PRIVACY FIXING AND PREDATORY PRIVACY: THE INTERSECTION OF BIG DATA, PRIVACY POLICIES AND ANTITRUST

BY BENJAMIN R. DRYDEN & SHANKAR (SEAN) IYER [1]

I. INTRODUCTION

Imagine that two leading, competing online dating websites announce sweeping reforms to their privacy practices. The two companies — let's call them "Charmed" and "Doctor Love" — jointly agree to bring the commercialization of their subscribers' data to an end. Press releases from both companies declare that members will no longer need to fear information about their sexual orientation or dating history falling into the hands of advertisers. The agreement sets a new best practice for the entire online dating industry.

The media, consumer advocates and the FTC unite in praising the move. And indeed, from a consumer protection standpoint, Charmed and Doctor Love's agreement to adopt best privacy practices for the online dating industry is laudable. An online dating service might have a great deal of highly sensitive data about its members and, all else equal, it is safe to assume that most consumers would rather keep some of this sensitive information out of advertisers' hands.

From a competition standpoint, however, the agreement between Charmed and Doctor Love raises a number of questions. Obviously, if Charmed and Doctor Love were to announce an agreement that they would each start charging subscribers the same rate of $29.95 per month, this would be a *per se* illegal price-fixing agreement; the two companies would likely face criminal investigations and treble-damages lawsuits within days. Likewise, if the two companies agreed with each other not to offer customer satisfaction guarantees, or if they agreed not to poach one another's customers, they would likely find themselves on the wrong end of antitrust law. So, one might reasonably ask, is the adoption of best privacy practices any different — from either a theoretical or legal perspective — than price fixing? And if so, why?

This article will address these questions. It will proceed in four parts. First, we will discuss the competitive implications of corporate privacy policies. As we will explain, privacy is an area where society's goals of protecting consumers can potentially conflict with its goals of promoting free competition. Second, we will propose a legal framework for evaluating whether a company's privacy practices might harm competition — situations that we will call "privacy fixing" and "predatory privacy." Third, we will consider what it might take to prove (or disprove) a claim of privacy fixing or predatory privacy. And fourth, we

1 Benjamin Dryden is a senior counsel in the Washington D.C. office of Foley & Lardner LLP. Shankar (Sean) Iyer is an Executive Vice President in the Washington D.C. and New York offices of Compass Lexecon.

will conclude with some remarks on what the concepts of privacy fixing and predatory privacy might mean for businesses, standard-setting organizations and law enforcement agencies like the FTC.

II. BIG DATA AND THE COMPETITIVE IMPLICATIONS OF PRIVACY

Before we discuss the legal aspects of privacy fixing, it is important to explain why the issue matters. Protecting privacy may seem so obvious a social good that any comparison with price fixing looks silly. As we will explain, however, under the right circumstances — such as "big data" industries where privacy practices may be an important element of non-price competition or may pose barriers to entry — privacy policies can have meaningful competitive consequences.

To return to our example, suppose that Charmed and Doctor Love were the two first movers in the online dating space. They both have millions of active members. All of Charmed's revenue, and the great majority of Doctor Love's revenue, comes from the monthly fees that their members gladly pay. Recently, however, Doctor Love has developed an ancillary line of revenue from the sale of advertisements on Doctor Love's mobile app. Doctor Love harvests its users' ages, dating histories, sexual orientations and mobile GPS coordinates to sell highly targeted, behavioral advertisements for the app. Over time, consumer watchdogs take notice of Doctor Love's practices and start to complain on privacy grounds.

