Conference draft of June, 2013; please do not cite or quote without permission.

Privacy, Antitrust, and Power

Frank Pasquale

INTRODUCTION

Within a neoclassical economic framework, the relationship between Internet privacy and competition is direct and positive. Consumers set out to obtain an optimal amount of privacy as a feature of the Internet services they consume. Just as a car buyer might choose a Volvo over a Ford because the Volvo is said to have better crash impact protection than the Ford, so too might a search engine user choose DuckDuckGo over Google because of the privacy DuckDuckGo offers.[1] Companies compete to offer more or less privacy to users.[2] If there are many companies in a given field, they will probably offer many different levels of privacy to consumers. If consumers choose to use services from companies that offer little to no privacy protection, that reveals a preference to spend little to nothing on (or looking for) privacy.

Within the neoclassical model, there is little reason for government to limit a firm's collection, analysis, and use of data. Consumers individually decide how much information they want to release about themselves into commercial ecosystems. Indeed, such limits might even undermine the competition that is supposed to be the primary provider of privacy.[3] Companies may need to share data

---

[1] Google's advocates frequently mention DuckDuckGo as a competitor, but industry experts are skeptical. Brooke Gladstone, *Can a Small Search Engine Take on Google?*, ON THE MEDIA (Apr. 12, 2013), http://www.onthemedia.org/2013/apr/12/duck-duck-go-and-competition-search-market/transcript/ ("DuckDuckGo doesn't collect any of your personal data, at all, full stop. . . . Still, Danny Sullivan, who founded Search Engine Land.com, laughed when Google cited DuckDuckGo as a contender. 'It would be like a major baseball player saying, yeah, there's plenty of great athletes out there, look at this kid who's in eighth grade. And the only reason it can really get counted is because there's relatively little competition in the space . . . .'").

[2] DOC SEARLS, THE INTENTION ECONOMY 188 (2012) ("We don't need to change laws. Not yet, anyway. Freedom of contract is already embedded in standing law, and all we need now are tools that will cause practice to change. We've started to make those.").

[3] Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, 103 NW. U. L. REV. 1, 11–12 (2008) ("An uneven playing field that allows one firm to use the information that it sees while blocking others from doing the same thing creates market power through limiting competition. We rarely want to do that. And privacy rules that limit how information can be used and shared across firms will artificially push towards greater consolidation, something that usually works against maintaining robust competition."). Picker argued that privacy laws restricting interfirm (but not intrafirm) data-sharing may actually undermine competition by encouraging consolidation of firms..

with one another in order to compete effectively. Privacy laws that interfere with that sharing press firms to merge, so that they can seamlessly utilize data that they would have sold or traded to one another in the absence of privacy laws restricting that action.

It would be nice to believe that market forces are in fact promoting optimal levels of privacy. It would also be comforting if antitrust law indirectly promoted optimal privacy options by assuring a diverse range of firms that can compete to supply privacy at various levels (and in various forms).[4] But this position has been rendered less and less plausible both by technological change and doctrinal evolution. Antitrust law has been slow to recognize privacy as a dimension of product quality, and the competition that antitrust promotes can do as much to trample privacy as to protect it.[5] In an era of big data, every business has an incentive to be nosy in order to maximize profits.[6]

The neoliberal account of "competition promoting privacy" only achieves surface plausibility by privileging the short-term "preferences" of consumers to avoid data sharing.[7] The narrowness of "notice-and-consent" as a privacy model nicely matches the short-term economic models now dominating American antitrust law. The establishment in the field is largely unconcerned with too-big-to-fail banks, near monopoly in search advertising, media consolidation, and other forms of industrial concentration. By focusing myopically on efficiency gains that can be temporary or exaggerated, they gloss over the long term pathologies of corporate concentration.[8] So, too, does a notice-and-consent privacy regime privilege snap

[4] "Indirectly" is used here because it is now antitrust orthodoxy that this field of law exists only to protect competition, not competitors, and therefore is concerned first and foremost with *directly promoting consumer welfare.* For an account of the rise of consumer welfare as antitrust's standard (and the problems this has caused), *see* Barak Orbach, *How Antitrust Lost Its Goal*, 81 FORDHAM L. REV. 2253, 2253 (2013) ("[W]hile 'consumer welfare' was offered as a remedy for reconciling contradictions and inconsistencies in antitrust, the adoption of the consumer welfare standard sparked an enduring controversy, causing confusion and doctrinal uncertainty.").

[5] As Paul Ohm has documented, competition among broadband ISPs has led them to "search[] for new sources of revenue . . . [by] 'trading user secrets for cash,' which Google has proved can be a very lucrative market." Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1423, 1425-27 (2009) (describing the many commercial pressures leading carriers to monetize behavioral data at the expense of user privacy).

[6] VIKTOR-MAYER SCHÖNBERGER AND KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 93 (2013).

[7] Even if consumers tried to opt out more often, notice-and-consent is increasingly irrelevant because, in an era of big data, whatever one might try to hide by keeping certain pieces of data private is increasingly easy to infer from other pieces of data. *Id.* at 183.

[8] For a critique of contemporary antitrust, *see* BARRY C. LYNN, CORNERED: THE NEW MONOPOLY CAPITALISM AND THE ECONOMICS OF DESTRUCTION 30 (2010) ("[S]uperconsolidation is pretty much

judgments of consumers to "opt-in" to one-sided contracts over a reflective consideration of how data flows might be optimized for consumers' interests generally. As privacy declines and companies consolidate, mainstream antitrust and privacy theory often legitimates the process. Some scholarship can even amount to the "structural production of ignorance," characterizing scenarios as "consent" and "competition" when they are experienced by consumers and users as coercive and monopolistic.[9]

Other commentators have made the case for more comprehensive and holistic visions of privacy and antitrust law.[10] This essay aims only to develop some connections between the key failures of each field. Part I of this essay analyzes the flaws in conceiving of privacy of a purchasable commodity. Part II suggests policy changes that account for the implications of the complexity of consumer privacy. This essay's aim is less to propose concrete reforms than to illuminate the shaky foundations of today's privacy and antitrust policymaking. Once that is done, federal and state agencies can develop a new orientation toward the problems caused by the centrifugal pull of data and market share into an ever-smaller group of dominant firms. The primary purpose of privacy law (as applied to corporations) and antitrust law is to deter and punish unfair, deceptive, or harmful behavior. Improving market processes is only one tool among the many that privacy and antitrust policy makers should use to achieve these aims.

