THE LAW AND ECONOMICS OF DATA AND PRIVACY IN ANTITRUST ANALYSIS

Geoffrey A. Manne & R. Ben Sperry

August 2014 – DRAFT

Introduction

The conclusion of this article is that privacy has little or no rational relevance for antitrust policy. "Privacy" is relevant to antitrust law and economics at all for little reason other than that a meme caught on — largely a function of comments made by policy advocates and policymakers like Peter Swire and Pamela Jones Harbour (including her statement in the Google-DoubleClick merger) – that privacy is antitrust relevant.

Simply put, for a product characteristic to be relevant to a competitive analysis, the characteristic itself must be relevant — and it must be logically affected by monopoly in ways that may harm consumers (e.g., in mergers, there must be an increased ability and incentive, as a result of a proposed merger, for the post-merger firm to degrade privacy as an exercise of monopoly power). But no one has offered a coherent story of how degrading privacy can be anticompetitive — or even what, precisely, "degrading privacy" means.

Not that there haven't been attempts. Below, in Part I, we outline the reigning theories of how to incorporate privacy into antitrust analysis. In Part II, we focus on the problems facing an antitrust analysis based on privacy concerns. In Part III, we conclude that antitrust may not be the best way for dealing with social problems like privacy, and consider alternative legal avenues to ameliorate such harms.

I. Theories of Privacy in Antitrust Analysis

Several scholars and policymakers have indeed proposed that antitrust should incorporate effects on privacy in a proper analysis. "How, why, and when" privacy considerations should be considered differ among them, however. The best categorization of these diverse approaches was offered by Peter Swire in his testimony submitted to the FTC Town Hall on Behavioral Advertising (with two important additions from the subsequent literature):[1] (1) the fundamental

[1] *Behavioral Advertising: Tracking, Targeting, and Technology: Town Hall Before the FTC*, (Oct. 18, 2007) (testimony of Peter Swire, Professor, Moritz College of Law of the Ohio State University), *available at* http://www.americanprogress.org/issues/regulation/news/2007/10/19/3564/protecting-consumers-privacy-matters-in-antitrust-analysis/.

human rights approach;[2] (2) the undue concentration of economic power approach;[3] (3) the exploitation/facilitation of price discrimination approach;[4] (4) the foreclosure of access to data approach;[5] (5) the privacy as nonprice competition approach;[6] (6) the skeptical approach.[7]

While there are distinctions between these approaches, many advocates seem to identify them as complements and offer various combinations of them.[8] And while the DoubleClick merger was the context in which many first considered privacy's place in antitrust analysis,[9] a

---

[2] *See, e.g.*, *An Examination of the Google-DoubleClick Merger and the Online Advertising Industry: What are the Risks for Competition and Privacy?: Hearing Before the Subcomm. on Antitrust, Competition Policy and Consumer Rights*, 110th Cong. 13-17 (Sept. 27, 2007) (testimony of Marc Rotenberg, President of EPIC), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110shrg39015/pdf/CHRG-110shrg39015.pdf.

[3] *An Examination of the Google-DoubleClick Merger and the Online Advertising Industry: What are the Risks for Competition and Privacy?: Hearing Before the Subcomm. on Antitrust, Competition Policy and Consumer Rights*, 110th Cong. 2 (Sept. 27, 2007) (statement of Sen. Herb Kohl), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110shrg39015/pdf/CHRG-110shrg39015.pdf; Frank Pasquale, *Social Networks and Antitrust: The Problem of Diverse Consumer Preferences*, Presentation at George Mason University Law Review Conference (Jan. 26, 2012), *available at* http://www.georgemasonlawreview.org/doc/Pasquale_SocNetwork.pdf.

[4] *See* Nathan Newman, *The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google* 40 WM. MITCHELL L. REV. (forthcoming 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2310146.

[5] *See, e.g.*, Nathan Newman, *Search, Antitrust and the Economics of the Control of User Data*, 20 YALE J. ON REG. (forthcoming 2014), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309547; Pamela Jones Harbour & Tara Isa Koslov, *Section 2 in a Web2.0 World: An Expanded Vision of Relevant Product Markets*, 76 ANTITRUST L.J. 769, 773 (2010); *An Examination of the Google-DoubleClick Merger and the Online Advertising Industry: What are the Risks for Competition and Privacy?: Hearing Before the Subcomm. on Antitrust, Competition Policy and Consumer Rights*, 110th Cong. 7-9 (Sept. 27, 2007) (testimony of Brad Smith, Senior Vice President of Microsoft), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-110shrg39015/pdf/CHRG-110shrg39015.pdf.

[6] *See, e.g.*, Harbour & Koslov, *supra* note 5, at 773-74; Swire, *supra* note 1, at 4-7.

[7] *See, e.g.*, James C. Cooper, *Privacy and Antitrust: Underpants Gnomes, The First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129 (2013); Allen P. Grunes, *Another Look at Privacy*, 20 GEO. MASON L. REV. 1107 (2013).

[8] *See, e.g.*, George Bauer, *eMonopoly: Why Internet-Based Monopolies have an Inherent "Get-Out-of-Jail-Free-Card"*, 76 Brook. L. Rev. 731, 770-72 (2011) (arguing a variation of the undue concentration approach and the privacy as nonprice competition approach); Eli Edwards, *Stepping Up to the Plate: the Google-DoubleClick Merger and the Role of the Federal Trade Commission in Protecting Online Data Privacy* (Working Paper, Apr. 25, 2008), *available at* http://ssrn.com/abstract=1370734 (arguing each theory to some extent); Senator Al Franken, Remarks to the American Bar Association (Antitrust Section) 18-27 (Mar. 29, 2012), *available at* http://assets.sbnation.com/assets/1033745/franken_aba_antitrust_speech.pdf (same); Pasquale, *supra* note 3 (same); Harbour & Koslov, *supra* note 5, at 773-74 (arguing foreclosure of access and privacy as nonprice competition).

[9] Statement of Federal Trade Commission, Google/DoubleClick, FTC File No. 071-0170 (Dec. 20, 2007), *available at* http://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf.

few scholars have argued their analyses could be extended into Section 2 monopolization cases as well.[10]

Below, we briefly present each approach and the scholars who have advocated for them.

A. Privacy as Human Right

The fundamental human rights approach encourages the FTC to seek to minimize or avoid the infringement of the right to privacy during antitrust review. In his Senate testimony on the Google-DoubleClick merger, EPIC President Marc Rotenberg has argued that "[i]t is our view that unless the Commission establishes substantial privacy safeguards by means of a consent decree, Google's proposed acquisition of DoubleClick should be blocked."[11]

The human rights approach has received little attention from scholars,[12] beyond passing mention from Swire,[13] and fails to be antitrust-relevant under current jurisprudence.

This approach does not consider the economic benefits, to either consumers or the market, of data collection and use. At the very least, it places such an extremely high value on privacy that there is no balancing or consideration of tradeoffs.

While this may reflect the views of a few consumers, the vast majority do not have such strong preferences. Those infra-marginal consumers who do have these preferences can pay the costs of meeting their atypical demand

The services that are often at issue are largely, or completely, free of direct consumer cost. Nevertheless, it is unreasonable (and would be deleterious to consumer welfare) to expect an infinite variety of freely available products sufficient to meet every consumer demand to be provided at no cost. And here, as one would expect from a well-functioning market, variety, including more-privacy-protective products and services, is available at some price.

Most users pay by having their data collected and then seeing targeted ads or having that information sold for other uses. Those who wish to avoid such data collection or use must gener-

---

[10] *See e.g.*, Harbour & Koslov, *supra* note 5, at 774 n.15; Newman, *Search*, *supra* note 5, at 5-62; Bauer, *supra* note 8, at 771.

[11] Rotenberg, *supra* note 2.

[12] At least in conjunction with antitrust. For instance, see Julie E. Cohen, *What Privacy is For*, 126. HARV. L. REV. (forthcoming 2013), *available at* http://www.harvardlawreview.org/symposium/papers2012/cohen.pdf.

[13] Swire, *supra* note 1.

ally pay for the products directly, but have options to do so. Among other things, those consumers can generally pay by purchasing services that don't collect or use data in objectionable ways (for example, self-hosted or other paid email services instead of Gmail or Yahoo Mail) or by using services that may have lower quality or other, different characteristics, but that don't collect data (for example, search engines that don't collect data but may not be as effective as those that do). Similarly, there are a number of "self-help" mechanisms (like third-party applications or incognito browsing) that can minimize the exposure of data at some cost to underlying product functionality.

Each consumer can make his or her own choice to suit his or her own weighing of the costs and benefits, and treatment of privacy as a right entails imposition of costs dramatically out of proportion to the benefits, given the ready availability of self help (and protection from consumer protection and other laws). We should care about letting consumers express their preferences, not about imposing our preferences (or a minority preference) on them.

B. Undue Concentration of Economic Power

The undue concentration of economic power approach is represented best by Senator Herb Kohl and scholar Frank Pasquale. To lead off the Senate Judiciary hearing on Google and DoubleClick, Senator Kohl stated:

> Some commentators believe that antitrust policymakers should not be concerned with these fundamental issues of privacy, and merely be content to limit their review to traditional questions of effects on advertising rates. We disagree. The antitrust laws were written more than a century ago out of a concern with the effects of undue concentrations of economic power for our society as a whole, and not just merely their effects on consumers' pocketbooks. No one concerned with antitrust policy should stand idly by if industry consolidation jeopardizes the vital privacy interests of our citizens so essential to our democracy.[14]

A variation of this approach can be found in Frank Pasquale's work, where he argues that dominant general-purpose search engines (i.e. Google) are essential facilities to society due to their cultural and political impact.[15] He thinks this is a strong rationale for government regulation,

---

[14] Sen. Kohl, *supra* note 3, at .

[15] *See* Frank Pasquale, *Dominant Search Engines: An Essential Cultural & Political Facility*, *in* THE NEXT DIGITAL DECADE: ESSAYS ON THE FUTURE OF THE INTERNET 401-18 (2010).

even beyond antitrust, in order to protect the interests of users, including privacy.[16] This big-is-bad approach no longer has a lot of persuasive effect in antitrust jurisprudence. The consumer welfare standard and its focus on competition have replaced the focus on protecting smaller competitors from those bigger than them.

The undue concentration of power approach focuses on the size of companies that gain access to private data and argue this is bad for the economy or society at large. From an economic point of view, this is an interjection of the bad economics of the Populist school that dominated antitrust thinking before the Chicago school revolution and its advanced models of consumer welfare.

