry was directed primarily at the government.[129]

For example, David Schneier begins his book, *Data and Goliath*, by noting that one might consider the typical cell phone contract as an implicit bargain. The user gets to make and receive calls; in return, the company knows where the user is at all times.[130] Schneier concedes that one might consider this a good deal, even though the surveillance by private companies is extensive. It is only when Schneier links private surveillance to government surveillance that he introduces terms like "intimidation," "social control," "Orwellian," and "totalitarian."[131]

However, unlike private actors, the government's power is constrained by the Constitution and the balance of powers. For example, the U.S. Court of Appeals for the Second Circuit recently held that a provision of the USA Patriot Act, allowing the systematic collection of phone records in bulk, is illegal because it exceeds the scope of Congress's power.[132] This Part discusses how private entities have *more* power in certain ways than the government to limit citizens' speech, arbitrarily deprive citizens of property, and subject citizens to unreasonable searches and seizures.

---

128. *See generally* Allyson Haynes Stuart, *Google Search Results: Buried If Not Forgotten* (Oct. 21, 2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2343398.

129. *See, e.g.*, Editorial, *President Obama's Dragnet*, N.Y. TIMES (June 6, 2013), http://www.nytimes.com/2013/06/07/opinion/president-obamas-dragnet.html?ref=opinion&_r=0 (claiming that the Obama administration was abusing its power and had lost all credibility when it came to transparency and accountability); Editorial, *Massive Secret Surveillance Betrays Americans: Our View*, USA TODAY (June 6, 2013), http://www.usatoday.com/story/opinion/2013/06/06/nsa-phone-records-verizon-internet-editorials-debates/2398819/ (calling NSA surveillance outrageous).

130. SCHNEIER, *supra* note 9, at 1.

131. *Id.* at 2.

132. ACLU v. Clapper, No. 14-42-CV, 2015 WL 2097814, at 1* (2d Cir. May 7, 2015).

1. Speech Restrictions and the Private Regulatory Nature of the Internet

The government may not pass laws abridging the freedom of speech.[133] Private companies, however, may enter into contracts where individuals agree to limit their ability to speak freely. Courts routinely uphold non-disclosure and non-disparagement clauses in employment, confidentiality, and other negotiated agreements. Speech-restricting clauses in non-negotiated agreements, however, raise serious questions of consent and fairness. As discussed in Part II.A., courts have routinely upheld wrap contracting forms under theories of constructive assent and constructive notice even where users lacked actual notice and failed to actually assent to terms. Courts might refuse to enforce non-disparagement clauses that impose penalties on the grounds of unconscionability. However, they may never have the opportunity to do so given that many wrap contracts containing such provisions also contain binding mandatory arbitration clauses. Thus, it would be left to an arbitrator to determine whether such a clause would be unconscionable. Because arbitration decisions are not part of public record, there would be neither precedent to inform the future behavior of businesses or consumers nor opportunity to appeal decisions, which would essentially erode the common law.[134] Furthermore, most consumers would likely not risk challenging the enforceability of a penalty-imposing non-disparagement clause. Instead, they would likely abide by the clause to avoid legal fees, the imposition of fines, and/or damage to their credit.

Non-disparagement clauses are not the only mechanism by which online companies may restrict users' speech. They can also enforce Codes of Conduct that restrict certain language. While Codes of Conduct are typically used to enforce norms of civility,[135] they may also stifle speech that expresses political views or perspectives that would be constitutionally protected. Internet companies also establish policies that stifle speech. For example, enforcing its "real names" policy, Facebook shut down the accounts of members of the lesbian, gay, bisexual, and transgender community who used

133. U.S. CONST. amend. I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.").

134. *See* RADIN, *supra* note 85, at 134 (contending that firms include mandatory arbitration provisions in their contracts because "arbitration has no precedential value" and "leaves no written public record").

135. The use of Codes of Conduct to enforce civility norms should be condoned. Our concern here is that companies have discretion to regulate speech without oversight. Furthermore, the lack of transparency and the arbitrariness of decisions raise due process concerns. *See* discussion *infra* Part III.C.1.a–b.

pseudonyms for a variety of reasons, including protecting themselves from harassment for their personal expression and political views.[136]

The power of private companies to control speech through the exercise of their proprietorship rights poses serious consequences online because of the private nature of the Internet. As Dawn Nunziato has explained, the "vast majority of speech on the Internet today occurs within private places and spaces that are owned and regulated by private entities."[137] Consequently, as Jack Balkin has noted, censorship "is as likely to come from private entities that control telecommunications networks and online services as from the government."[138]

The constitutional protections afforded by the First Amendment for free speech only apply to state actors.[139] Internet giants establish their own "free speech" rules in their TOS or Acceptance Use Policies. As Marvin Ammuri writes, lawyers who work for the Internet giants "effectively engage in private speech rulemaking, adjudication, and enforcement"[140] when they draft and implement these policies and the procedures to enforce them. The lawmaking power of lawyers and others who institute and implement the content policies at the Internet giants' direction has prompted Jeffrey Rosen to comment that these individuals wield "more power . . . than any president or judge."[141]