---

standard operating procedure for all industries in the United States these days."); Richard Du Boff and Edward S. Herman, *Mergers, Concentrations, and the Erosion of Democracy*, 53 MONTHLY REVIEW 1 (2001), *available at* http://monthlyreview.org/2001/05/01/mergers-concentration-and-the-erosion-of-democracy ("Antitrust action, already limited in its effectiveness, is likely to be less so in a globalizing economy.").

[9] Robert N. Proctor, *Agnotology: A Missing Term to Describe the Cultural Production of Ignorance (and Its Study), in* AGNOTOLOGY: THE MAKING AND UNMAKING OF IGNORANCE 3 (Robert N. Proctor & Londa N. Schiebinger eds., 2008). As Ralph Miliband put it in his eulogy for C. Wright Mills, "many social scientists, in the struggle between enlightenment and obscurantism, are on the wrong side, or refuse to be involved, which comes to the same." Ralph Miliband, *Tribute to C. Wright Mills*, NEW LEFT REVIEW (Dec. 12, 2012), http://www.newleftproject.org/index.php/site/article_comments/tribute_to_c_wright_mills. The same insight applies to attorneys.

[10] Maurice E. Stucke, *Better Competition Advocacy*, 82 ST. JOHN'S L. REV. 951, 1001 (2008); Julie E. Cohen, *Network Stories*, 70 LAW & CONTEMP. PROBS. 91, 92 (2007) (describing what "makes the network good"); JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 1-3 (2011); Julie Cohen, *What is Privacy For?*, 126 HARVARD L. REV. 1904, 1906 (2013).

I. PARADOXES OF PRIVACY

There are normative rationales for giving individuals control over data—but there are almost always equal and opposite rationales for openness and sharing. Privacy advocates sometimes attempt to solve these conflicts by adopting a neoliberal model of identity management, which often recommends notice-and-consent policies.[11] Unfortunately, there is little evidence that the current notice-and-consent frameworks' presumed model for privacy protection is empirically supported.

Consumers neither experience nor hope for meaningful protection of privacy in the "terms of service" foisted on them and the "privacy settings" that leading companies offer them.[12] Former FTC Chairman Jon Leibowitz admitted as much, beginning a roundtable by stating, "[w]e all agree that consumers don't read privacy policies."[13] It would take months or even years to read through all the privacy giveaways that bind consumers online, and the payoff for doing so is vanishingly low.[14] When was the last time a consumer actually renegotiated terms in his or her favor?[15] The prospect of altering the terms of service for an intermediary like Facebook or Google is beyond the ambition of almost all users.[16]

---

[11] FRED H. CATE & VIKTOR MAYER-SCHÖNBERGER, NOTICE AND CONSENT IN A WORLD OF BIG DATA 3 (Microsoft Global Privacy Summit Summary Report and Outcomes 2012), *available at* http://www.microsoft.com/en-us/download/details.aspx?id=35596.

[12] Timothy J. Muris, Chairman, Fed. Trade Comm'n, Remarks at the Privacy 2001 Conference (Oct. 4, 2001), *available at* http://www.ftc.gov/speeches/muris/privisp1002.shtm (describing futility of notices); Frank Pasquale, *Crowdsourcing Interpretation of TOS* (Aug. 19, 2012, 3:30 PM), http://www.concurringopinions.com/archives/2012/08/crowdsourcing-the-interpretation-of-terms-of-service-agreements.html (discussing belated effort to make terms of service more tractable).

[13] Jon Leibowitz, Chairman, Fed. Trade Comm'n, Introductory Remarks at the FTC Privacy Roundtable (Dec. 7, 2009), *available at* http://www.ftc.gov/speeches/leibowitz/091207privacyremarks.pdf. As Distinguished Professor and C. Ben Dutton Professor of Law, Director of the Center for Applied Cybersecurity Research, and Director of the Center for Law, Ethics, and Applied Research in Health Information at Indiana University Fred H. Cate observes, this is "a remarkable acknowledgement from the U.S. federal agency that has probably done the most to promote [privacy policies]." Fred Cate, *Protecting Privacy in Health Research: The Limits of Individual Choice* 98 CALIF. L. REV. 1765, 1772 (2010).

[14] Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC (Mar. 1, 2012, 2:24 PM), http://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

[15] MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW 107 (2013) (observing the adhesive nature of the contracts).

[16] Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 469 (2006) ("[N]o one reads [many of these] forms of contract anyway . . . ."); Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Testing a Law and Economics Approach to Standard Form Contracts* 1 (N.Y. Univ. Law & Econ. Working Papers, Paper No. 195, 2009), *available at* http://lsr.nellco.org/cgi/viewcontent.cgi?article=1199&context=nyu_lewp ("We track the Internet

Consumers vaguely understand that online data collection creates a "digital self," or profile, of their behavior.[17] But, consumers have little confidence that they can detect or deter unfair, discriminatory, or inaccurate versions of that profile.[18] It is debatable whether privacy as self-protection via shrewd data disclosure is even a self-concept that policy makers should seek to cultivate. In a world where consumers are expected to zealously guard their data (or suffer the consequences), consumers most in need of fair information practices are least likely to have the resources to actually demand and secure their data.[19] The proper allocation of surveillance has very little relationship with users' desire to pay for privacy, and indeed may be inversely correlated with it (i.e., the person who cares enough to try to make her online actions completely anonymous may be a criminal or a heroic dissident). It very difficult to value the actions that privacy protects in the abstract.