Brad Smith, Microsoft's general counsel, has suggested that

> Given the nature and economics of online advertising, this concentration of user information means that no other company will be able to target ads as profitably. It will substantially reduce the ability of others to compete.[17]

This is the "big is bad" argument, with specific reference to the online world. However, it doesn't seem a cognizable harm that a single company might have a concentration of user information absent a claim that a) this information is rivalrous (it is not, and as most online searchers multi-home, many search products may simultaneously amass similar information about their customers), b) indispensible (essential facilities claims are strongly disfavored in US jurisprudence, and it is not clear that any particular collection of information is essential to competition in online advertising markets), and c) likely to be abused at scale (of which there is no evidence).

It is important to remember that the fact that there *can be harms* in the privacy area says nothing about the ability or incentive of a larger firm to engage in this type of harm. Small firms can degrade privacy protections as easily as big firms; the fact of its "bigness" has no obvious logical connection to a firm's ability or incentive to degrade privacy.

C. Exploitation/Facilitation of Price Discrimination

This approach is really two related arguments put forward by Nathan Newman in a recent law review article, focusing primarily on establishing an antitrust case against Google. The exploi-

---

[16] Pasquale, *supra* note 3; *see also* Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009 (2013).

[17] Smith, *supra* note 5.

tation approach focuses on the losses to consumers from Google's harvesting their data. Drawing on Joseph Stiglitz's work on information asymmetries, he argues that Google acts as a digital sharecropper, exploiting the value of personal data of its users, who systematically undervalue this data, while overvaluing the benefits of Google's services.[18] A second argument he advances is that Google facilitates price discrimination and the "tawdry side of capitalism" through its comprehensive data tracking on behalf of its advertisers.[19] He argues the harms from price discrimination and resulting socio-economic inequality are cognizable for antitrust purposes.[20]

The main problem with this theory, which will be addressed in more detail below, is whether these harms are really *antitrust* harms. While Newman has thought out his preferred remedies in detail,[21] many are not related to antitrust at all. Not all social problems are best handled by antitrust, even if they can be established, and as Newman's own argument shows, many of the harms he is concerned about have been handled under current law without extending antitrust's domain.

D. Foreclosure of Access to Data

The foreclosure of access to data argument may have been first forwarded by Microsoft during the Google-DoubleClick merger,[22] but it also received attention from Pamela Jones Harbour in her dissent from that case,[23] and a later law review article she co-authored.[24] A few other scholars also thought this could be an area where privacy concerns may come into play—

---

[18] *See* Newman, *The Costs of Lost Privacy*, *supra* note 4, at 11-19. *See also* Ryan Calo, *Digital Market Manipulation* (University of Washington School of Law Legal Studies Research Paper No. 2013-27, Aug. 15, 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309703 (arguing a similar theme using behavioral economics).

[19] *See Newman*, *The Costs of Lost Privacy*, *supra* note 4, at 36-46.

[20] *Id.* at 47 ("In measuring consumer harm, then, it is therefore the broad financial losses to consumer welfare facilitated by lost privacy and Google's data mining efforts, including the predatory behavioral targeting of users provided by Google based on its control of user data, that should be a prime focus for investigation by antitrust regulators and legislative leaders. Much of this is no doubt in the day-to-day price discrimination encouraged for businesses using online advertising but a significant fraction is also from companies engaged in unethical to illegal activities facilitated by the company.").

[21] *See* Newman, *Search*, *supra* note 5, at 62-69.

[22] *See* Smith, *supra* note 5.

[23] *See* Dissenting Statement of Commissioner Pamela Jones Harbour, Google/DoubleClick, FTC File No. 071-0170, at 5-8 (Dec. 20, 2007), *available at* http://www.ftc.gov/os/caselist/0710170/071220harbour.pdf.

[24] Harbour & Koslov, *supra* note 5, at 773-74, 783-87.

usually as part of a broader argument against Google or other alleged Internet monopolies.[25] This argument is based on the idea that either a monopolist has—or a merger could create—the ability to foreclose access to private data of consumers, making others unable to compete successfully in the marketplace for behavioral advertising.

The foreclosure of access approach is an unusual one from a privacy perspective. The theory is that one company or group of companies has too much consumer data available to them and this creates a barrier to entry or other competitive harm by preventing others from getting into the data collection and use business.

E. Privacy as Nonprice Competition

The privacy as nonprice competition approach is probably the most robust theory of privacy in antitrust analysis. The argument is a simple syllogism: (1) price is not the only way businesses compete, and antitrust jurisprudence recognizes nonprice competition; (2) privacy is an important source of nonprice competition; (3) reductions in nonprice competition due to a merger (or perhaps due to exclusionary acts) are actionable under antitrust law; (C) therefore, reductions in privacy due to a merger should be cognizable harms under antitrust law.[26] The obvious problem is *how* to analyze (and quantify) privacy concerns within antitrust, even accepting this basic argument.

Newman connects this argument to the foreclosure of access to data argument, adding detail to the outline Swire started. Newman argues that Google has monopoly control over data that cannot be overcome by market forces.[27] As a result of the superior data at its disposal through its multiple avenues of data collection,[28] and *not* through superior innovation in its search algorithm,[29] Google offers much greater return for advertisers than alternative search engines.[30] As a result, it lacks incentive to compete on privacy grounds.[31]

---

[25] *Id.* at 783-87; *see also* Bauer, *supra* note 8, at 770-72.

[26] Swire, *supra* note 1, at 4-6. *See also* Newman, *Search*, *supra* note 5, at 62-69 (arguing that antitrust remedies are necessary to reduce Google's market power so that they have to compete on privacy grounds).

[27] Newman, *Search*, *supra* note 5, at 15-17, 70-73.

[28] *Id.* at 28-33.

[29] *Id.* at 36.

[30] *Id.* at 24-28.

[31] *Id.* at 28, 73.

It is plausible that this approach may represent the *only* way to effectively incorporate privacy into antitrust analysis: that is, the foreclosure to access argument isn't really about privacy; it's about data as a good or input. What remains resolutely unclear, however, is how having a *larger* amount of data could reduce nonprice privacy competition.

F. Skeptics

There have been skeptics of the above approaches incorporating privacy into antitrust analysis. One criticism is that advocates downplay the beneficial uses of data to consumers.[32] Another is that there are First Amendment concerns to applying antitrust law to the collection and use of data.[33] A third is that consumers have different subjective preferences for privacy and should not have the preferences of regulators imposed upon them.[34] Skeptics point out that privacy concerns fit uncomfortably into antitrust analysis.[35]

II. The Difficulties of Applying Privacy in Antitrust Analysis

Not all of the above approaches are tethered to modern antitrust law and the consumer welfare standard. The privacy as human right approach is essentially a standard-less interjection of a non-contestable theory of privacy into antitrust analysis. The undue concentration of economic power approach can be dismissed as inconsistent with the purpose of antitrust law as recognized by the courts and competition agencies since the so-called Chicago Revolution. Ignoring the skeptics since they are fellow critics, this leaves exploitation/facilitation of price discrimination, foreclosure of access to data, and privacy as nonprice competition approaches. Below, we discuss in more detail why these approaches fall short.

The first problem is that it is very difficult to operationalize "privacy." In Part II.A, we discuss the law and economics of nonprice characteristics to try to determine how privacy can be analyzed, accepting that it is a product characteristic on which companies may compete. The second problem is market definition. In Part II.B, we analyze the market for data proposed by Harbour and Koslov, suggesting that their approach is inadequate. The third problem is competitive injury. In Part II.C, we will consider the strength of claims by Newman and others that Google has used "bad acts" to harm competition. The final problem is remedies. In Part II.D,

---

[32] Cooper, *supra* note 7, at 7-10.

[33] *Id.* at 10-15.

[34] *Id.* at 15-18.

[35] *See* Grunes, *supra* note 7, at 1111-14.

we will describe the difficulties for courts and agencies to fashion and enforce remedies, especially those proposed by Newman, to alleviate the asserted privacy harms.

A. Operationalizing Privacy - How Do We Analyze Nonprice Effects?

The most straightforward antitrust approach proposed by privacy advocates is privacy as nonprice competition – product quality competition.

> In brief, privacy harms can reduce *consumer welfare*, which is a principal goal of modern antitrust analysis. In addition, privacy harms can lead to a reduction in the *quality of a good or service*, which is a standard category of harm that results from market power. Where these sorts of harms exist, it is a normal part of antitrust analysis to assess such harms and seek to minimize them.[36]

The difficulty with this approach is that it is not operationalizable, at least not in the fashion advocates suggest.

Nonprice effects are difficult to incorporate into effective economic analysis. They are difficult to quantify, of course, and they may be incommensurable with the economic effects against which they must be weighed. At the same time, these effects are likely to be speculative, highly fact-dependent, and of ambiguous character. Perhaps most important, that one can *identify* a product characteristic neither means that it is a salient attribute of product *quality* to the relevant (marginal) consumers, nor that diminishing it will help a manufacturer or seller realize supra-competitive returns.

Nevertheless, for some nonprice attributes competitive effects analysis may be appropriate, as the Horizontal Merger Guidelines have long recognized:

> Enhanced market power can also be manifested in non-price terms and conditions that adversely affect customers, including reduced product quality, reduced product variety, reduced service, or diminished innovation. Such non-price effects may coexist with price effects, or can arise in their absence.[37]

> The unifying theme of the Guidelines is that mergers should not be permitted to create or enhance market power or to facilitate its exercise. Market power to a seller is the ability profitably to maintain prices above competitive levels for a significant period of time. . . . Sellers with market power also may lessen

---

[36] Swire, *supra* note 1.

[37] 2010 Merger Guidelines, sec. 1.

> competition on dimensions other than price, such as product quality, service, or innovation.[38]

The problem, as noted, is operationalizing this dynamic. Some nonprice effects may indeed not show up in a price analysis, but some also will. Even a monopolist faces demand-side limits on its pricing freedom, and some degradations of quality will be reflected in lower prices (even for a monopolist). It is unclear how or whether, even if a reduction in product quality might be identified, it can be quantified, and its effect separated from simultaneous price effects.

At the same time, and of particular importance to assessing the effect of possible changes in the use of data that are implemented in high-tech markets, or to assessing the net effect of agglomerations of data via merger (as in Google/DoubleClick), is the fact that such effects may arise simultaneously with *other* nonprice effects cutting in a different direction – most notably innovation, where new uses of data or the availability of new data sets may enable innovative products or business models.