---

136. James Nichols, *Facebook "Name Change" Policy Disproportionately Affecting LGBT Community*, HUFFINGTON POST (Sept. 15, 2014), http://www.huffingtonpost.com/2014/09/15/facebook-name-change_n_5824836.html; Valeriya Safronova, *Drag Performers Fight Facebook's "Real Name" Policy*, N.Y. TIMES (Sept. 24, 2014), http://www.nytimes.com/2014/09/25/fashion/drag-performers-fight-facebooks-real-name-policy.html?_r=0.

137. Dawn C. Nunziato, *The Death of the Public Forum in Cyberspace*, 20 BERKELEY TECH. L.J. 1115 passim (2005).

138. Jack M. Balkin, *The Future of Free Expression in a Digital Age,* 36 PEPP. L. REV. 427, 437 (2009). *See also* Stuart, *supra* note 128, at 30 ("Many have accused Google of hand-editing its own search results in order to punish behavior it views as violating its Terms of Service.").

139. Balkin, *supra* note 138, at 429. *See also* Marjorie Heins, *The Brave New World of Social Media Censorship,* 127 HARV. L. REV. F. 325, 326 (2014) (noting that most of what Facebook proscribes in its Statement of Rights and Responsibilities is protected by the First Amendment and its internal appeals process is "mysterious at best").

140. Marvin Ammori, *The "New" New York Times: Free Speech Lawyering in the Age of Google and Twitter*, 127 HARV. L. REV. 2259, 2273 (2014).

141. Jeffrey Rosen, *The Delete Squad: Google, Twitter, Facebook and the New Global Battle Over the Future of Free Speech,* NEW REP. (Apr. 29, 2013), http://www.newrepublic.com/article/113045/free-speech-internet-silicon-valley-making-rules. Rosen refers to these individuals as the "Deciders." *Id.* He writes that "[a]s corporate rather than government actors, the Deciders aren't formally bound by the First Amendment." *Id*. Marvin Ammori notes that "some of the most important First Amendment lawyering today is happening at top technology companies." Ammori, *supra* note 140, at 2262.

a. How Section 230 of the CDA Diminishes Users' Ability to Control Speech

The ability of private companies to impose greater restrictions on speech than state actors may be beneficial in establishing and enforcing civil behavior. Yet, websites are not required to enforce any civility norms at all. On the contrary, under judicial interpretation of Section 230 of the CDA, websites are expressly protected from liability for content posted by third parties. Section 230 provides the Internet giants with blanket immunity from civil liability for any choice they may make about the regulation or non-regulation of speech on multi-sided platforms, or what the CDA terms "interactive computer services."[142] Section 230 provides:

> (c) Protection for "Good Samaritan" blocking and screening of offensive material
>
> (1) Treatment of publisher or speaker
>
> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
>
> (2) Civil liability
>
> No provider or user of an interactive computer service shall be held liable on account of –
>
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical

142. The CDA defines "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. § 230(f)(2) (2012). The term has been interpreted broadly to include all websites and online services. *See generally* Joel R. Reidenberg et al., *Section 230 of the Communications Decency Act: A Survey of the Legal Literature and Reform Proposals* 2, FORDHAM CTR. ON L. & INFO. POL'Y AT FORDHAM LAW SCH. (Apr. 25, 2012), http://law.fordham.edu/assets/CLIP/Fordham_CLIP_CDA_230_Report_4-25-12.pdf.

> means to restrict access to material described in paragraph (1).[143]

Other provisions of the CDA make clear that the immunity covers claims that might be made against Internet giants or other providers of interactive services under state or local laws.[144]

The power to control users' speech and the freedom from responsibility for such speech puts users in a precarious situation with respect to liability for what they say online. The Internet has spawned a norm of impulsivity where users post without carefully considering the consequences. A user may post a false or defamatory comment or review while in an emotionally-inflamed state. Because the poster is often anonymous, the subject of a harmful or false post often has no recourse but to appeal to the website to remove it. A website, however, has no obligation to remove such a posting, even if the poster himself requests its removal. Due to Section 230 immunity, the website may have no incentive to remove even defamatory content. The poster, however, is not immune from liability.[145] As a result, the website is in the mighty position of having the power to control the continued publication of the speech without having any of the responsibility for it.

b. Speech Restrictions and Non-Disparagement Clauses

Even users posting truthful or non-defamatory content may wish to remove a negative review. For example, in one case, a couple attempted to have their negative review removed after being threatened by a company that claimed the couple had violated its TOS by doing so.[146] The website where they posted the review, Ripoff Reports, refused to allow them to do so unless the couple first went through the website's arbitration process.[147] The arbitration process, however, would have cost $2000.[148] While one might argue that a website's refusal to remove reviews even upon request of the poster protects truthful reviews from being removed by businesses, it takes the decision out of the hands of the original poster and places it into the hands of the website, which is immune from tort liability for the post. It also creates a moral hazard where the website hosting the post may benefit from a defamatory post. Such a post may increase traffic to the site or, as in the case of Ripoff

143. 47 U.S.C. § 230(c).