Like the need for health care, the need for privacy may actually be negatively correlated with income.[20] Or, privacy laws may become one more set of

---

browsing behavior of 45,091 households with respect to 66 online software companies to study the extent to which potential buyers access the associated important standard form contract, the end user license agreement. We find that only one or two out of every thousand retail software shoppers chooses to access the license agreement, and those few that do spend too little time, on average, to have read more than a small portion of the license text.").

[18] Daniel J. Solove popularized the term "the digital person" in 2004 with a book of the same title. For an example of its implications in social media, see Rob Horning, *Google Alert for the Soul*, THE NEW INQUIRY (Apr. 12, 2013), http://thenewinquiry.com/essays/google-alert-for-the-soul/ ("The data self allows us to view the self as productive along neoliberalist lines, giving a protocol for handling both too much visibility and too much information. . . Social media instigate what Bernard Stiegler has called a "grammatization of the social": giving standard forms by which everyday-life experience can be captured and processed to imbue it with legible meaning. It makes that experience "real" in the sense that augments our reputation in the data forms neoliberalism demands. It makes memories into curated cultural capital.").

[19] Michele Estrin Gilman, *The Class Differential in Privacy Law*, 77 BROOK. L. REV. 1389, 1423 (2012) ("[T]here are statutes that protect against disclosure of credit histories, student records, debts, bank records, tax returns, television viewing habits, health information, and . . . video rentals. Obviously, Americans from every social class benefit from these protections. Still, this bevy of statutes does not protect anyone from the embarrassment that occurs when the government or private entities gather information in an intrusive or demeaning manner in the first place. This mistreatment tends to happen disproportionately to the poor and other marginalized groups.").

[20] To model this: Stipulate a population with Group A, which is relatively prosperous and has the time and money to hire agents to use notice-and-consent privacy provisions to its advantage (i.e., figuring out exactly how to disclose information to put its members in the best light possible). Meanwhile, most of Group B is too busy working several jobs to use contracts or law to its advantage in that way. We should not be surprised if Group A leverages its mastery of privacy law to enhance its position relative to Group B. Better regulation would restrict use of data, rather than allow users to restrict collection of data. For more criticism of "ability to pay" as a guide to social value, *see* Reza Dibadj, *Beyond Facile Assumptions and Radical Assertions: A Case for "Critical Legal Economics*," 2003 UTAH L. REV. 1155, 1161 (2003) ("[T]hree of the most basic assumptions to the popular [law & economics]

rules that the haves manipulate to increase their advantages over the have-nots. In a world where persons are persistently ranked and stigmatized via data collection, an equilibrium featuring wealthy individuals who have purchased privacy, and poorer individuals who cannot afford it, may be worse than an equilibrium where no one has access to this "product." As data scientist Cathy O'Neil observes:

> There are very real problems in the information-gathering space, and we need to address them, but one of the most important issues is that the very people who can't afford to pay for their reputation to be kept clean are the real victims of the system. . . . [T]hrough using the services from companies Reputation.com and because of the nature of the personalization of internet usage, the very legislators who need to act on behalf of their most vulnerable citizens won't even see the problem since they don't share it.[21]

One day, perhaps, services like Reputation.com will scale and will offer more affordable "products" to a mass audience. But even this market-based model fails, because privacy protection is not remotely a "thing." Rather, privacy is a social practice.[22] One can almost never contract for a certain level of privacy protection and expect that mere assurance to be the end of the matter. In a world of constantly evolving threats and vulnerabilities, restricting data flows can be as complex and beset by asymmetric information (and uncertain outcomes) as health care. Users have so many points of vulnerability that it seems futile to focus on fixing any one of them. For example, a consumer could refrain from talking about personal illnesses on Gmail or Facebook. But, how could someone be sure that insurance paperwork, credit or bank records, or websites visited online did not somehow betray such conditions? The information could end up in the hands of a profiler like Axciom or a scraper linking online handles to real identities.[23]

---

enterprise—that people are rational, that ability to pay determines value, and that the common law is efficient—while couched in the metaphors of science, remain unsubstantiated.").

[21] Cathy O'Neil, *Fighting the information war (but only on behalf of rich people)*, MATHBABE (Dec. 11, 2012), http://mathbabe.org/2012/12/11/fighting-the-information-war-but-only-on-behalf-of-rich-people/. O'Neil also predicts that reputation management services " could well create a problem to produce a market for their product." *Id.*

[22] Cohen, *Privacy*, *supra* note 10, at 1905 ("[F]reedom from surveillance, whether public or private, is foundational to the practice of informed and reflective citizenship. Privacy therefore is an indispensable structural feature of liberal democratic political systems."); Frank Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency In Internet Intermediaries*, 104 NW. U. L. REV 105, 151-54 (2010) (describing privacy as an irreducibly social practice).

[23] *See, e.g.*, Julia Angwin & Steve Stecklow, *'Scrapers' Dig Deep for Data on Web*, WALL ST. J. (Oct. 11, 2010, 9:30 PM), http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html. The entire

Faced with these daunting challenges to market-based models of privacy as purchasable commodity, the libertarian privacy establishment nevertheless asserts that there is no need for reform presently because consumers are revealing strong preferences for privacy-invasive services.[24] But consumers are not flocking to companies like Facebook and Google out of a conscious preference for the privacy policies on offer. Rather, they are drawn to such firms because of their fine-tuning and personalization of search and social network services. Each firm's hostility to privacy may be an important reason why they have the data needed to provide such fine-tuning and personalization, or they may simply be taking advantage of near-monopoly status as the highest quality search and social network experience.[25] Given the opacity of operations at such firms, we may never know how necessary invasions of privacy are to their business models.