This latter point is particularly important. As Jones and Williams have shown, the social benefits of R&D are significantly larger than the internalized, private benefits.[39] As a consequence, competitive analysis will almost certainly miss substantial and important benefits that won't be reflected in price (or product quality) in narrowly-defined markets.[40] And this almost certainly understates the social effect given the extent to which measurement of the dynamic, long-term benefits of innovation are difficult to identify and measure.

In the merger context (where most of the concern about privacy-as-product-quality have been raised), one concern is that the accumulation of "too much" information about too many con-

---

[38] 1997 Merger Guidelines, sec. 0.1 & note 6.

[39] Charles I. Jones & John C. Williams, *Measuring the Social Return to R&D*, 113 Q. J. ECON. 1119 (1998) (estimating that the social return to R&D investment far exceeds the private return, meaning existing incentives for innovation are already lower than optimal).

[40] In other words, the *Philadelphia National Bank* limit on consideration of out of market efficiencies ensures that innovation benefits that extend beyond the immediate market will be discounted. *See* United States v. Philadelphia National Bank, 374 U.S. 321 (1963). *See also* Joshua D. Wright, *Comment on the Proposed Update on the Horizontal Merger Guidelines: Accounting for Out-of-Market Efficiencies*, George Mason University Law & Economics Research Paper 10-38 (May 2010), *available at* http://www.law.gmu.edu/assets/files/publications/working_papers/1038CommentontheProposedUpdate.pdf. ("This 'out of market' efficiency problem obviously does not originate with the new HMGs, nor with the HMGs at all. The cause of the problem is *Philadelphia National Bank*.").

sumers' is itself (or perhaps will inevitably lead to) a degradation of quality affecting the merging parties' products.

But that "problem" is almost certainly fully internalized by individual consumers. Consumers, with the assistance of consumer protection agencies like the FTC itself, are generally able to assess the risks of disclosure or other misuse of their information, and to assess the costs to themselves. It is difficult to see why a company's mere possession of private information *about other people* is of much concern to any individual consumer. For each consumer, the "problem" of a large concentration of information being accumulated in a single company is seemingly insignificant.

At the same time, however, specific privacy policies that may affect the company's treatment of the consumer's own, specific information may be relevant. Concentration, then—control over information collected from a particularly large group of consumers, for example—is not likely a significant harm. At the same time, however, where consumers are paying a zero price (as search engine users and advertising consumers do in the Google case), nonprice competition, including over privacy policies, may be the only source of cognizable effects.

But in that case it must still be shown that a monopolist would have the ability and incentive (and, in the case of a merger, that they would be merger-specific) to curtail privacy protections as a means of exercising its monopoly power.

In the normal case, a monopolistic firm has an incentive to degrade quality because it saves money by so doing and the demand elasticity is smaller for downward adjustments in quality than it is for corresponding increases in price. But in the case of privacy protections, where, for example, one "harm" might be the maintenance of personal information on a firm's servers for extended periods without deletion, it would seem that a firm might incur *more* cost in degrading (storing information) than in maintaining (deleting cumbersome information from limited storage space) privacy.

Moreover, there is an important definitional question concerning exactly what "harm" is in this context. The problem is that privacy "harms" are not simply transfers from consumers to producers creating the famous deadweight loss of antitrust textbooks. Rather, the collection and use of larger amounts of information by a company like Google has the ability to *improve the quality* of Google's product. And antitrust injury is not often triggered because a merger might have the effect of *improving* product quality and *decreasing* price.

Similarly, the problem with claims that concentration will lead to a "less-privacy-protective structure" for online activity is that it is analytically empty. One must make out a case, at minimum, that a move to this sort of structure would reward the monopolist in some way, either

by reducing its costs or by increasing revenue from some other source. Absent a coordinated effects argument (which has not to our knowledge been raised), concentration alone is insufficient; unilateral effects must be shown for a merger to be anticompetitive.

In short, proponents of the theory of product-quality harm from monopolization of data need to make out a case for why the feared privacy degradation would occur at all, and this they have not done.

Perhaps the most significant implementation of the nonprice competition approach is the "consumer choice" literature – a literature almost exclusively developed by two scholars (Robert Lande and Neil Averitt) and not generally accepted by either mainstream scholars or the courts.[41] In fact, Professor Lande has drawn the connection between consumer choice and privacy directly, noting that "consumers also want an optimal level of variety, innovation, quality, and other forms of nonprice competition. Including privacy protection."[42]

The basic consumer choice argument is that reductions in choice—in part determined by constrained nonprice variation—should be a cognizable antitrust harm.

Applied to data and privacy, the argument is that market power over data reduces incentives to compete on this dimension, giving rise to, for example, insufficiently privacy-protective products and business models.

The connection with "reduced" privacy protections as a "bad" is clear, although the argument doesn't necessarily turn on a trend toward "degraded" privacy but rather simply a reduction in options.

This distinction, however, begins to point up the difficulty in applying a nonprice competition/consumer choice approach to privacy. As Wright and Ginsburg note,

> If the consumer choice standard were no more than an evidence-based approach to incorporating nonprice competition into the traditional welfare standard, it would be unobjectionable. Averitt and Lande, however, clearly contemplate a departure from the welfare standard in favor of a strong presumption of illegality for any business conduct that reduces the number of choices available to consumers. The flaw in this approach is that **both eco-**

[41] *See, e.g.,* Brantley v. NBCUniversal Inc., et al., 675 F.3d 1192, 1202 (9th Cir. 2012) ("[A]llegations that an agreement has the effect of reducing consumers' choices or increasing prices to consumers does not sufficiently allege an injury to competition. Both effects are fully consistent with a free, competitive market.").

[42] Robert H. Lande, *The Microsoft-Yahoo Merger: Yes, Privacy is an Antitrust Concern*, FTC WATCH, Feb. 25, 2008 at 1.

> **nomic theory and empirical evidence are replete with examples of business conduct that simultaneously reduces choice and increases welfare in the form of lower prices, increased innovation, or higher quality products and services.**[43]

This criticism applies in particular to reductions in choice arising from alleged reductions in nonprice competition from data uses. Almost by definition innovative uses of data can be tarred with the "reduced privacy" epithet, as every experiment with a new use of data or the collection of a new category of data likely entails a reduction in "privacy" relative to the *status quo*. The relevant consideration, as Wright and Ginsburg suggest, is whether such a change, even if it does entail a reduction in choice or objective product quality along one dimension, is on net welfare increasing given the increased innovation or other positive characteristic it may involve. As James Cooper notes, "antitrust has no solicitude for marketplace behavior that does not pose a threat to competition, irrespective of its effect on consumer privacy."[44]

Unfortunately for proponents of a nonprice competition theory of privacy and antitrust, not only is there no obvious reason why monopolists would have an incentive to degrade privacy, there is also no necessary connection between degraded privacy and anticompetitive outcomes.

B. Market Definition - What is a Market for Data?

Harbour and Koslov suggest defining the relevant market in data/privacy cases as the data market in cyberspace or online data used for behavioral advertising.[45] In effect, Harbour and Koslov describe a market in data itself: "markets for data, separate and apart from markets for the services fueled by these data. Data market definition would reflect the distinction between data collection at one point in time and expanded data usage at some later date."[46]

The problem is that this conception of the market is too broad to be meaningful or useful. Sure, the participants all have something in common, but are the uses of the data related enough to all be competitors? Do users of search data, retail data, grocery data, entertainment data, political data, social networking data, etc. really all compete in the same market? There are bene-

---

[43] Joshua D. Wright & Douglas H. Ginsburg, *The Goals of Antitrust: Welfare Trumps Choice*, 81 FORDHAM L. REV. 2405 (2013) (emphasis added).

[44] Cooper, *supra* note 7, at 6.

[45] Harbour & Koslov, *supra* note 5, at 783-85.

[46] Id.

ficial crossover uses, but does a grocery chain compete with Nike for data on women's shoes enough to consider them competitors?

Even if the market is simply "data," regardless of its use, there is little reason to think that a few major players control the market. There are many ways for competitors to get competitive datasets; Countless websites and services collect information. Google may be the dominant search engine, but people do much more than search on the Internet. Think of the quality and quantity of data Amazon, ESPN, Netflix, WebMD, Washington Post, Kayak, Twitter, etc. can collect. Then consider all of the non-web data that is collected: reward cards for every sort of store, retail purchases, public information, consumer feedback and surveys, etc.

At the same time, narrower markets may not make much sense, either. In the main, data is "non-rivalrous." While this is not always true—certainly some data sets may be entirely proprietary, based on information not otherwise accessible, and non-replicable—generally there are many sources of data for many uses, and it is difficult to exclude other firms from access to substitute data. In other words, the data themselves are generally only valuable to the extent they describe some underlying consumer characteristics, and these characteristics can be described in many different ways, with data collected from a range of sources, minimizing the true "monopoly" of any particular set of data.

To be sure, one can imagine *Kodak*-like situations where data wholly internal to a particular firm is "essential" and otherwise unavailable to firms in ancillary markets. But how likely is this? As Steve Salop has explained, discussing (favorably) the analysis in *Kodak*,

> The plaintiffs would first need to demonstrate that Kodak had the power to exclude its competitors. If the ISOs were able to find equally good alternative sources of equally good parts after Kodak's change in conduct, then Kodak's alleged anticompetitive strategy would fail. Second, the plaintiffs would need to demonstrate that consumers were injured. If consumers could substitute equally efficient self-service or could make an even-up trade for alternative equipment, they would not have been injured by the refusal to deal and again Kodak's alleged anticompetitive strategy would fail. In that case, Kodak would not have power over price.[47]

To prevail on such a basis with respect to, say, a hypothetical data monopolization case against Google, a plaintiff would have to show that competing platforms were unable to find equally

[47] Steven C. Salop, The First Principles Approach to Antitrust, Kodak, and Antitrust at the Millennium, 68 Antitrust L.J. 187, 192 (2000).

good, alternative sources of data. But think Facebook, Amazon, Twitter, Yahoo/Bing, Acxiom, Experian, and the like. Alternative sources abound, even if they aren't "search" data. In such a case, narrowing the market to "search data" would seem inappropriate. Depending whom you ask, data in the US alone is a $300 million a year or so business, with 3 million employees. That's a lot of resources offering something that allegedly only Google has. There are multiple sources for the same or equivalent data precisely because most data is built on observed behavior, and many firms may observe behavior simultaneously. Whether these data are "search" data or otherwise is likely not antitrust-relevant.

And even those data sources that are "closed" and proprietary aren't really — as they are all trying to get at the same underlying characteristics of the consumers they describe: the fact that Facebook has data no one else has does not mean that Facebook is the only site that knows things about its users that are relevant to advertisers.