144. *See id.* § 230(e)(3) ("No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.").

145. *See* Nancy S. Kim, *Website Design and Liability,* 52 JURIMETRICS 383 (2012) (explaining how courts have interpreted section 230 to provide websites with broad immunity which creates more potential harm for both victims and posters).

146. Pamela Brown, *Couple Fined for Negative Online Review,* CNN (Dec. 26, 2013), http://www.cnn.com/2013/12/02/tech/couple-fined-for-negative-review/index.html.

147. *Id.*

148. *Id.*

Report, the company may be able to force a regretful poster into paying mandatory arbitration fees or other fees as a condition to removing the post.

2. Deprivation of Personal Property Without Due Process

The Constitution protects citizens against the deprivation of property without due process.[149] The government could not deprive citizens of the use of their cars or homes, for example, without due process. Internet giants, however, are freed from any such constitutional constraints. Consumers entrust companies like Yahoo, Facebook, and Google with their private correspondence, photos, music, and contact lists. These companies encourage users to store content to their sites, and users often invest substantial time and energy to cultivate their accounts. Users – and the website themselves – view the content posted by users to be proprietary to the users. Yahoo's TOS, for example, state that "Yahoo does not claim ownership of Content you submit or make available for inclusion on the Yahoo Services," although it does claim a "worldwide, royalty-free and non-exclusive license" to it.[150] Google, too, states that its users "retain ownership of any intellectual property rights" and that "what belongs to you stays yours."[151] Google, however, does take a "worldwide license" to use the content for various purposes.[152] Although Facebook's Statement of Rights and Responsibilities states that users "own all of the content and information you post on Facebook," the company takes a "non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content" posted in connection with Facebook.[153]

All three companies, however, state that they may terminate their services if users fail to comply with terms or policies. Google states that it "may suspend or stop providing Services to you if you do not comply with our terms or policies or if we are investigating suspected misconduct."[154] Yahoo

---

149. U.S. CONST. amend. V (providing that no person shall be "deprived of life, liberty or property, without due process of law; nor shall private property be taken for public use, without just compensation"). The Fourteenth Amendment provides:

> No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

U.S. CONST. amend. XIV § 1.

150. *Yahoo Terms of Service*, YAHOO! (last updated Mar. 16, 2012), https://policies.yahoo.com/us/en/yahoo/terms/utos/index.html (last visited July 19, 2015).

151. *Google Terms of Service*, GOOGLE (last modified April 14, 2014), http://www.google.com/intl/en/policies/terms/ (last visited July 19, 2015).

152. *Id*.

153. *Statement of Rights and Responsibilities*, FACEBOOK (last revised Jan. 30, 2015), https://www.facebook.com/legal/terms (last visited July 19, 2015).

154. *Google Terms of Service*, *supra* note 151.

states that it may "*without prior notice*, immediately terminate, limit your access to or suspend your Yahoo account, any associated email address, and access to your Yahoo Services."[155] The reasons for such termination or limitation of access include "breaches or violations of the TOS or other incorporated agreements or guidelines."[156] Furthermore, Yahoo states that all terminations and suspensions shall be made "in Yahoo's sole discretion[,]" and "Yahoo shall not be liable to you or any third party for any termination of your account, any associated email address, or access to the Yahoo Services."[157] Facebook states that it may terminate users' accounts if they "violate the letter or spirit" of their Statement of Rights or Responsibilities or "otherwise create risk or possible legal exposure" for the company.[158] It will notify users of such termination "by email or at the next time you attempt to access your account."[159]

Users may find themselves locked out of their accounts without prior notice or an opportunity to save their data or notify their contacts. Users depend on the availability of these sites and have integrated their services into their daily lives. They may store important information on their sites, and they may have created strong communities and relationships that are accessible only through these sites.[160] Many users depend on the websites for work-related activities.[161] They view the content they post as their own property. Yet, the companies have the power to banish them without prior notice or due process.

Furthermore, this power is one that Internet giants are not afraid to exercise. While companies should be allowed to terminate or suspend the accounts of users who violate website policies and norms of conduct, the exercise of that power should be subject to some sort of due process or transparent review process. Companies can now suspend or terminate accounts without explanation or prior notice. Users are often confounded and frustrated to find that they are locked out for no apparent reason.[162] Internet companies typically automate customer service and respond to queries via email. Terminated customers typically have no ability to communicate with an actual customer service representative, and efforts to resolve the problem may take weeks, even for those users who are eventually reinstated. The company may

155. *Yahoo Terms of Service*, *supra* note 150.