Nevertheless, we can at least strive to describe their economic role more precisely: they are less services than they are *platforms* for finding services (and, occasionally, goods). Facebook, Google, and even Internet service providers ("ISPs") might be thought of less as sellers of particular end-services, than as advisors or gatekeepers, or connectors between users and what they want.[26] In this intermediary role, Internet companies are far closer to health insurers or mortgage brokers than they are to sellers of products or services.[27] People are not using Google or Facebook for the platform itself—rather, they are trying to find things through the platform. As much as consumers may want to learn about the ultimate

---

"What They Know" series at the Wall Street Journal—dozens of articles dating back to 2010—reveals, on an almost weekly basis, commercial entities (ranging from device fingerprinters to data miners to scrapers) capable of analyzing data points, reidentifying data sources, and otherwise defeating once-reasonable privacy precautions.

[24] Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 984-85 (2013) (describing consumer preferences for privacy-invasive services such as Gmail and Facebook).

[25] For an economic sociology of such near-monopoly services, see LUCIEN KARPIK, VALUING THE UNIQUE: THE ECONOMICS OF SINGULARITIES 3 (2010) ("[N]eoclassical economics, even in its latest versions, ignores one particular category of markets. . . . These overlooked markets are markets of singular, incommensurable products.").

[26] Even those who downplay the role of search engines as conduits recognize their essentially intermediary function. James Grimmelmann, *Speech Engines*, 98 MINN. L. REV. (forthcoming 2014) ("[S]earch engines are not primarily conduits or editors, but advisors. They help users achieve their diverse and individualized information goals by sorting through the unimaginable scale and chaos of the Internet.").

[27] Ioannis Lianos, Evgenia Motchenkova, and Eric Bartelsman *Market Dominance and Quality of Search Results in the Search Engine Market: Analysis of Exploitative and Exclusionary Abuses*, 9 J. COMPETITION L. & ECON. 1, 3 (2013), *available at* http://jcle.oxfordjournals.org/content/early/2013/04/25/joclec.nhs037.short?rss=1 ("The search engine acts as a platform intermediating between content providers (who want users), users (who want content), and advertisers (who want users).").

services they are looking for, consumers are unlikely to want to spend much time learning about the privacy policies (among other features) of the services they use to find the services they are looking for. There is simply not enough time in the day to scrutinize the practices of most firms—particularly those so unique and dominant that it is exceedingly unlikely that any term will be so adverse that it justifies switching to a vastly worse alternative.[28]

II. FROM CHIMERICAL COMPETITION TO POWER-BALANCING REGULATION

Given the enormous computing capacity and storage necessary to run such platforms, and the self-reinforcing data advantage of dominant firms, there is unlikely to be much competition in search and social networking.[29] Even if consumers were actually shopping for pro-privacy terms when participating in search and social networking activities, they are likely to have as little choice there as they have in their Internet service provision.[30] Moreover, just as it is difficult to switch operating systems or Internet service providers, it is very difficult to ask one's "social graph" (or network of friends) to transfer themselves to a new platform. And, it may be impossible to extract from Google the personalized "training" a user passively does through searches to help it determine optimal results.[31]

Given the difficulty of "exit" in these scenarios, neoclassical economic approaches to both privacy and competition are misguided. When a service collects information about a user, the situation is so far from the usual arms-length market

---

[28] For a sensitive consideration of the many impediments to notice and choice in a related context, see Pedro G. Leon et al., *Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising*, CYLAB (May 10, 2012), http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11017.pdf.

[29] Frank Pasquale, *Seven Reasons to Doubt Competition in the General Search Engine Market*, MADISONIAN (Mar. 18, 2009), http://madisonian.net/2009/03/18/seven-reasons-to-doubt-competition-in-the-general-search-engine-market/; Pasquale, *supra* note 22, at 140 (describing in detail barriers to entry in general purpose search).

[30] SUSAN CRAWFORD, CAPTIVE AUDIENCE: THE TELECOM INDUSTRY AND MONOPOLY POWER IN THE NEW GILDED AGE 111-14 (2013) (describing ISP duopolies); Frank Pasquale, *Paradoxes of Digital Antitrust*, HARV. J. L. & TECH (forthcoming 2013) (describing search near-monopoly); Frank Pasquale, *Platforms, Power, and Freedom of Expression* 4 (2013) (unpublished manuscript) (on file with author) (describing power of Apple, Twitter, Facebook, and Google in spheres of apps, microblogging, social networking, and search).

[31] This is because Google, like other similarly situated companies, is likely to resist permitting export of all the algorithms and data necessary to reconstruct such training elsewhere. Either element, without the other, may well prove useless. As Lev Manovich has observed, "Together, data structures and algorithms are two halves of the ontology of the world according to a computer." Lev Manovich, *Database as Symbolic Form*, 5 CONVERGENCE: THE INTERNATIONAL JOURNAL OF RESEARCH INTO NEW MEDIA TECHNOLOGIES 80, 84 (1999).

transaction that transactional approaches can only be misleading. It is necessary to look to other ways of *equalizing the power relationship that surveillance entails*, and to stop trying to characterize lack of surveillance as a product that individuals have varying preferences for and purchase accordingly.[32]

This process can begin by re-examining the concept of "unfairness." In key cases, the FTC has charged a company with unfair trade practices when its security and privacy policies markedly diverged from industry standards.[33] This is a good start, but risks a "downward ratchet" if business practices generally deteriorate. As the agency has extraordinarily limited resources to police businesses (which, in turn, see little downside to "pushing the privacy envelope"), an implicit baseline approach keyed to present industry practices may be self-defeating. Industry standards, like "reasonable expectations of privacy" in the 4th Amendment context, are bound to decline without a more substantive commitment to protecting what is really at stake for consumers.[34]

Professor Michael Walzer's concept of "spheres of justice" suggests an alternative approach. [35] As Walzer argues, there are forms of allocation suited to different spheres of human experiences, be they necessities or luxuries, love or war, politics or education.[36] Sometimes the market works best, but in many other cases an alternative logic of allocation ought to prevail.[37] Rather than allocating a benefit (like deregulation) or burden (like monitoring and surveillance) based on abstract

---

[32] As Neil Richards has argued, the surveillance studies literature has demonstrated in detail that "surveillance is harmful" at least in part because it "gives the watcher power over the watched." Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1945, 1956 (2013).