Meanwhile, some assessments of injury in the privacy context turn on improperly *narrow* market definitions based on consumer attributes. For example, Professor Swire informs us that some people fall into a "high privacy concern" category and yet others a "medium concern category."[48] He goes on to claim that

> For these individuals, their consumer preferences are subject to harm if standard online surfing shifts to a less privacy-protective structure due to a merger or dominant firm behavior. In essence, consumers "pay" more for a good if greater privacy intrusions are contrary to their preferences. Under standard economic analysis, and standard antitrust analysis, harm to consumer preferences should be part of the regulatory homework for the competition agencies—such harms should be considered along with other harms and benefits from a proposed merger.[49]

It may be correct that some consumers prefer more privacy protection online. But where these are, by definition, particularly sensitive consumers, it is a mistake to give the harms incurred by them too much weight – particularly in merger analysis where such consumers are certainly infra-marginal, and thus irrelevant to an appropriate assessment of the proper market.

---

[48] Cite Swire FTC testimony, *citing* Ponnurangam Kumaraguru & Lorrie Faith Cranor, "Privacy Indexes: A Survey of Westin's Studies," (2005), available at http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf.

[49] Id.

In other words, identifying effects on particularly sensitive consumers may result in overly-narrow market definitions of the "strange red-haired, bearded, one-eyed man-with-a-limp" variety.[50]

1. The Data Market

What are "market shares" on data? Who has data, and how do they use it? Do "data monopolists" sell or otherwise make data available? What do companies do with their data?

According to the privacy advocacy group Abine, there are "[m]ore than 200 data collection companies and ad networks [using] approximately 600 different tracking technologies to gather and sell information on people's web habits."[51] These companies include ad networks or exchanges, data brokers, retargeters, ad or data buyers, analytics or measurement companies, ad delivery and operations groups, publishers, and other assorted groups using web tools or widgets. On top of these online groups, there are offline data collectors and analyzers as well. All would have to be included in any possible market for data as a whole.

But who benefits from the data market? Consumers benefit because they see ads better targeted to them about products they may want. More advertising revenue allows sites, especially smaller ones, to remain profitable while charging no fee to consumers. Consumers also get the benefit of better tailored search engines, social networks, product suggestions, and online mapping.

Advertisers benefit because of greater exposure to the right viewers and less waste on uninterested viewers. This allows them to spend less on advertising, freeing up more resources to go toward product improvement and price reductions. Additionally, smaller and newer firms can afford to advertise, increasing their ability to compete with incumbents.

Additionally, any company that collects data benefits because there is now a wider market for something they possess. Previously, the demand for their data may have been tiny or non-existent.

---

[50] United States v. Grinnell, 384 U.S. 563, 590-91 (1966) (Fortas, J. dissenting).

[51] www.abine.com.

2. *Responding to Foreclosure of Access to Data Approach*

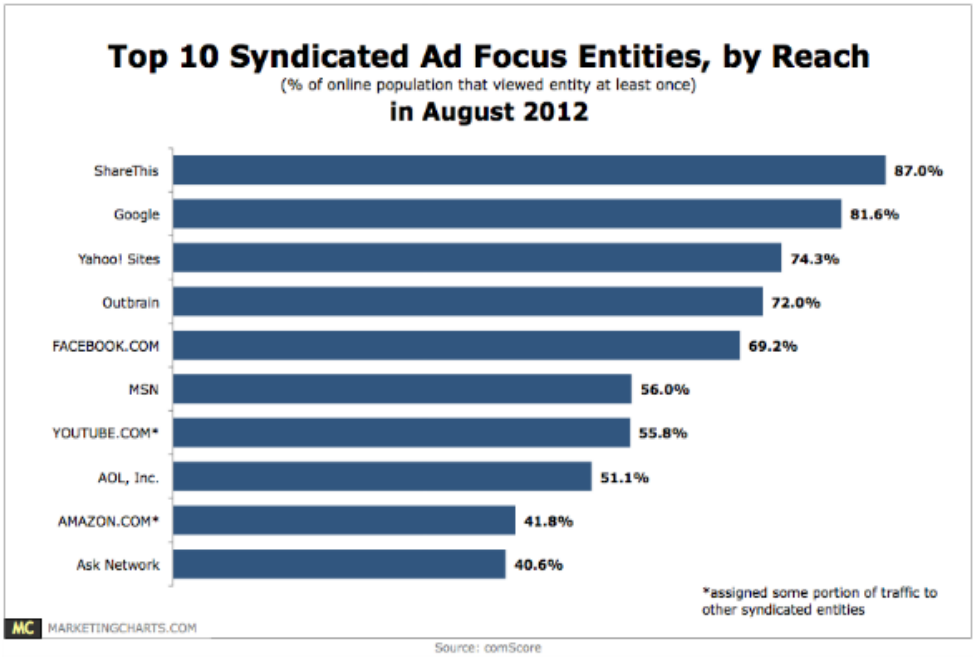
One major problem with this theory is that there are none of the classic signs of exclusion or foreclosure of access. There are no signs of refusal to deal agreements. Also, it is impossible to buy up all of the data, a necessary input in the business, because ownership is non-rivalrous.

A related argument is that the market is subject to network effects, making new entry very difficult. Those putting the argument forward point to specific products where the effect appears, such as search engines and social networks where having more users improves the product, thus drawing more users.

But how do network effects apply in a market definition of simply data in itself, the one Harbour and Koslov suggest? Is the network effect in the data market: the more data you collect, the more you can sell each unit for, allowing you to collect more data? A sort of an increasing marginal utility, at least up to a point? Or does collecting some data make collecting more even easier?

The barriers to entry are not in any way due to conduct by the incumbent. In fact, the incumbent almost certainly had to go through the same process and overcome the same barriers. The first two barriers are time and money. A competitor can either buy the data it desires, which may be expensive, or it can collect data itself and build databases over time. The third barrier is the skill it takes to make productive uses of the data. None of this indicates, though, that there is foreclosure of access or exclusionary conduct.

Plus, evidence from the advertising networks market suggests a lack of any dominant firm in terms of penetration rates. Thus, it seems unlikely that any network has data to which others do not have access. For instance, this 2012 chart from Comscore shows several networks have high penetration rates, suggesting these ad networks are competing for many of the same eyeballs and gaining access to much of the same data:



But, this whole approach misses the point. It's not just all about having more data. What makes Google's search better is likely attributable largely to its algorithms, not just its access to data. Something had to differentiate it to initiate the network effect and it was the algorithm, not data. The same goes for Facebook. It became dominant not by having all sorts of data, but by creating a better product that drew users. Did Facebook's most plausible competitor in recent memory, Google+, fail to gain market share because it lacked data? Not likely.

One point, noted by Commissioner Brill, is that the FTC's consumer protection mission clashes with its antitrust mission when data is considered a barrier to entry.[52] The barrier to entry argument is that if having more data presents a barrier to entry, then competitors need to have enough data to compete. But that presents consumer protection problems if the concern is about data collection in itself. If the consumer protection mission drives policy too much, new rules that limit the purchase or sale of data (perhaps only allowing data use for purpose it was collected) could create a significant barrier to entry in the data market. All data would have to be collected organically by the service provider. That could greatly increase the cost, in terms of time, of becoming a viable competitor to incumbents.

So do we need to alter one of these? Should the consumer protection harm be something other than mere collection/storage, like leaks or improper uses? Should the barrier to entry argu-

[52] CITE

ment be abandoned because it encourages greater collection or forced sharing, as in an essential facilities case?

C. Competitive Injury - What is the Harm to Competition?

If nonprice effects cannot be relied upon to establish competitive injury (as explained above), then what can be the basis for incorporating privacy concerns into antitrust? The best attempt probably comes from Nathan Newman's multi-faceted foray. One of Newman's arguments is that the harm to competition is the exploitation of users due to an information asymmetry: consumers undervalue their data and overestimate the benefits received from Google, while Google knows full well the value of that data to them and their advertisers.[53] He points to the value extracted by Google and the advertisers which rely on it to argue there is a competitive injury to consumers.[54] Newman also argues that Google's data collection facilitates price discrimination[55] and other harms he describes as the "tawdry side of capitalism."[56]

This analysis suffers from at least three fundamental flaws. One, Newman's information asymmetry story breaks down upon further investigation. Newman misunderstands the economic relationship between Google, users, and advertisers, leading him to see exploitation where there is beneficial exchange. Two, price discrimination is not generally considered an antitrust harm under modern jurisprudence and the highly discredited Robinson-Patman Act only applies in very limited circumstances. Three, many of the other harms he alleges that Google facilitates are already dealt with by law other than antitrust.

1. Information Asymmetry Leading to Exploitation

Newman's information asymmetry analysis is predicated on the idea that Google's users undervalue their data and overvalue the benefits of Google's services. Newman draws on Joseph Stiglitz and argues that Google is able to maintain its monopoly position by extracting data from its users for too low of a price. He points to a story that suggests the data of an individual could be worth as much as $5,000 to Google and its advertisers.[57]

---

[53] *See* Newman, *Costs of Lost Privacy*, *supra* note 4, at 11-20.

[54] *Id.* at 22.

[55] *Id.* at 23-27.

[56] *Id.* at 36-46 (alleging Google's data collection facilitates racial profiling, the subprime mortgage crisis, financial exploitation, and illegal drug sales).

[57] *Id.* at 22 (citing Quentin Fottrell, *Who Would Pay $5,000 to Use Google? (You)*, SMARTMONEY.COM (Jan 25, 2012), http://blogs.smartmoney.com/advice/2012/01/25/who-would-pay-5000-to-use-google-you/ ("'Their entire

Newman's information asymmetry story has superficial plausibility. Consumers in real world markets never have the perfect information that certain models presume. But, businesses also fail to have perfect information, and this fact is glossed over by Newman. The market process is useful because it incentivizes participants to gain information because the costs and benefits of decisions are borne by each person.[58]

Increasingly, polls show users are growing less concerned about the tradeoff inherent in the Google "transaction": data for advertising in exchange for un-priced search, email, etc.[59] This may be consistent with the process of society adapting to new innovations after initial reluctance over issues of creepiness, that has happened after techno-panics several times in American history.[60] Now, consumers may prefer an exchange in which they get all the benefits with no costs, but this does not mean they don't understand the exchange taking place. Regardless, polls are less reliable than revealed preferences in the marketplace to inform us about customer preferences.[61] On the other hand, economic experiments suggest that most consumers place a low price on privacy protection—as the market results reveal.[62] While Newman describes these market results as exploitation, they may actually be real consumer preferences in light of the opportunity costs.