156. *Id.*

157. *Id.*

158. *Statement of Rights and Responsibilities*, *supra* note 153.

159. *Id.*

160. Alina Tugend, *Barred from Facebook, and Wondering Why*, N.Y. TIMES (Sept. 19, 2014), http://www.nytimes.com/2014/09/20/your-money/kicked-off-facebook-and-wondering-why.html?recp=19&_r=0.

161. *Id.*

162. *Id.*

provide no explanation as to why the account was suspended in the first place.[163]

Internet giants also effectively deprive users of due process by using forum selection clauses. For example, Google's TOS state that all claims relating to the use of its service "will be litigated exclusively in the federal or state courts of Santa Clara County, California, USA, and you and Google consent to personal jurisdiction in those courts."[164] A non-California resident wishing to sue Google would have to file a lawsuit in California and hire a California-based attorney. A typical Google user would not be able to expend the resources to do this and would essentially have no recourse against Google.[165] Some Internet giants impose mandatory arbitration clauses upon their users. Microsoft's service agreement, for example, states that other than small claims disputes, users must submit to "individual binding arbitration;" "class arbitrations aren't permitted," and users are "giving up the right to litigate disputes in court before a judge or jury."[166]

3. Email Scanning and Other Unreasonable Searches and Seizures

Google, Yahoo, Facebook, and Microsoft all reserve the right to scan or analyze user content. Google's TOS state that its "automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising and spam and malware detection. This analysis occurs as the content is sent, received,

---

163. *See id.* One user's account was disabled for a month for reasons that were found to be unfounded. *Id.*

164. *Google Terms of Service*, *supra* note 151.

165. Surprisingly, the terms of use of some of the most popular Internet giants (Google, Facebook, Yahoo, and Twitter) do not contain mandatory arbitration clauses that are common on many other websites. *See Google Terms of Service*, *supra* note 151; *Statement of Rights and Responsibilities*, *supra* note 153; *Yahoo Terms of Service*, *supra* note 150; *Twitter Terms of Service*, TWITTER (effective May 18, 2015), https://twitter.com/tos?lang=en (last visited Sept. 24, 2015). This may have more to do with California state law than any policy decision on the part of these companies as all of these companies are located in California and their terms of use specify California as the governing law. *Yahoo Terms of Service*, *supra* note 150; *Google Terms of Service*, *supra* note 151; *Statement of Rights and Responsibilities*, *supra* note 153. On other hand, Microsoft, which has a mandatory arbitration clause, is based in Washington and adopts Washington as the governing law. *Arbitration and Dispute Resolution*, MICROSOFT (last updated Nov. 20, 2014), https://www.microsoft.com/en-us/Legal/arbitration/default.aspx (last visited July 19, 2015). The authors suspect that given recent U.S. Supreme Court decisions striking down California's laws limiting arbitration, the Internet giants based in California may soon change their Terms of Use to impose mandatory arbitration. *See, e.g.*, AT&T Mobility v. Concepcion, 131 S. Ct. 1740 (2011).

166. *Microsoft Services Agreement*, MICROSOFT (last updated June 11, 2014), http://windows.microsoft.com/en-us/windows/microsoft-services-agreement (last visited July 19, 2015).

and when it is stored."[167] Yahoo's TOS state that, "Yahoo may or may not pre-screen Content," and Yahoo:

> [M]ay access, preserve and disclose your account information and Content if required to do so by law or in a good faith belief that such access preservation or disclosure is reasonably necessary to (i) comply with legal process; (ii) enforce the TOS; (iii) respond to claims that any Content violates the rights of third parties; (iv) respond to your requests for customer service; or (v) protect the rights, property or personal safety of Yahoo, its users and the public.[168]

Facebook's Statement of Rights and Responsibilities states that the company can "analyze your application, content, and data for any purpose, including commercial (such as for targeting the delivery of advertisements and indexing content for search)."[169] Microsoft Outlook's TOS state that Microsoft has the "world right, without charge, to use Content as necessary: to provide the Services to you, to protect you, and to improve Microsoft products and services."[170] Microsoft's Privacy Statement reveals that the company may:

> [U]se automated means to isolate information from email, chats, or photos in order to help detect and protect against spam and malware and to improve the services with new features that make them easier to use. We may also access and use your information and content when we are alerted to violations of the Microsoft Services Agreement.[171]

Some may argue that data collection by private entities is not as threatening because they are only trying to sell things to us. Unlike the government, private companies do not have police power. Accordingly, their ability to "punish" us based upon information they collect about us is limited to their property or contractual rights. They may be able to terminate our ability to access our accounts, but they cannot throw us in jail based upon what they find out about us through data mining.