[33] Ohm, *supra* note 24, at 977 ("The FTC might use its section five power to police 'unfair or deceptive acts or practices' to link a brand to a particular level of privacy. This might be the best way to implement branded privacy because it likely represents a new remedy for the FTC but not a new substantive rule."); *see also, e.g.*, Complaint at 3, In re The TJX Companies, Inc., F.T.C. File No. 072-3055 (Mar. 27, 2008), *available at* http://www.ftc.gov/os/caselist/0723055/080327complaint.pdf ("[R]espondent's failure to employ reasonable and appropriate security measures to protect personal information caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was and is an unfair act or practice."); Complaint at 12, FTC v. Wyndham, F.T.C. File No. 102-3142 (June 26, 2012), *available at* http://ftc.gov/os/caselist/1023142/120626wyndamhotelscmpt.pdf.

[34] Eric Talley, *Expectations in Legal Doctrine*, in PARADOXES AND INCONSISTENCIES IN LAW 183, 195 (Oren Perez & Gunther Teubner eds., 2006) ("Legal tests that circuitously turn on parties' expectations about the eventual outcome of the same legal test can be found in a number of . . . areas of law . . . .In criminal law, the Fourth Amendment right to privacy is governed by whether a suspect has 'a reasonable expectation of privacy.'").

[35] MICHAEL WALZER, SPHERES OF JUSTICE: A DEFENSE OF PLURALISM AND EQUALITY 10-17 (1983).

[36] *Id.*

[37] *Id.*

considerations of efficiency, Walzer's work suggests that there are unique and separate standards prevailing in different fields.[38] A company not collecting much information on its customers may not need very much privacy regulation; by contrast, the firm that bases its entire business model on knowing as much as possible about users ought to be subject to extensive monitoring.

To the extent a company creates profiles of individuals and collects data on them, a third party ought to be collecting reports from the company on how it is using that information, to whom it is selling the data, and how it maintains the security of the data.[39] This logic has already deployed in the health privacy context (where firms deploying electronic records are subject to more stringent data protections under "accounting of disclosures" rules than are other firms).[40] It can also be recognized as part of the logic of the twenty-year consent orders that resulted from FTC actions against Facebook (Beacon) and Google (Buzz).[41]

As social scientist danah boyd has complained, Facebook "[u]sers have no sense of how their data is being used."[42] Large Internet firms are black boxes. They assure users that information is being used in their best interests, but the verbiage recalls the old science fiction tale "To Serve Man."[43] Sometimes data can help route

[38] *Id.*

[39] The Federal Trade Commission's subpoenas to data brokers in December, 2012, indicate a willingness to consider this standard. Press Release, Fed. Trade Comm'n, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec, 18, 2012) *available at* http://ftc.gov/opa/2012/12/databrokers.shtm.

[40] "Before HITECH, the HIPAA Privacy Rule made it very difficult for patients to fully understand the nature and range of health information accumulated about them, especially because disclosures for 'treatment, payment and health care operations' did not need to be accounted for. After HITECH, any record kept electronically needs to be in the accounting." Frank Pasquale and Tara Adams Ragone, *The Future of HIPAA in the Cloud* 26 (Mar. 22, 2012) (manuscript on file with author), citing 45 C.F.R. § 164.528(a)(1)(i) (2010) and 42 U.S.C. § 17935(c)(1) (Supp. III, 2010) ("In applying section 164.528 of title 45, Code of Federal Regulations, in the case that a covered entity uses or maintains an electronic health record with respect to protected health information. . . . the exception under paragraph (a)(1)(i) of such section shall not apply to disclosures through an electronic health record made by such entity of such information.").

[41] Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges that it Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), *available at* http://ftc.gov/opa/2011/11/privacysettlement.shtm; Press Release, Fed. Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of its Buzz Social Network (Mar. 30, 2011), *available at* http://www.ftc.gov/opa/2011/03/google.shtm.

[42] danah boyd, *Facebook and 'Radical Transparency' (a rant)*, APOPHENIA (May 14, 2010), http://www.zephoria.org/thoughts/archives/2010/05/14/facebook-and-radical-transparency-a-rant.html.

[43] In the story, alien invaders who end war and provide other help for humans proclaim their allegiance to a volume titled "To Serve Man." It turns out to be a cookbook. *The Twilight Zone: To Serve Man* (CBS television broadcast Mar. 2, 1962), *available at* http://www.imdb.com/title/tt0734684/combined.

the user to what she needs. Other times, as legal scholar Nathan Newman notes, it can be used to find "pain points:"

> [P]eople have different maximum prices that they are willing to pay, a so-called "pain point" after which they won't buy the product. The ideal for a seller would be to sell a product to each customer at their individual "pain point" price without them knowing that any other deal is available.[44]

To serve both users and advertisers, Internet companies are going to continue to compile large datasets about the users regardless of whether the Internet companies need to obtain explicit consent to do so. The question is not: "how can we best permit consumers to opt out of data collection, or give meaningful consent to it?" Few consumers will choose to opt out of data collection, the most vulnerable have the least time to do so, and there is hyperbolic discounting of the value of one's data. Rather, the question should be: "is there a way to assure responsible use of the massive stores of information now being compiled?" The best way to do this is to develop accountings of the collection, analysis, and use of data so that policy makers and third party analysts can identify particularly troubling actions and recommend regulation or legislation designed to stop them.