---

market cap is related to how much data is being collected and used,' says Jules Polonetsky, director of the Future of Privacy Forum, a Washington, D.C.-based think-tank.")). Despite the grabbing headline, the value of an average user's data is likely far less than that amount. *See* Ben Sperry, *Google: Great Deal or Greatest Deal*, Truth on the Market (Oct. 11, 2013), http://truthonthemarket.com/2013/10/11/google-great-deal-or-greatest-deal/.

[58] *See* F. A. Hayek, *The Use of Knowledge in Society*, 35 AM. ECON. REV. 519 (1945).

[59] *Cf. Poll: Consumers concerned about internet privacy*, CONSUMERS UNION (Sept. 25, 2008), http://consumersunion.org/news/poll-consumers-concerned-about-internet-privacy/ (finding "72 percent are concerned that their online behaviors were being tracked and profiled by companies"); *Consumer Comments to the NTIA on "Multistakeholder Process To Develop Consumer Data Privacy Codes of Conduct"*, CONSUMERS UNION (Apr. 2, 2012), http://consumersunion.org/research/consumer-comments-to-the-national-telecommunications-and-information-administration-on-multistakeholder-process-to-develop-consumer-data-privacy-codes-of-conduct/ (finding 44% of consumers are concerned with "Advertisers targeting you with personalized ads by collecting data about your interests and purchases online").

[60] *See* Adam Thierer, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 MINN. J. L. SCI. & TECH. 309 (2013), *available at* http://purl.umn.edu/144225.

[61] *See* Berin Szoka, *Privacy Polls v. Real World Tradeoffs*, 5 PROGRESS & FREEDOM FOUND., vol. 10, Nov. 2009, *available at* http://www.pff.org/issues-pubs/ps/2009/pdf/ps5.10-privacy-polls-tradeoffs.pdf.

[62] *See, e.g.*, Alastair R. Beresford, Dorothea Kübler, Sören Preibusch, *Unwillingness to Pay for Privacy: A Field Experiment* (SFB 649 Discussion Paper 2011-010, 2011), *available at* http://edoc.hu-berlin.de/series/sfb-649-papers/2011-10/PDF/10.pdf; Jens Grossklags & Alessandro Acquisti, *When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information*, *in* PROCEEDINGS OF SIXTH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (2007), *available at* http://weis2007.econinfosec.org/papers/66.pdf.

Newman's story evinces a misunderstanding of how the market process works here. He dismisses the idea that this is a double-sided market, stating that while advertisers need consumers, the consumers do not need advertisers.[63] Perhaps consumers don't need advertisers if they wish to pay for search and all of the other services Google provides, but if they want to continue to have these services for free, consumers do need advertisers. For instance, specialized legal search engines like Westlaw and Lexis do little tracking and are not ad-supported. But, the price for using these services are considerably higher than zero:[64]

2010 Westlaw Classic Retail Costs for Law Firms

File/Service	Hourly (per minute)	Transactional (per search)
All Federal Cases	$19.05	
Ohio State and Federal Cases	$23.08	
Sixth Circuit Cases	$8.60	
All Ohio Cases	$8.60	
Get a Document/Find		$14.00 (primary) $24.00 (secondary)
KeyCite		$6.25

Costs have increased since 2010.

Google does not price per search or require a subscription to find business and legal information available from services like Bloomberg, which has a "low" flat rate of $450 per month per user.[65]

The ad-supported system provides search to the masses, giving them access to a universe of information, including many of the federal cases previously available for search only through Westlaw and Lexis, all for the price of $0. It is hard to quantify just how valuable this is to users, but it seems considerable. Reducing transaction costs by an astronomical amount has occurred

---

[63] Newman, *Search*, *supra* note 5, at 8 ("Google's search users don't need advertisers, but advertisers need users.").

[64] *Cost Effective Legal Research*, CLEVELAND-MARSHALL COLLEGE OF LAW LIBRARY (Sept. 5, 2013), http://guides.law.csuohio.edu/wexis_pricing.

[65] Robert Ambrogi, *What Do You Pay for Westlaw or LexisNexis?*, LawSites (Jul. 13, 2011), http://www.lawsitesblog.com/2011/07/what-do-you-pay-for-westlaw-or-lexisnexis.html.

as a result of search engines like Google. And this doesn't even include all of its other services, like Gmail, Google Docs, Google Calendar, etc. For instance, one calculator suggests that the value of Gmail to the average user is $3,588.85.[66]

By comparison, most users are not likely worth anything approaching that much to Google. In 2012, one person calculated that market value per user to Google was $221.93 and the average revenue per user was $43.16.[67]

But, even this number is misleading. Google makes money by selling access to advertisers, who are willing to buy this because they believe it increases their ability to sell a good or service to consumers. Advertisers only make money, though, if consumers buy their products. So, in the end, the value of the consumers to Google and its advertisers is ultimately dependent on the choice of consumers to buy goods and services. To find the source of Google's power to make money from advertisers, one need only look in the mirror.[68]

While there are alternatives in the marketplace like DuckDuckGo which only serve up contextual ads and do not do the data collection that Google does, the cost to users is less valuable search results.[69] And it is not apparent that consumers prefer the tracking-free experience. Revealed preferences in search and elsewhere suggests the "price" of viewing a targeted ad is a much lower psychic burden for most people than paying even just a few cents per month for an ad-free experience. For instance, consumers almost always choose free apps over the 99 cent alternative without ads.[70]

---

[66] *See, e.g.*, Mike Barton, *How Much is Your Gmail Account Worth?*, Wired (Jul. 25, 2012), http://www.wired.com/2012/07/gmail-account-worth/; Jay Garmon, *What is My Gmail Account Really Worth?*, backupify: The Cloud to Cloud Backup Blog (Jul. 25, 2012), http://blog.backupify.com/2012/07/25/what-is-my-gmail-account-really-worth/. *See also Gmail v. Outlook: The Real Question is Cost*, READY MADE WEB (Jan. 7, 2010), http://readymadeweb.com/2010/01/07/gmail-vs-outlook-the-real-question-is-cost/ (estimating the cost for an on-site server as $25.18 per user per month, compared to the $8.47 for companies using Google's fully Web-based Gmail).

[67] Dan Dzomback, *How Much is a User Worth?*, THE MOTLEY FOOL (Aug. 27, 2012), http://www.fool.com/investing/general/2012/08/27/how-much-is-a-user-worth.aspx.

[68] *See Something Wall Mart This Way Comes*, (Comedy Central television broadcast Nov. 3, 2004) at 19:00, *available at* http://southpark.cc.com/full-episodes/so8e09-something-wall-mart-this-way-comes.

[69] *See, e.g.*, Brian Mayer, *I Used DuckDuckGo for a Week and Had to Switch Back. Here's why.*, BrianMayer (Jun. 28, 2013), http://notes.brianmayer.com/i-used-duckduckgo-for-a-week-and-had-to-switch-back.

[70] Mary Ellen Gordon, *The History of App Pricing, and Why Most Apps are Free*, The Flurry Blog (Jul. 18, 2013), http://blog.flurry.com/bid/99013/The-History-of-App-Pricing-And-Why-Most-Apps-Are-Free.

Contrary to Newman, it is not apparent that consumers undervalue their data or overvalue Google's benefits. The revealed preferences of consumers suggest they are taking advantage of what they perceive to be a good deal. To second guess consumers choices and wish to make them on their behalf is paternalism, dressed up in the guise of a "market failure" that does not exist.

2. Facilitation of Price Discrimination

The second way Newman tries to connect privacy to antitrust injury is his argument that Google's practices facilitate the ability of their advertisers to engage in price discrimination. There are several problems with this argument. First, it is not clear that Google would be the relevant party to sue in an antitrust case based upon price discrimination. Second, antitrust law recognizes that not all price discrimination is anticompetitive. Third, the Robinson-Patman Act would not apply here because its protections do not extend to end consumers like Google's users.

The first point should be quite obvious. Newman has an implicit assumption that Google would be at fault for anticompetitive price discrimination just by collecting data used for profiles relied upon by advertisers and companies that then allegedly engage in price discrimination. If anyone could be sued here, it would be those companies that actually engage in the price discrimination, not Google itself. Newman does not even make an explicit argument about Google colluding with advertisers to engage in price discrimination. Newman's argument about Google's complicity in such schemes may be a reason for ex ante regulation of what data can be collected from or who it can be shared with, but it is not an argument that incorporates privacy into antitrust analysis.

While the first point is more than enough to dispose of Newman's theory as an antitrust matter, further elaboration on the economics of price discrimination will show why it is not even generally condemned in antitrust law as anticompetitive.

Neman makes a plausible sounding argument about the harm of price discrimination. Because Google is able to collect a great deal of data about its users for analysis, businesses could segment groups based on certain characteristics and offer different deals.[71] The resulting price discrimination could lead to many consumers paying more than they would have in the absence of the data provided by Google. Therefore, Newman argues, the data collection by Google facilitates price discrimination that harms consumer welfare. In particular, he notes

[71] *See* Newman, *Costs of Lost Privacy*, *supra* note 4, at 22-27.

that now-Google economist Hal Varian has wrote extensively in his career about the ability of businesses to charge myopic consumers higher in certain instances where such consumers may be identified.[72]

Newman's argument misses a large part of the story, though. The flip side is that price discrimination could have benefits to those who receive *lower* prices from the scheme than they would have in the absence of Google's data collection.[73] If this group is as big as or bigger than the group who pays higher prices, then it is difficult to state the practice leads to a reduction in consumer welfare, even if this can be divorced from total welfare.[74]

Further, his analysis fails to consider the dynamic efficiencies of price discrimination. In a static model of third-degree price discrimination, some buyers receive lower prices (and purchase higher quantities), while other buyers receive higher prices (and purchase lower quantities). Thus, the net impact of price discrimination on output is ambiguous.[75] But, in a dynamic model, price discrimination may often be pro-competitive because the profits provide incentives for entry and allow for additional investments in innovation and increasing product variety, expanding retail outlets, or research and development.[76] Price discrimination may allow for increased competition to all consumers, including previously unreached poorer consumers, a pro-competitive outcome.[77] Contrary to the received wisdom,[78] economists have noticed that price discrimination is present in even competitive markets.[79] For all of his condemnation of neoclassical and Chicago school economics,[80] it is actually Newman that falls into the trap of relying upon an outdated static model in this case.

While Newman focuses on the possible negative effects to one subset of consumers, he ignores the positive effects of businesses being able to expand output by serving previously un-

---

[72] *See id.* at 28-32 (citing Hal Varian, *A Theory of Sales*, 70 AM. ECON. REV. 651 (1980); Alessandro Acquisti and Hal R. Varian, *Conditioning Prices on Purchase History*, 24 MARKETING SCIENCE 367 (2005)).