Yet, Internet giants may also act as agents for or on behalf of governmental entities engaging in what Jack Balkin refers to as "public/private cooperation or co-optation."[172] As Snowden's disclosures revealed, the infor-

---

167. *Google Terms of Service*, *supra* note 151.

168. *Yahoo Terms of Service*, *supra* note 150.

169. *Facebook Platform Policy*, FACEBOOK (last updated March 25, 2015), https://developers.facebook.com/policy (last visited July 19, 2015).

170. *Microsoft Services Agreement*, *supra* note 166.

171. *Microsoft Privacy Statement*, MICROSOFT (last updated July 2015), https://www.microsoft.com/en-us/privacystatement/ (last visited July 19, 2015).

172. *See* Jack M. Balkin, *Old School/New School Speech Regulation,* 127 HARV. L. REV. 2296, 2298–99 (2014). Balkin states:

mation collected as part of these companies' efforts to monetize our data could be summoned by, and released to, the government. While the relationship between technology companies and the federal government may not be as cozy as it once was in the aftermath of Snowden's revelations,[173] we expect the cooperative relationship to continue. As David Schneier has noted, corporate and government surveillance are intertwined and support one another in a public private surveillance partnership.[174] Most companies' TOS expressly state that user information may be shared with law enforcement or governmental authorities.[175]

Furthermore, data collection by private entities may affect whether someone has a reasonable expectation of privacy worthy of Fourth Amend-

---

> To the extent that the government does not own the infrastructure of free expression, it needs to coerce or co-opt private owners to assist in speech regulation and surveillance—to help the state identify speakers and sites that the government seeks to watch, regulate, or shut down. To this end, the government may offer a combination of carrots and sticks, including legal immunity for assisting the government's efforts at surveillance and control. Owners of private infrastructure, hoping to reduce legal uncertainty and to ensure an uncomplicated business environment, often have incentives to be helpful even without direct government threats.

Id.

173. *See* Devlin Barrett, Danny Yadron & Daisuke Wakabayashi, *Apple and Others Encrypt Phones, Fueling Government Standoff*, WALL ST. J. (Nov. 18, 2014) http://www.wsj.com/articles/apple-and-others-encrypt-phones-fueling-government-standoff-1416367801 ("Technology companies are pushing back more against government requests for cooperation and beefing up their use of encryption" post-Snowden.).

174. SCHNEIER, *supra* note 9, at 78.

175. *See, e.g.*, *Privacy Policy*, GOOGLE (last modified June 30, 2015), http://www.google.com/intl/en/policies/privacy/ (last visited July 19, 2015) ("We will share personal information . . . to protect against harm . . . as required or permitted by law."). *See also Data Policy*, FACEBOOK (last revised Jan. 30, 2015), https://www.facebook.com/about/privacy/other ("We may . . . share your information in response to a legal request. . . . We may also . . . share information when . . . necessary to detect, prevent and address fraud and other illegal activity."). Facebook's Privacy Policy also states that it will "use the information we collect" to "prevent potentially illegal activities, and to enforce our Statement of Rights and Responsibilities." *Id. See also* Yahoo's Terms of Service, which state:

> Yahoo may access, preserve and disclose your account information and Content if required to do so by law or in a good faith belief that such . . . disclosure is reasonably necessary to (i) comply with legal process; (ii) enforce the TOS; (iii) respond to claims that any Content violates the rights of third parties; (iv) respond to your requests for customer services; or (v) protect the rights, property or personal safety of Yahoo, its users and the public.

Yahoo Terms of Service, *supra* note 150.

ment protection.[176] Under the third-party doctrine, the Supreme Court has stated that a criminal defendant has no legitimate expectation of privacy in information voluntarily conveyed to third parties.[177] The Supreme Court's reasoning in that case was based on a distinction between the collection of metadata and the collection of content.[178] That distinction now seems to be increasingly illusory.[179] As a result, expansive data collecting conducted by Internet giants erodes the constitutional rights of citizens who seek to protect themselves from governmental searches.[180]

Internet giants' TOS allow them to police their own sites to prevent illegal activity, not simply respond to governmental requests. Because they are not constrained by constitutional limitations, and because their TOS allow them to search their users' accounts, they have an unprecedented ability to ferret out potentially incriminating information. For example, Google alerted Texas police to information that led to the arrest of a child pornography suspect.[181] Unlike police, who are prohibited from going on a fishing expedition, Google regularly scans users' emails, purportedly in order to furnish users with personalized advertisements. Microsoft, too, recently discovered child pornographic images in the course of scanning its users' accounts.[182]

176. *See* Smith v. Maryland, 442 U.S. 735, 742–46 (1979) (finding that defendant had no legitimate expectation of privacy in phone numbers he dialed because he knew that phone numbers were conveyed to telephone company which records the information).