The responsible use of stored data is particularly important as firms create "medical reputations" without even accessing medical records. FICO can generate a medication adherence score, and life insurers use predictive analytics to extrapolate policyholders' likely year of death.[45] In an era of big data, companies do not even need to consult the "health care sector" to impute various medical conditions or disabilities to data subjects.[46] As Professor Nicolas Terry has explained, judgments about individuals' health status do not need to be based on medical records:

> The health care sector and its stakeholders constitute an area considerably larger than the HIPAA-regulated zone. As a result, some traditional health information circulates in what may be termed a HIPAA-free zone. Further,

---

[44] Nathan S. Newman, *The Cost of Lost Privacy: Search, Antitrust, and the Economics of the Control of User Data* 78 (2011) (on file with author). Calculations of pain points are of immense value, and "what is largely missed in analyses defending Google from antitrust action is how that ever expanding control of user personal data and its critical value to online advertisers creates an insurmountable barrier to entry for new competition." *Id.* at 1.

[45] Tara Parker Pope, *Keeping Score on How You Take Your Medicine*, NEW YORK TIMES (June 20, 2011, 5:23PM), http://well.blogs.nytimes.com/2011/06/20/keeping-score-on-how-you-take-your-medicine/; Eric Siegel, *5 Reasons Organizations Predict When You Will Die*, SMARTBLOG (Feb. 27, 2013), http://smartblogs.com/leadership/2013/02/27/5-reasons-organizations-predict-when-you-will-die/.

[46] *See* Nicolas P. Terry, *Protecting Patient Privacy in the Age of Big Data*, 81 UMKC L. REV. 385, 394 (2012).

> the very concept of health sector specific regulation is flawed because health related or medically inflected data frequently circulates outside of the traditionally recognized health care sector. In both cases agreed-upon health privacy exceptionalism is jeopardized.[47]

Given these developments, it would not be unreasonable to expect big data firms to make "accountings of disclosures" of the data they hold in the same way that entities covered under the Health Insurance Portability and Accountability Act ("HIPAA") are required to. Patients have "the right to an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested," and to have the information in formats that allow their own trusted interpreters to make sense of it.[48] Before the Health Information Technology for Economic and Clinical Health ("HITECH"), the HIPAA Privacy Rule made it very difficult for patients to fully understand the nature and range of health information disclosures of their records, especially because disclosures for "treatment, payment and health care operations" did not need to be accounted for.[49] After HITECH, any disclosure of a record kept electronically needs to be in the accounting.[50]

Some industry comments on HITECH rulemaking have vigorously opposed aggressive implementation of consumer rights, claiming that appropriate technology does not yet exist.[51] But audit logs can already record the activity taking

---

[47] *Id.* at 387.
[48] 45 C.F.R. § 164.528(a)(1) (2010).
[49] *Id.* § 164.528(a)(1)(i).
[50] Before HITECH, 45 C.F.R. § 164.528 restricted the right to an accounting of disclosures by exempting disclosures that were "to carry out treatment, payment and health care operations." *Id.* HITECH removed that exception. 42 U.S.C. § 17935(c)(1) (Supp. III 2010) ("In applying section 164.528 of title 45, Code of Federal Regulations, in the case that a covered entity uses or maintains an electronic health record with respect to protected health information. . . . the exception under paragraph (a)(1)(i) of such section shall not apply to disclosures through an electronic health record made by such entity of such information.").
[51] *OCR's Proposed Revisions to Accounting for Disclosures Standard Produces Strong Opposition from Many Covered Entities*, MCDERMOTT, WILL, & EMERY 1 (October 14, 2011), http://www.mwe.com/info/news/wp1011b.pdf; Jennifer L. Edlind, HIPAA Privacy Rule Accounting of Disclosures (RIN 0991-AB62); Notice of Proposed Rulemaking, 76 Fed. Reg. 31426 (May 31, 2011) 1-2 (Aug. 1, 2011), http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0302 (responding to request for comment on HIPAA Privacy Rule and Accounting of Disclosures in capacity as University Hospital Privacy Officer); Larry Davis, Attention: HIPAA Privacy Rule Accounting of Disclosures (RIN 0991-AB62); Notice of Proposed Rulemaking, 76 Fed. Reg. 31426 (May 31, 2011) 1-3 (July 21, 2011), http://www.regulations.gov/#!documentDetail;D=HHS-OCR-2011-0011-0086 (responding to request for comment on HIPAA Privacy Rule and Accounting of Disclosures in capacity as St. Bernards Healthcare Corporate Compliance Officer).

place in many information-sharing networks,[52] including "queries made by users, the information accessed, information flows between systems, and date-and-time-markers for those activities."[53] If audit logs are immutable and pervasively attributable to entities accessing and using information, they should seriously deter misuse of data.[54]

The Department of Health and Human Services ("HHS") has also confirmed the importance of maintaining patients' ability to retrieve their records in accessible formats.[55] Covered entities must provide individuals "with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format."[56] By guaranteeing an accounting of disclosures, HITECH also promoted individuals' rights to determine how their records had been used.[57] In any twelve-month period, the first accounting that an

[52] 28 C.F.R. § 23.20(g) (2012). The audit trail is a *sine qua non* for technological due process. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1306 (2008) (exploring the due process implications of automated system determinations and arguing that technological due process requires the inclusion of audit trails into automated systems). Nevertheless, even this mechanism of protection must be carefully implemented so that the audit process itself does not create its own potential for breaches. *See, e.g.*, Dom Nicastro, *HIPAA Auditor Involved in Own Data Breach,* HEALTHLEADERS MEDIA (Aug. 8, 2011), http://www.healthleadersmedia.com/page-1/PHY-269480/HIPAA-Auditor-Involved-in-Own-Data-Breach (discussing a situation where a firm hired to conduct audits lost an unencrypted flash drive with 4,500 patient records).