[73] Newman quickly dismisses this idea as a "hope" that has not come to fruition. *Id.* at 25.

[74] As Newman suggests we do. *See id.* at 31 n.67.

[75] *See, e.g.*, Joshua D. Wright, *Missed Opportunities in* Independent Ink, Cato Supreme Court Rev. 2005-2006, at 348, *available at* http://object.cato.org/sites/cato.org/files/serials/files/supreme-court-review/2006/9/wright.pdf.

[76] *Id.* at 350.

[77] *Id.*

[78] *See* William M. Landes & Richard A. Posner, *Market Power in Antitrust Cases*, 94 HARV. L. REV. 937, 977 (1981).

[79] *See, e.g.*, 70 ANTITRUST L.J. 593 (2003) (symposium articles discussing competitive price discrimination).

[80] *See* Newman, *Costs of Lost Privacy*, *supra* note 4, at 7, 27; Newman, *Search*, *supra* note 5, at 2-4; 47-51; 69-73.

derserved consumers. It is unlikely that a business relying on metrics would want to only serve those who can pay more by charging them a lower price, while charging those who cannot afford it a larger one, as Newman suggests Google's advertisers are doing.[81] If anything, price discrimination would likely promote egalitarian outcomes that Newman desires by allowing companies to offer lower prices to poorer segments of the population which can be identified by data collection and analysis.

In an error cost framework, courts and antitrust regulators should refrain from declaring conduct anticompetitive unless the likelihood of procompetitive outcomes is extremely low.[82] It may be difficult for antitrust regulators to differentiate positive price discrimination from negative price discrimination. Here, it seems unlikely that the price discrimination "facilitated" by Google is anticompetitive. Google analytics is used by lots of businesses, many of which compete with one another in the same markets, to offer the best deal to consumers through targeted advertising. It seems just as, if not more, likely that Google is increasing consumer welfare by helping businesses find consumers interested in their products and serving up more relevant advertisements to those consumers—thus increasing the amount of positive sum transactions overall.

Finally, in his attempt to make price discrimination antitrust-relevant, Newman points to the Robinson-Patman Act, a New Deal-Era amendment to the Clayton Act's prohibitions on price discrimination.[83] Unfortunately for Newman's theory, the Robinson-Patman Act's prohibitions do not extend to price discrimination against end consumers. Newman himself recognizes this fact, and does not offer any argument on how the Act could be used.[84] Further, the Robinson-

---

[81] *See* Newman, *Costs of Lost Privacy*, *supra* note 4, at 25.

[82] Frank H. Easterbrook, *The Limits of Antitrust*, 63 TEX. L. REV. 1 (1984). The error cost model is well-accepted in the antitrust law and economics literature. *See, e.g.*, RICHARD A. POSNER, ANTITRUST LAW, at ix (2nd ed. 2001); C. Frederick Beckner & Steven C. Salop, *Decision Theory and Antitrust Rules*, 67 ANTITRUST L.J. 41 (1999); David S. Evans & A. Jorge Padilla, *Designing Antitrust Rules for Assessing Unilateral Practices: A Neo-Chicago Approach*, 72 U. CHI. L. REV. 73 (2005); Luke Froeb et al., *Vertical antitrust policy as a problem of inference*, 23 INT'L; J. INDUS. ORG. 639 (2005); Keith N. Hylton & Michael Salinger, *Tying Law and Policy: A Decision-Theoretic Approach*, 69 ANTITRUST L.J. 469 (2001); Geoffrey A. Manne & Joshua D. Wright, *Innovation and the Limits of Antitrust*, 6 J. COMPETITION L. & ECON. 153 (2010).

[83] Robinson-Patman Act, 15 U.S.C. § 13 (2012).

[84] *See* Newman, *Costs of Lost Privacy*, *supra* note 4, at 35-36.

Patman Act has fallen into great disrepute because of the outdated economic model it was based upon, leading the Antitrust Modernization Commission to call for its repeal in 2007[85]:

> By broadly discouraging price discounts, the Robinson-Patman Act potentially harms competition and consumers. The goal of the antitrust laws is to protect competition that benefits consumers. The Robinson-Patman Act does not promote competition, however. Instead, the Act protects competitors, often at the expense of competition that otherwise would benefit consumers, thereby producing anticompetitive outcomes. The Act prevents or discourages discounting that could enable retailers to lower prices to consumers. "The chief 'evil' condemned by the Act [is] low prices, not discriminatory prices." The Act thus reflects "faulty economic assumptions" and a significant "misunderstanding of the competitive process."[86]

Newman's valiant attempt to connect privacy to antitrust through the harm of price discrimination is unlikely to be a successful one in front of any court or competition agency.

3. Facilitation of the "Tawdry Side of Capitalism"

Newman's final argument connecting privacy to antitrust is that Google's data collection facilitates discriminatory and exploitative business practices, as well as illegal transactions.[87] The difficulty with this argument, from an antitrust perspective, is that it is completely unrelated to antitrust law. While the harms may be real, this does not make them cognizable by antitrust law. Newman himself recognizes that many of these harms are already been dealt with by marketplace backlashes, or by the FTC through its consumer protection powers, or by statutes shaped to those purposes.[88]

Newman links Google to a variety of ugly practices, such as racial profiling and discrimination,[89] the subprime mortgage crisis,[90] financial exploitation through payday lending,[91] and illegal drug advertising.[92]

---

[85] *See* ANTITRUST MODERNIZATION COMMISSION, REPORT AND RECOMMENDATIONS at iii, 20, 311-32 (Apr. 2007), *available at* http://govinfo.library.unt.edu/amc/report_recommendation/amc_final_report.pdf.

[86] *Id.* at 317 (internal citations omitted).

[87] *See* Newman, *Costs of Lost Privacy*, *supra* note 4, at 36-46; Newman, *Search*, *supra* note 5, at 52-59.

[88] *See* Newman, *Costs of Lost Privacy*, *supra* note 4, at 43 (CFPB rules against abuses by pay-day lenders); *id.* at 45-46 (civil forfeiture agreed to by Google for facilitating illegal pharmaceutical sales); Newman, *Search*, *supra* note 5, at 52-54 (backlash to Google streetview); *id.* at 58-59 (FTC Section 5 action against Google Buzz which ended in consent decree).

[89] Newman, *Costs of Lost Privacy*, *supra* note 4, at 37-40.

Much like the problem of price discrimination, Newman sees fit to attribute harms from advertisers to Google itself. With minor exceptions, the law does not hold data collectors or analysts liable for the uses of information by third parties.

Nonetheless, it is also important to note that most of the examples of harmful business practices Newman decries are already illegal. Steering Hispanics and blacks to more expensive subprime mortgages than whites did lead to a settlement with the DOJ for discriminatory lending.[93] Many of the practices that led to the subprime mortgage crisis were illegal,[94] and others became so.[95] Some subprime mortgages, of course, were not exploitative or illegal at all,[96] and Google should hardly be penalized for facilitating and profiting from them. The same can be said about payday lending and loan modification programs—illegal versions have been shut down, but those which are beneficial to consumers cannot be considered evil to profit from. Finally, Newman details how Google already paid the largest civil forfeiture fine in history for knowingly allowing advertisements of illegal pharmaceuticals on their site.[97]

Antitrust only recognizes harm to competition as injury for its purposes. These harms are dealt with by statutes designed for those purposes. Fears about Google facilitating these harms are likely better handled by extending the reach of those statutes, if necessary and efficient to do so under a cost-benefit analysis, than by the unwieldy application of antitrust law.

D. Remedies - How Can Antitrust Regulators Craft a Remedy?

Another difficulty is that antitrust law does not provide an easy remedy for courts or competition agencies to apply to privacy issues.

Part of the difficulty in understanding the possible remedies is thinking through the actual causes of action plaintiffs could bring even under the theories expounded above. The issue of

---

[90] *Id.* at 40-42.

[91] *Id.* at 42-45.

[92] *Id.* at 45-46.

[93] *See id.* at 39 n.89. *See also* Equal Credit Opportunity Act, 15 U.S.C. § 1691 (2012); Fair Housing Act, 42 U.S.C. § 3605 (2012).

[94] *See, e.g.*, Community Reinvestment Act, 12 U.S.C. § 2901 *et seq.* (2012).

[95] *See* Dodd–Frank Wall Street Reform and Consumer Protection Act, Pub .L. 111–203 (signed into law Jul. 21, 2010) (codified in various places).

[96] *See* Todd J. Zywicki & Joseph D. Adamson, *The Law & Economics of Subprime Lending*, 80 U. COLO. L. REV. 1, 20-23 (2008).

[97] *See* Newman, *Costs of Lost Privacy*, *supra* note 4, at 45-46.

remedies could arise in ways as numerous as the causes of actions in antitrust law itself. It is relatively easy to imagine how courts or regulators could block or attach conditions to mergers which grant a company too large of a share of data or that will substantially reduce competition for privacy protection. But, it is much harder to foresee how a court or competition authority could remedy privacy concerns if they could somehow prove a Section 2 monopolization suit imagined by some scholars.[98]

This can be seen by analyzing the proposal put forward by Nathan Newman, the one advocate antitrust remedies for privacy problems. His proposals suffer from several flaws (some of which he even identifies). The first problem is that many of his proposed remedies are not antitrust remedies at all, but actually consumer protection-oriented or legislative in nature. A second problem is that there are legal and practical barriers to courts and agencies enforcing the proposed remedies. A third is that the remedies may not actually promote greater privacy protection.

Newman's remedies are pretty simple really:

> Broadly, remedies can address Google's dominance in three major ways, separately and in combination: (1) Reduce Google's control of overall user data, (2) Create a real market for user data by empowering users, (3) Impose public interest obligations on Google to restrain damage to consumer welfare.[99]

Newman imagines that these remedies will increase privacy protection for consumers. But, the efficacy and difficulties in applying these remedies, both for legal and practical reasons, are strong reasons not to apply antitrust law to these concerns at all.

The first suggested remedy, and the one most antitrust-relevant, is to reduce Google's control of overall user data, which Newman sees as the source of its anti-competitive behavior:

> There are a number of tools possible for reducing Google's share of user data and advertising online… These include eliminating any contractual limits on advertisers "multi-homing" their advertising campaigns on multiple platforms and eliminating restrictions on software tools to easily manage ad campaigns on multiple platforms. However, unless Google's disproportionate control of user data is reduced, this is unlikely to make any rival search advertising platform economically viable. One option that resembles most traditional anti-

[98] As well as in private plaintiff suits alleging an exclusionary practice by a large data owner somehow hurt competition and/or consumers.