177. *Id*. at 743–44. For example, the Supreme Court noted that a criminal defendant had no legitimate expectation of privacy in financial information voluntarily conveyed to banks. *Id*. at 744. *See also* Note, *Data Mining, Dog Sniffs, and the Fourth Amendment,* 128 HARV. L. REV. 691, 697–98 (2014) (discussing *Smith v. Maryland* and concluding that, with some exceptions, "the Fourth Amendment leaves unprotected any information that has fallen or could legally fall into the hands of a private third party").

178. *Smith*, 442 U.S. at 742 (finding that no "search" had occurred for Fourth Amendment purposes when the telephone company installed a pen register to record the numbers petitioner had dialed because citizens have no reasonable expectation of privacy with respect to such information).

179. *See* SCHNEIER, *supra* note 9, at 20–23 (illustrating the ease with which one can deduce content from metadata); ACLU v. Clapper, 959 F. Supp. 2d 724, 748 (S.D.N.Y. 2013) (describing how telephony metadata, and especially aggregated metadata, can reveal content), *vacated and remanded*, No. 14-42-CV, 2015 WL 2097814 (2d Cir. May 7, 2015).

180. At the same time, government access to big data is also eroding constitutional limitations. *See* Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 331–32 (2015) (predicting that "big data policing" may render the reasonable suspicion requirement "practically irrelevant").

181. Alroy Menezes, *Google Helps Law Enforcement Crack Down on Child Pornography, Defends Policy,* INT'L BUS. TIMES (Aug. 5, 2014), http://www.ibtimes.com/google-helps-law-enforcement-crack-down-child-pornography-defends-policy-1648858.

182. Leo Kelion, *Microsoft Tip Leads to Child Porn Arrest in Pennsylvania*, BBC NEWS (Aug. 6, 2014), http://www.bbc.com/news/technology-28682686.

Because these are private companies, they are not subject to the constitutional requirement of a warrant.[183] While there is undoubtedly little sympathy for a child pornographer, Microsoft's and Google's ability to engage in what would amount to an unlawful search and seizure if conducted by a governmental entity raises disconcerting questions about civil liberty protections in a society where Internet giants have all the power of governmental entities but are subject to none of the constitutional limitations.

Elected officials pledge to act in the public interest, and if they fail to do so, their constituents may vote them out of office. In sharp contrast, Internet companies have none of these constraints. Internet giants operate their online properties like fiefdoms with the power to manipulate and control users' online activities. They use wrap contracts to obtain more rights while minimizing their liabilities. Unlike the government, the Internet giants have no mandate to act in the public interest. On the contrary, they are accountable primarily to their shareholders, and their corporate objective is the maximization of shareholder profit. Yet Internet giants – not the government – regulate and shape the online world with unprecedented control over what the public does, reads, and thinks. They are the ones – not the government – with the unprecedented broad discretion and power to rifle through our virtual papers and track our online movements in an attempt to profit off of our contacts, behaviors, and habits. Furthermore, unlike the government, private companies, in their interactions with consumers, are not limited by constitutional protections – and consumers have no right to trial. The Codes of Conduct are governance systems, but they are implemented through the "legislation" of TOS. These TOS establish the rules that govern each site.

D. The Best of Both Worlds: Corporations as Quasi-Governmental Agencies and as Empowered Citizens

We have described how Internet giants use wrap contracts and a constructed notion of consent to become private regulators and private legislators whose rules trump those arrived at through democratic processes. Today, the world inhabited by Internet giants is a grand one. They enjoy the benefits of regulatory power akin to that of a government agency, and in certain respects, their power exceeds that of legislatures. Yet, they still enjoy the rights of personhood, perhaps to an unprecedented degree due to recent decisions of the Supreme Court – decisions that extend First Amendment protections to

183. *See* Avidan Cover, *Corporate Avatars and the Erosion of the Populist Fourth* Amendment, 100 IOWA L. REV. (2015) (describing the third-party doctrine as enabling corporations as avatars that are supposed to protect individual privacy interests but cannot because powerful tech companies function almost like mini-states with "vested interests in cooperating with the government"); Jane Bambauer, *The Lost Nuance of Big Data Policing*, 94 TEX. L. REV. (forthcoming 2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2572448 (advocating reforms of the third-party doctrine that would eliminate data collection practices that compromise civil liberties while permitting liberty-enhancing innovations in policing).

corporate persons[184] and recognize their personhood for the purpose of the free exercise of religion under the Religious Freedom Restoration Act.[185] Our point here is not to criticize these decisions, but to point out that it is peculiar to grant corporate entities the freedoms that natural persons enjoy while they exercise powers and enjoy immunities akin to those of the government, yet without the attendant regulatory accountability or oversight.