[53] MARKLE TASK FORCE ON NAT'L SEC. IN THE INFO. AGE, MARKLE FOUND., IMPLEMENTING A TRUSTED INFORMATION SHARING ENVIRONMENT: USING IMMUTABLE AUDIT LOGS TO INCREASE SECURITY, TRUST, AND ACCOUNTABILITY 1 (2006). The Markle Foundation has worked on important reports on deploying cutting edge information technology in agencies, including HHS. *Id.* at 1; *see also* Sandra Nunn, *Managing Audit Trails*, 80 J. AM. HEALTH INFO. MGMT. ASS'N 44, 44 (2009) ("Audit trails are records with retention requirements.").

[54] For a discussion of the importance of immutable audit logs, see Danielle Keats Citron and Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L. J. 1441, 1473 (2011) (explaining that "immutable audit logs . . . [promote] data integrity and relevance. . . . [by] watermark[ing data] with its provenance, assuring attributions and verifiability of observations (much as citations help assure the validity of an assertion in an academic work)[and promoting] tethering and full attribution of data to allow corrections to propagate through the system") (internal citations omitted).

[55] 45 C.F.R. § 164.524(c)(2).

[56] *Id.*

[57] *See id.* § 164.528(a). Such accountings must include "(i) The date of the disclosure; (ii) The name of the entity or person who received the protected health information and, if known, the address of such entity or person; (iii) A brief description of the protected health information disclosed; and (iv) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for a disclosure under §§164.502(a)(2)(ii) or 164.512, if any." *Id.* § 164.528(b)(2).

individual requests from a covered entity must be provided for free within sixty days of the request (with some narrow exceptions).[58]

Developing a similar, "watching the watchers" approach to privacy in the context of large Internet firms would also help create the monitoring infrastructure necessary to allow antitrust authorities to determine whether firms are acting in an anticompetitive manner. In the recent antitrust inquiries regarding Google in the United States, the FTC stated that virtually every instance of suspected anticompetitive conduct could be explained as an earnest effort to improve the quality of Google's search engine results.[59] It is still unclear whether the agency had the technical competence to make that judgment. To assess the difference between actions aimed at improving user experience and those designed to nip would-be competitors in the bud, policy makers need explicit evidence regarding the use of data in changing search algorithms (and adjusting the processing of quality signals assigned to the sites that Google ranks). It is not clear from the agency's final judgment (a sparse, four page document) what types of expertise or methods the FTC deployed to make such distinctions.

---

[58] *Id.* § 164.528(c)(2) ("The covered entity must provide the first accounting to an individual in any 12 month period without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee."). Patients may also direct a CE to transmit a copy of the record to a designee, and there are limits on the fee, which cannot be more than the labor cost involved, and images and other linked data are to be included. *Id.* §§ 164.502(g)(1), 164.526(c)(4).

[59] FED. TRADE COMM'N, STATEMENT OF THE FED. TRADE COMM'N REGARDING GOOGLE'S SEARCH PRACTICES IN THE MATTER OF GOOGLE INC., FTC FILE NO. 111-0163 (Jan. 3, 2013), *available at* http://ftc.gov/os/2013/01/130103googlesearchstmtofcomm.pdf. ("The totality of the evidence indicates that, in the main, Google adopted [changes] improve the quality of its search results, and that any negative impact on actual or potential competitors was incidental to that purpose."). See also Jon Leibowitz, Chairman, Fed. Trade Comm'n, Google Press Conference 5 (Jan. 3, 2013), *available at* http://ftc.gov/speeches/leibowitz/130103googleleibowitzremarks.pdf ("Although some evidence suggested that Google was trying to eliminate competition, Google's primary reason for changing the look and feel of its search results to highlight its own products was to improve the user experience. Similarly, changes to Google's algorithm that had the effect of demoting certain competing websites had some plausible connection with improving Google's search results, especially when competitors often tried to game Google's algorithm in ways that benefitted those firms, but not consumers looking for the best search results. Tellingly, Google's search engine rivals engaged in many of the same product design choices that Google did, suggesting that this practice benefits consumers."). Liebowitz does not even acknowledge, let alone try to disprove, the possibility of a lemons equilibrium having given rise to the common "product design choices" among search engines. Frank Pasquale, *Google Antitrust: The FTC Folds*, MADISONIAN (Jan. 3, 2013), http://madisonian.net/2013/01/03/google-antitrust-the-ftc-folds/.

Routinely making information available about data collection will help develop the infrastructure and analytics necessary to bring antitrust enforcement into the twenty-first century by assuring rapid understanding of the corporate actions underlying the complaints of companies like NavX, Foundem, Yelp, and Nextag. The key to competition on the Internet is not trying to create the conditions for the development of another Google, Facebook, or Apple. Rather, policy makers need to ensure that the companies that occupy such commanding heights in the Internet ecosystem do not use their dominant positions to exclude and discourage firms operating in adjacent fields (such as specialized search in the case of Google, or app development in the case of Apple).

Since "sunlight is the best disinfectant," surveillance of these dominant firms' practices could allay fears of the venture capitalists and innovators (who are loathe to enter online markets knowing that a dominant firm could effectively cut off their air supply on a whim). Monitoring should do to leading Internet companies what they do to their users each day: systematically study, categorize, and characterize their behavior. Ordinary users and small firms rarely have the time or expertise to identify inaccurate, discriminatory, or unfair profiling. Governmental entities need to take the lead here, either developing the institutional capacity to find suspect practices or to hire contractors to do so. Such actions will lay a foundation for policy that responds to core normative concerns regarding the collection, analysis, and use of data, and promotes competition online. Without this type of auditing and monitoring, policymakers will be regulating in the dark.