[99] Newman, *Search*, *supra* note 5, at 63.

> trust remedies would be to have Google divest itself of some of the user products, such as Gmail, YouTube, Google Offers, and/or its Android ecosystem, which harvest user data for the company. This would serve the dual purposes of reducing the overall data advantage Google has over existing advertising competitors and it would potentially create additional competitors with a compelling base of user data to compete with Google within the online advertising market. Much of concern about Google's recent integrated privacy policy, both in the United States and by European privacy regulators, was explicitly that rich sources of user data from search would now be combined with data on video viewing habits to create a much more intrusive user profile. Separating these assets into different companies would greatly reduce those privacy concerns by having less integrated profiles of each user in any one hand, while eliminating the dominance Google has in search advertising through its current control of those integrated profiles.[100]

Along the same lines, Newman also suggests that search neutrality be imposed upon Google for its main product of search.[101] In this way, Google's monopoly power over user data, and the loss of privacy which allegedly goes with it, will be reduced.

Remedies like forced sharing of user data with competitors or breaking up Google into constituent parts (search products, email product, YouTube, etc.) will not necessarily lead to greater privacy protection for Internet users. Forcing Google to share data would mean even more entities have access to information that privacy advocates think should be private to begin with. And splitting Google's services up would quite possibly increase competition to "harvest" more personal data from Internet user—a presumably counterproductive result from privacy advocates' point of view. On top of this practical problem, there are legal barriers to the proposed remedy of search neutrality, both under antitrust law and the First Amendment.[102]

The second proposed remedy is to create a market for data. Newman supposes this can occur by imposing Do-Not-Track by default, either by FTC or legislative action.[103] These remedies are

---

[100] *Id.* at 63-64.

[101] *See id.* at 64-65.

[102] Newman recognizes the antitrust limitations, *see id.* at 64-65 n.90, but does not even consider the possibility that the First Amendment may restrict the remedy of search neutrality. *See e.g.*, Eugene Volokh & Donald M. Falk, *Google First Amendment Protection for Search Engine Results*, 8 J.L. ECON. & POL'Y 883 (2012), *available at* http://www2.law.ucla.edu/volokh/searchengine.pdf; Langdon v. Google, Inc., 474 F. Supp. 2d 622, 629–30 (D. Del. 2007); Search King, Inc. v. Google Technology, Inc., No. CIV-02-1457-M, 2003 WL 21464568 (W.D. Okla. May 27, 2003).

[103] Newman, *Search*, *supra* note 5, at 65-67.

themselves recognized to be outside of antitrust's domain, however.[104] The final proposed remedy is along the same lines: Newman encourages regulators to force Google into consent decrees on issues like search neutrality and providing baseline levels of privacy protection.[105] Perhaps Do-Not-Track or baseline privacy protections could come about by a multi-stakeholder process that then could be enforced by the FTC under its Section 5 authority, but using established consumer protection power is different than proposing antitrust law applies.

A good rule of thumb for antitrust law is that if there is no remedy for the harm under the law, then antitrust law really doesn't apply. Newman fails to establish specifically antitrust remedies that do not have practical and legal barriers. But, there is one more significant problem. Newman focuses a great deal on what he sees as under protection of privacy. But the use of antitrust law to create another set of remedies for problems which are better dealt with by other law could actually reduce consumer welfare—the very goal of antitrust law in the first place:

> Under-enforcement or failure to effectively remedy a violation harms consumers through higher prices, decreased quality, and reduced output and innovation. Markets are distorted, victims go uncompensated, and violators reap windfalls. But it would be a mistake to assume that for any particular violation "piling on" more enforcement and more relief is always better -- that somehow taking redundant cracks at remedying an antitrust violation automatically results in a stronger enforcement scheme and, ultimately, in stronger competition.
>
> The greatest danger in over-enforcement of competition laws and over-remedying is that they will retard legitimate, pro-competitive behavior -- that is, reduce the very favored conduct that the laws are intended to encourage and protect. To avoid overwhelming costs and burdens, firms may steer so far clear of potentially questionable conduct that they end up avoiding legitimate behavior that may have benefitted consumers. Piling on multiple layers of enforcement or relief may also provide windfalls to other market participants, which further distorts the market away from what competition itself would create. And, of course, it places unnecessary burdens on enforcement agen-

[104] Newman, *Costs of Lost Privacy*, *supra* note 4, at 48.

[105] Newman, *Search*, *supra* note 5, at 68-69.

> cies, courts, and parties -- costs that ultimately the taxpayers we serve will bear.[106]

As will be detailed below, other remedies do exist—and have been used to varying levels of success. To add antitrust remedies on top of these others may actually over-deter beneficial conduct and leave consumers worse off than if antitrust law did not apply at all.

III. Not All Social Problems Are Amenable to Antitrust Law

As mentioned above, Newman recognized that antitrust may not be the best framework for dealing with privacy issues:

> [B]ecause of the complexity of implementing [antitrust] remedies through agencies and the courts, some reforms might better be implemented through existing powers of the Federal Trade Commission and other agencies. Other measures may call for additional legislation to bring both antitrust and consumer protection laws more explicitly up-to-date to address the broad consumer harm and rising economic inequality stemming from data mining online.[107]

Even without further legislation, current laws, on top of the dynamic marketplace itself, can already significantly deter privacy abuses while still allowing companies to offer consumers the exchange of targeted advertising for free content.

A. Policymakers Should Consider Error-Costs Before Suggesting Changes to Antitrust Law

As explained in this paper, there is no easy way to incorporate privacy into antitrust analysis, and, currently, antitrust law does not do so. The models suggested in the academic literature and in Pamela Jones-Habour's DoubleClick dissent would likely be difficult for agencies and courts to enforce.

Before altering antitrust law by attempting to include privacy in its domain, policymakers should consider the error cost framework. If all of the suggested models would increase the probability of type 1 errors (i.e. false positives where courts and agencies find behavior anti-competitive that is not), then they should not be adopted. Generally, type 2 errors (i.e. false

---

[106] Deborah Platt Majoras, *Antitrust Remedies in the United States: Adhering to Sound Principles in a Multi-Faceted Scheme*, Speech Before the Canadian Bar Association National Law Section (2002), *available at* http://www.justice.gov/atr/public/speeches/200354.htm.

[107] Newman, *Costs of Lost Privacy*, *supra* note 4, at 48.

negatives where courts and agencies find behavior pro-competitive that it not) are overcome in the marketplace due to competition. Profits create incentives for potential competitors to enter and reduce monopoly power. Type 1 errors are not as easy to overcome, as market participants no longer use such practices after such a finding, to the detriment of consumers.

Applying the error-cost framework to the arguments presented on the use of privacy in antitrust analysis suggests that the costs would outweigh the benefits. Proponents have not successfully explained how to incorporate privacy into a nonprice effects analysis, how to understand a market for data, or what is the competitive injury. Until they can do so, it seems like the skeptics have the better argument. There are pro-competitive reasons for the allegedly privacy-invasive practices like data collection, analysis, behavioral advertising, and even price discrimination. While there are theories of how these practices *could* lead to harm, the difficulty of analyzing privacy under an antitrust framework or providing a remedy suggests a different regulatory structure is necessary.

B. Law Already Exists to Deal with Privacy Concerns Outside of Antitrust

The preceding argument does not mean that privacy harms have should have no remedy. While antitrust law's domain should be limited to competitive harms that can only tangentially deal with privacy concerns, consumer protection law and the common law can—and to a large extent already do—reach privacy harms.

1. Section 5

Under Section 5 of the FTC Act, the FTC has enforcement authority over unfair or deceptive practices.[108] The FTC outlined its priorities on enforcement in its Policy Statement on Unfairness and Policy Statement on Deception. Section 5 largely codified at the Policy Statement on Unfairness, which states:

> The Commission shall have no authority... to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.[109]

The Deception Statement requires (1) a representation, omission or practice that is likely to mislead the consumer, (2) viewing it from the perspective of a consumer acting reasonably in

---

[108] *See* 15 U.S.C. § 45.

[109] 15 U.S.C. § 45(n) (2012).

the circumstances, and (3) the representation, omission, or practice must be a "material" one.[110] Ideally, the FTC would use this authority to develop a quasi-common law of privacy.[111]

Currently, the FTC has chosen to enforce the law primarily through leveraging its power to get settlements, which are not binding law and do little to explain how Section 5 applies to the facts of the case.[112] Nonetheless, it is clear that Section 5 reaches bad privacy acts, whether businesses create reasonably unavoidable harms to consumers or fail to live up to a promise of privacy.

The FTC routinely finds particular practices to be deceptive when the businesses promise to abide by a privacy policy and failed to do so.[113] Of course, the FTC assumes that the failures it enforces were *material* deceptions solely on the basis that they were expressly promised on a business' website.[114] While the FTC routinely sidesteps proving materiality in deception cases,[115] this does not mean that privacy promises weren't relied upon by privacy-sensitive consumers to their detriment.

Similarly, in a number of cases the FTC has found certain practices that may undermine privacy protections to be unfair.[116] While the FTC rarely explains how the facts fit the three prongs of unfairness in its complaints or consent decrees, such enforcement actions are often defensible uses of the Commission's authority.

2. Sector-Specific Privacy Legislation

FACTA, FCRA, COPPA, Graham-Leach-Bliley, etc.

---

[110] FTC Policy Statement on Deception, *appended to* Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984), *available at* http://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

[111] *See, e.g.*, Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

[112] *See* Geoffrey A. Manne & Ben Sperry, *FTC Process and the Misguided Notion of an FTC "Common Law" of Data Security* (Working Paper, May 14, 2014), *available at* http://masonlec.org/site/rte_uploads/files/manne%20%26%20sperry%20-%20ftc%20common%20law%20conference%20paper.pdf.

[113] Cite to examples from empirical data security paper, Id.

[114] Id.

[115] Howard Beales draft paper

[116] Manne & Sperry, supra note 112.

3. Common Law Privacy Protections

Unlike statutory law, which is based upon the text of legislation passed by representatives, or regulations, which are enacted and enforced by regulatory agencies, the common law is made up of rules developed in response to real-world disputes adjudicated in courts.