The cumulative effect of Internet giants' power of private legislation and the protection afforded them by federal legislation is that Internet giants enjoy broad immunity from any claims that might be brought against them for offensive content on their websites – for example, for libel – and from any claims that might be brought against them for enforcing their governance systems arbitrarily and suppressing users' rights of free expression or free association. They are also immune from liability if their cooperation with the government violates their users' statutory, constitutional, or contractual privacy rights.[186]

III. DOWNGRADING "CONSENT"

Companies claim that users' consent to intrusive uses of their personal data simply because they have clicked on an "accept" icon or continued to use a website after having received constructive notice. Contract law's primary objective is to enforce the reasonable expectations of the parties, yet Internet giants claim contractual consent to justify intrusive uses of personal information that disappoint the reasonable expectations of consumers.

The problem of online privacy is complex because it involves various types of data and a multitude of purposes for which data may be used.[187] Consequently, we believe that there is no "one-size-fits-all" solution to the problems outlined in this Article. A necessary first step, however, is to drastically limit – even eliminate – the role of contractual consent in determining the boundaries of what companies may do with personal information. Internet giants may be private actors, but they function like state entities and exert power over important rights. While private ordering among private actors is a cornerstone of the free market economy, a contract between an Internet

184. Citizens United v. FEC, 558 U.S. 310, 365 (2010) (recognizing the free speech rights of corporate entities).

185. *See* Burwell v. Hobby Lobby Stores, Inc., 134 S. Ct. 2751, 2768–69 (2014) (interpreting the term "person" in the Religious Freedom Restoration Act as protecting the religious liberty interests of for-profit corporations).

186. *See* H.R. 3321, 110th Cong. § 5(a) (2007); Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 50 U.S.C.A § 1881a(h) (West 2015) (immunizing companies from liability for cooperating with the government, even if doing so violates the terms of their agreements with their customers).

187. *See Big Data*, *supra* note 69, at 56 ("The context of data use matters tremendously. Data that is socially beneficial in one scenario can cause significant harm in another.").

giant and a consumer is more reminiscent of coercive state power than bargaining among private parties.

Given the monopolistic power of Internet giants, their fulfillment of traditional governmental functions, the cooperation between Internet giants and the State, and the inapplicability of traditional controls on government abuse, contracts between Internet giants and consumers should be viewed as unilaterally imposed private legislation, not as bargains. Furthermore, unlike adhesive contracts in other contexts, the quasi-governmental role of Internet giants means that the subject matter of these so-called contracts often involves important civil and political rights, not simply the maximization of economic profit or the furtherance of commercial interests. Given the absence of the traditional commercial justifications that courts have used to avoid reviewing the adequacy of bargains, courts should not hesitate to evaluate for fairness the terms of purported "contracts" between Internet giants and consumers.

Legislators, governmental agencies, and policymakers, too, should be careful not to inadvertently define consent in the realm of privacy to be satisfied through the anemic form of consent associated with form contracting. On the contrary, they should take pains to delegitimize consent obtained through blanket assent to contract terms. The use of personal information by companies should be permitted only in those instances where consent was specific, express, and voluntary.

"Specific" refers to each particular use of the data. "Express" means affirmative – an opt-in, rather than an opt-out.[188] "Voluntary" requires the availability of reasonable options, which is particularly important where the drafting party is an Internet giant that dominates a particular online activity. One click should not be construed to signify blanket assent to all terms contained in a wrap contract. Companies compete based upon the quality of the services offered; they do not compete on the basis of unread wrap contract terms. A requirement of specific assent raises the salience of wrap contracts by encumbering and affecting the quality of the customer experience, which may make the consent process itself a competitive advantage or disadvantage. Making the consent process reflect the bargain itself increases transparency, which may, in turn, encourage companies to reconsider their data-collection practices. As long as those data-collection practices remain obscure, there is little incentive for companies to restrain themselves or restrict their use of data.

Non-consent should not mean that consumers are barred from participating in a service over which an Internet giant holds a de facto monopoly, nor should non-consent prevent such consumers from continuing to participate in a service in which they have vested interests and where there are likely to be sunk and switching costs. Context matters, and permission to use data grant-

188. Other scholars have championed a specific assent approach. *See* James Gibson, *Vertical Boilerplate,* 70 WASH. & LEE L. REV. 161, 185–86 (2013); Russell Korobkin, *The Borat Problem in Negotiation: Fraud, Assent, and the Behavioral Law and Economics of Standard Form Contracts*, 101 CAL. L. REV. 51, 56 (2013).

ed in one context should not automatically transfer to other contexts.[189] Businesses could continue to use consumer personal information to provide services under a quasi-contract theory, but the use of data for purposes other than to provide services, at a minimum, should be subject to more onerous consent requirements.