CONCLUSION

Privacy and competition law are related in high-tech industries, but not in the usual way depicted in the literature. It is hard to imagine an online world in which users care deeply about purchasing privacy, or even consider it carefully as a quality of the service they are using. This is not because the users don't care about privacy. Rather, consumers have little to no real choice in the matter because the dominant services are so superior to also-ran competitors. Dominant firms see little to no reason to compete to improve their privacy practices when users are so unlikely to defect. A lemons equilibrium prevails.[60]

If the platforms at the heart of the digital economy were entirely committed to monetization and efficiency, they would offer consumers more options. A user might be offered the opportunity to pay, say, twice the discounted present value of

[60] *See* RADIN, *supra* note 15, at107-08 (2013).

the data he was expected to generate for the platform, and in return, to assure that data is unavailable for use by the platform.[61] But such a seemingly Pareto-optimal arrangement is not on offer, and its invisibility suggests why imbalances in power, rather than efficiency or consent, ought to be the normative focus of antitrust and privacy law.

Companies like Facebook and Google have totalizing visions. Mark Zuckerberg wants intimate details of the entire world on his social network.[62] Sergey Brin has said that the ideal search engine would be "like the mind of God."[63] Lest that be dismissed as a founder's hyperbole, the head of Google's search rankings team, Amit Singhal, has recently stated that "[t]he *Star Trek* computer is not just a metaphor that we use to explain to others what we're building. It is the ideal that we're aiming to build—the ideal version done realistically."[64] No doubt Steve Jobs's empire building aimed in a similar direction, and Apple's growing cash pile betokens the endurance of his vision.[65]

The leaders of these firms are not simply in it for the money. Rather, they seek to create platforms that nearly everyone must use to navigate and participate in an increasingly digital reality.[66] They are seeking a power akin to that held by media barons of old: to shape individuals' reality and perceptions.[67] That power

---

[61] While the number might seem unquantifiable, the imperatives of financialization mean that estimates are at least available internally. *See, e.g.*, Quentin Fottrell, *Who Would Pay $5,000 to Use Google? (You)*, SMARTMONEY, (Jan. 25, 2012), http://blogs.smartmoney.com/advice/2012/01/25/who-would-pay-5000-to-use-google-you/.

[62] *See, e.g.*, Emma Barnett, *Facebook Wants Your Life Story*, THE TELEGRAPH (Sept. 23, 2011), http://www.telegraph.co.uk/technology/facebook/8783750/Facebook-wants-your-life-story.html.

[63] Frank Pasquale, *Copyright in an Era of Information Overload: Toward the Privileging of Categorizers*, 60 VAND. L. REV. 135, 146 (2007).

[64] Farhad Manjoo, *Where No Search Engine Has Gone Before*, SLATE (Apr. 11, 2013), http://www.slate.com/articles/technology/technology/2013/04/google_has_a_single_towering_obsession_it_wants_to_build_the_star_trek_computer.html.

[65] TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES 269-79 (2010) (describing Apple as a media empire); *see also* john a. powell & Stephen Menendian, *Beyond Public/Private: Understanding Excessive Corporate Prerogative*, 100 KY. L.J. 43, 109 (2012).

[66] Indeed, given the interpenetration of on and offline worlds in a project like Google Glass, we may soon be able to delete "an increasingly digital" in that sentence. *See, e.g.*, Nathan Jurgenson, *Digital Dualism and the Fallacy of Web Objectivity*, THE SOCIETY PAGES (Sept. 13, 2011), http://thesocietypages.org/cyborgology/2011/09/13/digital-dualism-and-the-fallacy-of-web-objectivity/ (describing how the digital and physical are increasingly meshed).

[67] For a comparison of the power of old and new media, *see generally* WU, *supra* note 65. Wu regales the reader with stories of powerbrokers ranging from ATT's Theodore Vail to Google's Eric Schmidt. *Id.* at 3-5, 270. Wu also reminds readers that a pure market-plus-antitrust "approach is inadequate for any of the main 'public callings,' i.e., the businesses of money, transport, communications, and energy." *Id.* at 303.

may seem more fragmented today, when thousands of channels on YouTube and billions of Facebook newsfeeds appear to disperse the cultural hegemony that the three major broadcasters once achieved. But behind the surface diversity there is ever more concentration of activity in a small group of platforms that know ever more about their users.[68] That is a type of personalized knowledge, and opportunity for manipulation, that executives relying on old, analogue "Nielsen Ratings" could never have dreamed of.[69]

At their best, privacy and antitrust laws have recognized that type of power as something to be modulated and monitored.[70] The Privacy Act arose out of citizens' concerns about the unaccountable power of those in control of massive databases.[71] The Sherman Act was a direct response to the power of trusts in the late nineteenth century.[72] Enhanced technologies of monitoring data use are a step toward the revival of each area of law. Citizens and competition law authorities can only hold large firms accountable for unfair data practices and unfair competition if they have a clear sense of how data is being collected, analyzed, and used.

[68] For an insightful account of the role of new technologies in centralizing power, see generally DAVID GOLUMBIA, THE CULTURAL LOGIC OF COMPUTATION (2009).
[69] *See generally* Robert Epstein and Ronald E. Robertson, *Democracy at Risk: Manipulating Search Rankings Can Shift Voting Preferences Substantially Without Voter Awareness* (forthcoming May 2013) (on file with author; paper to be presented at the 25th annual meeting of the American Association for Psychological Science).
[70] C. Edwin Baker, *Media Concentration: Giving Up on Democracy*, 54 FLA. L. REV. 839, 857 (2002).
[71] U.S. DEP'T OF JUSTICE, OVERVIEW OF THE PRIVACY ACT OF 1974 4 (2012), *available at* http://www.justice.gov/opcl/1974privacyact-2012.pdf.
[72] Harry First and Spencer Weber Waller, *Antitrust's Democracy Deficit*, 81 FORDHAM L. REV. 2543, 2543-44 (2013) (describing "an antitrust system captured by lawyers and economists advancing their own self-referential goals, free of political control and economic accountability," and ignoring the "political values that we believe underlie the antitrust laws.").