One of the best descriptions of the common law calls it:

> the embodiment of broad and comprehensive unwritten principles, inspired by natural reason, an innate sense of justice, adopted by common consent for the regulation and government of the affairs of men. It is the growth of ages, and an examination of many of its principles, as enunciated and discussed in the books, discloses a constant improvement and development in keeping with advancing civilization and new conditions of society. Its guiding star has always been the rule of right and wrong, and in this country its principles demonstrate that there is in fact, as well as in theory, a remedy for all wrongs.[117]

The emphasis of the common law is on its evolutionary character:

> It must be remembered that the common law is the result of growth, and that its development has been determined by the social needs of the community which it governs. It is the resultant of conflicting social forces, and those forces which are for the time dominant leave their impress upon the law. It is of judicial origin, and seeks to establish doctrines and rules for the determination, protection, and enforcement of legal rights. Manifestly it must change as society changes and new rights are recognized. To be an efficient instrument, and not a mere abstraction, it must gradually adapt itself to changed conditions.[118]

There are a number of torts and contract remedies under the common law that apply to the privacy concerns advocates want to reach. Below we will describe a few of them and how they apply in turn.

a. Trespass to Chattels

Trespass to chattels is a common law tort which can prevent companies from invading privacy of consumers through certain tracking technologies, unless they have the consent of those consumers. The elements of trespass to chattels are (1) an act of the defendant that interferes with the plaintiff's right of possession in the chattel, (2) intent to perform the act bringing

[117] Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 233 (Minn. 1998).

[118] *Id.* at 234.

about the interference with the plaintiff's right of possession, (3) causation, and (4) damages.[119] Restatement (Second) of Torts § 218 states that:

> One who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if,
>
> (a) he dispossesses the other of the chattel, or
>
> (b) the chattel is impaired as to its condition, quality, or value, or
>
> (c) the possessor is deprived of the use of the chattel for a substantial time, or
>
> (d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.

For instance, harm to the network, computer, or device connected to the Internet as a result of certain tracking technologies could be actionable under this doctrine.

As an example, one court has allowed a trespass to chattels case to go forward against a company that installed spyware on the computer. In *Sotelo v. DirectRevenue*,[120] the federal district court did not dismiss a trespass to chattels claim because there was harm to the plaintiff's computer as a result of the spyware. In particular, the spyware "interfered with and damaged his personal property, namely his computer and his Internet connection, by over-burdening their resources and diminishing their functioning."[121]

b. Intrusion Upon Seclusion

The common law action for intrusion upon seclusion is another tort which could be used to protect privacy. The elements of an intrusion upon seclusion claim are that (1) the intrusion must be intentional; (2) the intrusive act must be into matters the victim reasonably expected would remain private; and (3) the intrusive act must be highly offensive to a reasonable person.[122]

One of the difficulties of using this tort is the question of whether it requires a showing of damages. The Restatement of Torts does not require a proof of damages.[123] Many courts fol-

---

[119] CITE

[120] *Sotelo v. DirectRevenue, LLC*, 384 F.Supp.2d 1219 (N.D. Ill. 2005).

[121] *Id.* at 1231.

[122] CITE

[123] *See* § 652B.

low the Restatement and do not require proof of damages as an element of the tort.[124] Other courts require proof of "anguish and suffering" or, more generically, "an injury" to have an actionable intrusion.[125] Privacy harms may be difficult to show, especially when the information collected is used simply for targeted advertising. However, if proof of anguish or suffering can be shown from the intrusion itself, plaintiffs may have success.

A second difficulty is whether people are purposefully making information public by using services, like when people accept cookies to visit websites on the Internet. Many courts follow a reasonable expectation of privacy much like the Fourth Amendment's when analyzing the second element.[126] This would make nearly all information passing through third parties into "public" information. However, there is case law that suggests that overzealous surveillance of public actions can amount to actionable intrusion.[127] Information that is shared to make an application or service work would probably not be considered private, but the use of tracking technology that amounts to overzealous surveillance of a person's life could, in fact, be actionable.

Courts have found intrusions even in the absence of physical intrusion, allowing it to cover circumstances not reached by trespass to chattels. This is particularly important in the digital age, where physical intrusions may not always be necessary to obtain private information. In *Thayer Corp. v. Reed*,[128] the court found that the misappropriation of private e-mails could constitute unreasonable intrusion upon the seclusion of another even absent a physical intrusion. The

---

[124] *See, e.g.*, *Sanders v. Am. Broad. Cos.*, 978 P.2d 67, 71 (Cal. 1999); *Swarthout v. Mut. Serv. Life Ins. Co.*, 632 N.W.2d 741, 744-45 (Minn. Ct. App. 2001); *Preferred Nat'l Ins. Co. v. Docusource, Inc.*, 829 A.2d 1068, 1075 (N.H. 2003).

[125] *See, e.g.*, *Narducci v. Vill. of Bellwood*, 444 F. Supp. 2d 924, 938 (N.D. Ill. 2006); *Busse v. Motorola, Inc.*, 813 N.E.2d 1013, 1017 (Ill. App. Ct. 2004); *Tex. Comptroller of Pub. Accounts v. Att'y Gen. of Tex.*, 244 S.W.3d 629, 636 (Tex. Ct. App. 2008).

[126] *See* William Dalsen, *Civil Remedies for Invasion of Privacy: A Perspective on Software Vendors and Intrusion Upon Seclusion*, 2009 WIS. L. REV. 1059, 1069 n. 48 (2009) (cases cited therein).

[127] *See Nader v. General Motors Corp.*, 255 N.E.2d 765, 771 (1970) ("[I]t is manifest that the mere observation of the plaintiff in a public place does not amount to an invasion of his privacy. But, under certain circumstances, surveillance may be so 'overzealous' as to render it actionable... Whether or not the surveillance in the present case falls into this latter category will depend on the nature of the proof. A person does not automatically make public everything he does merely by being in a public place, and the mere fact that Nader was in a bank did not give anyone the right to try to discover the amount of money he was withdrawing. On the other hand, if the plaintiff acted in such a way as to reveal that fact to any casual observer, then, it may not be said that the appellant intruded into his private sphere.").

[128] *Thayer Corp. v. Reed*, 2011 WL 2682723 (D. Me. 2011) (applying Maine law).

court noted that opening private mail and tapping and recording telephone conversations would be an invasion of privacy and that therefore the misappropriation of private e-mails could be similarly tortious.[129]

c. Fraud and Negligent Misrepresentation

Much like the FTC currently uses its Deception authority under Section 5, litigants using the doctrines of fraud and negligent misrepresentation can protect privacy by holding companies to their promises not to disclose certain information. Litigants can also use fraud to go after hackers who impersonate trusted sites or people in attempts to gain access to personal information. Common law fraud requires (1) a representation of an existing fact (2) that is material, (3) known to be false by the defendant, (4) with the intent that the plaintiff will act upon the representation, (5) with the plaintiff actually ignorant of the falsity (6) and the ignorance being reasonable, (7) with the plaintiff relying upon the truth of the representation, and (8) damages.[130] Negligent misrepresentation

Fraud could apply when a person, including a hacker, deceives someone and that person acts to their detriment due to relying on that deception. Situations include those where a website or application makes a promise to keep certain information private in either a privacy policy or by certifying compliance with self-regulatory code without any intention of doing so. Other invasions of privacy also easily fall under this definition: a spam email pretending to be from one's doctor and asking for health information; or a website imitating Facebook and collecting long-in data and using it to access pictures and messages. In both of these cases, the bad actor made a false and material representation that the victim acted on to their detriment.

The main difference between common law fraud and Section 5 Deception is that fraud requires the plaintiff to show actual reliance on the false representations. The materiality requirement of Section 5 is supposed to perform a similar function, but the FTC's Policy Statement on Deception and the courts allow the FTC to assume materiality just because a company makes a promise. While burdens of common law fraud may be too high to help consumers, negligent

---

[129] *See also Eysoldt v. ProScan Imaging*, 2011 WL 2021502 (Ohio Ct. App. 1st Dist. Hamilton County 2011) (the court held that there was sufficient evidence to support a verdict in favor of a Web site account holder on an invasion-of-seclusion type of invasion of privacy claim against a Web site domain name registrar, based on the registrar's intrusion into private e-mail accounts, even though the account holder did not prove that the registrar had accessed particular e-mails).

[130] CITE

misrepresentation may apply in a variety of situations where companies are party to promises in industry self-regulation.

d. Contract Remedies

Contract remedies could apply if a company fails to live up to contract's terms. This could be both explicit terms incorporated into the contract by reference, like in a terms of service or privacy policy, or implicit terms. For instance, courts have allowed juries to find an implied contractual term disallowing a company from disclosing sensitive personal information like credit card numbers.[131] Damages, though, are the normal remedy for breaches, and many courts do not find much value in any individual's de-identified spending habits when companies were sued for disclosing personal information for online behavioral advertising in breach of their stated privacy policies.

Individuals could also contract with websites to prevent the tracking of their movements online. In theory, this could be done with an in-browser do-not-track mechanism. It would indicate to the website that, as a part of the contract between the user and the site, the user does not wish to be tracked. "If courts enforce consumer-offered automated standardized contract terms, then companies will indeed be violating the promises they have made to consumers if they violate a do-not-track term. If corporations violate an actual contractual promise regarding privacy, the FTC will have more opportunity to become legally involved."[132]

This would require, though, that courts treat the do-not-track signal as a contract term, which is an idea not yet widely accepted. Joshua Fairfield argues that business-proffered contract terms and consumer-proffered terms should be given equal treatment. He notes how the current rules of contract law, at least as interpreted, "do not generally operate to permit consumers to offer and enforce their own online contract terms…[and] are regularly used to construe only the corporation's contractual terms."[133] As one example, he points to how in the classic UCC 2-207 "Battle of the Forms" provision, courts almost entirely disregard the consumer "by not recognizing or enforcing consumer expressions of preference as true contractual terms, or by finding that the corporate version of the deal is the only version."[134]

---

[131] *See, e.g.*, *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 159 (1st Cir. 2011).

[132] Joshua Fairfield, *"Do-Not-Track" As Contract*, 14 VANDERBILT J. OF ENT. & TECH. LAW 545, 590 (2012).

[133] *Id.* at 574.

[134] *Id.* at 577.

Such evolution of doctrine is a strong suit of the common law, with its flexibility and adaptability. Historically, the common law has adapted contract doctrines to societal needs; the same process can occur now in an organic fashion, feeling out the useful contours of any adaptation.

Before we acquiesce to a change in antitrust law in order accommodate privacy concerns it is not well designed to police, we should take some time to analyze how the common law of both torts and contracts develop to ameliorate those problems. The burden should be on privacy proponents to show not only that there is failure in the current legal market, but also that the proposed changes to antitrust law make sense under an error-cost framework.

Conclusion

[To be completed].