Furthermore, given the dominance of Internet giants in the online environment, legislators, governmental agencies, and policymakers should move away from consent – blanket or specific – altogether as a mechanism for establishing the boundaries of data collection and use. Currently, the law requires notice and choice, an approach Daniel Solove refers to as "privacy self-management."[190] Solove writes:

> Privacy self-management takes refuge in consent. It attempts to be neutral about substance – whether certain forms of collecting, using or disclosing personal data are good or bad – and instead focuses on whether people consent to various privacy practices. Consent legitimizes nearly any form of collection, use, or disclosure of personal data.[191]

Solove argues that privacy self-management fails to provide people with meaningful control over their data.[192] He makes several proposals to address the shortcomings of privacy self-management, including a "coherent approach to consent" that takes into account "social science discoveries about how people make decisions about personal data," and developing "more substantive privacy rules," including those that focus on downstream uses of data.[193] His views align with a White House commissioned report that recommended moving away from "notice and choice" – the dominant regulatory framework – and toward a "responsible use" framework that would hold data collectors and users accountable for the ways that they manage and use data.[194]

We agree that "notice and consent" imposes too heavy a burden upon consumers to read, understand, and, in some cases, object to uses of data. The government should take a more proactive role in regulating uses of personal information, a view with which most Americans may agree. A recent study found that 64% of those surveyed believe that the government should

189. *Big Data*, *supra* note 69, at 56 ("[M]ore attention on responsible use does not mean ignoring the context of collection. Part of using data responsibly could mean respecting the circumstances of its original collection.").

190. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma,* 126 HARV. L. REV. 1879 (2013).

191. *Id.* at 1880.

192. *Id.* at 1903.

193. *Id.*

194. *Big Data, supra* note 69, at 56.

do more to regulate advertisers.[195] Different procedures must be in place depending upon the type of data involved and the use of that data.[196]

Furthermore, as we have explained, Internet giants like Facebook and Google occupy a *sui generis* role in our society, controlling basic rights of citizens with little regulatory oversight. Given the tremendous power of Internet giants over online activity, the primary framework for protecting privacy should not depend upon consent. To eliminate "consent" as the mechanism by which data practices are sanctioned acknowledges that, in the online contracting context, consent is fictive. Consumers have very little bargaining power vis-à-vis Internet giants that control online services and establish business practices that affect fundamental online freedoms with little regulatory oversight. Clicking "Agree" may mean only that the consumer has no other option if she wants to participate in the modern world.[197] Given the reality of contractual consent and its fictive nature, private ordering should not be the process by which businesses establish – and courts and regulators permit – data-collection practices.

Instead, legislators and policymakers must do the hard work of determining responsible business practices and establishing regulations that protect the reasonable expectations of the individual in the use of personal information.[198] We need public laws that eliminate, or at least curtail, the use of so-called contracts, which are not based on consent, and of the artificial and diluted version of consent sanctioned by contract law. A bedrock of contract law is to enforce the reasonable expectations of the parties, and the current regime of enforcing boilerplate contracts, quite perversely, fails to do so.

---

195. Madden, *supra* note 61, at 30.

196. For example, in a recent survey, most Americans said they felt social security numbers, health information, and the content of phone conversations was "very sensitive" or "somewhat sensitive." *Id.* Only 31% felt the same about the "media you like." *Id*.

197. As Justice Thurgood Marshall noted in his dissenting opinion in *Smith v. Maryland* when discussing an individual's legitimate expectation of privacy:

> Implicit in the concept of assumption of risk is some notion of choice . . . unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance . . . . It is idle to speak of "assuming" risks in contexts where, as a practical matter, individuals have no realistic alternative.

Smith v. Maryland, 442 U.S. 735, 749–50 (1979) (Marshal, J., dissenting). Justice Marshall was referring to the use of the telephone, but today the "personal or professional necessity" applies to service provided by Internet giants that control the online landscape. *See id.*

198. The "reasonable expectations" approach is basically the same as the one mentioned in the White House report as the "'no surprises rule' articulated in the 'respect for context' principle in the Consumer Privacy Bill of Rights." *Big Data*, *supra* note 69.

CONCLUSION

Although the Snowden disclosures have focused the public's attention on the government's intrusive surveillance tactics, the public's concern over private entities' intrusive data collection and use has been comparatively muted. Companies disclose their wide-ranging and intrusive data-collection practices in privacy policies that few individuals read and that are consented to only through judicial fictions. Companies use forms and label them as contracts to justify their spying activities, spinning a tale of consent that courts have been too willing to accept. Internet giants' quasi-governmental authority and *de facto* monopolistic power render their putative agreements with private actors imbalanced and coercive. As state and federal governments consider how to best protect consumer privacy,[199] they should dismiss proposals that lean too heavily on consumer consent to sanction collection practices. Contractual consent – at least in its current diluted and fantastical form – is an invalid mechanism that distorts rather than reflects consumer preferences.

199. President Obama recently called for federal legislation to address online data breaches and student privacy. *See* Michael D. Shear & Natasha Singer, *Obama to Call for Laws Covering Data Hacking and Student Privacy*, N.Y. TIMES (Jan. 11, 2015), http://www.nytimes.com/2015/01/12/us/politics/obama-to-call-for-laws-covering-data-hacking-and-student-privacy.html.