In this world, an agreement between Charmed and Doctor Love to set an industry best practice against the sale of member data could actually have significant competitive consequences. One can think of the best practice as setting a new norm for member privacy. Under these facts, the agreement lessens a dimension of non-price, head-to-head competition between Charmed and Doctor Love, in that Charmed and Doctor Love will now offer an equal level of privacy protection to their members. Under the right conditions, this coordination could spill over into facilitating collusion on things like terms of use or even on monthly subscription prices. For instance, if Doctor Love uses its advertising revenue to subsidize its monthly subscription prices to undersell Charmed, then the elimination of this subsidy following the suspension of targeted advertisements could result in Doctor Love increasing its prices to be more in line with Charmed's prices. In this respect, the agreement on privacy practices would look like a classic, horizontal restraint of trade governed by Section 1 of the Sherman Act.[2]

The agreement between Charmed and Doctor Love could also raise monopolization issues under Section 2 of the Sherman Act.[3] To illustrate, let's introduce a couple more firms to the online dating marketplace — we can call them "Florida Daters" and "Can't Buy Me Love." Both are relatively recent entrants that have their own innovative way of making love connections, and they gradually chip away at the incumbents' networks. But since none has the membership sizes (and resulting network effects) that the incumbents do, they try new models to generate revenue. Florida Daters targets a specific geographical niche, and it adopts a model with two subscription tiers: a free, "basic" service, and a paid, "premium" service; it sells advertisements on both. Can't Buy Me Love eschews the subscription model altogether, and instead is a free service that is wholly supported by advertising. Both firms rely heavily on the sale of highly targeted advertisements based on sensitive member data.

In this world, the decision by Charmed and Doctor Love to jointly forgo revenue from the sale of data could create a barrier to entry that inhibits the growth of the new entrants. In an industry where privacy norms set by large incumbents dictate that user data will not be sold to advertisers, it can become very hard for smaller entrant firms that offer free content supported by advertising to compete with entrenched firms that have critical masses of paid subscribers. In this light, the agreement between Charmed and Doctor Love may protect the existing duopoly between them by creating an entry barrier to block new competition from gaining a sustainable foothold in online dating. If Charmed and Doctor Love succeed in convincing consumers not to do business with firms that sell user data to advertisers, they could kill the innovative business models that Florida Daters and Can't Buy Me Love have both developed. This conduct could potentially constitute not only a restraint of trade in violation of Section 1, but also could constitute actual or attempted monopolization, or conspiracy to monopolize, in breach of Section 2 of the Sherman Act.[4]

2 15 U.S.C. § 1.

3 15 U.S.C. § 2.

4 See generally Commissioner J. Thomas Rosch, *Do Not Track: Privacy In an Internet Age* (remarks at Loyola Chicago Antitrust Institute Forum, Oct. 14, 2011)

Thus, under either the Section 1 or Section 2 lens, two firms' coordinated adoption of a policy that is good for privacy can come at a genuine cost to competition. The question, then, is how antitrust law should approach these issues?

III. LEGAL FRAMEWORK FOR REVIEWING PRIVACY FIXING OR PREDATORY PRIVACY

A. Privacy Fixing as a Horizontal Restraint of Trade

In any case involving a horizontal "privacy-fixing" agreement between competitors, there are two key questions that a court or regulator would need to consider. First, do the antitrust laws even reach such non-price aspects of competition as companies' privacy policies? And second, if the antitrust laws do apply, would privacy fixing be deemed *per se* illegal, like price fixing, or instead would it be reviewed under a more flexible standard like the "rule of reason"?

The first question can be answered easily: yes, the antitrust laws apply to non-price elements of competition like privacy policies. The Supreme Court has made clear that "for antitrust purposes, there is no meaningful distinction between price and non-price components of a transaction."[5] In other words, because consumers presumably put some value on the privacy of their information, an agreement between competitors on privacy practices arguably could be viewed as effectively similar to an agreement between competitors on price. Moreover, an agreement between competitors on a non-price element of competition can spill over, one way or another, into affecting price elements of competition.

For these reasons, the antitrust laws have been applied to such horizontal agreements as agreements between competing car dealerships not to open on Saturdays,[6] agreements between competing airlines on the size of permissible carry-on luggage[7] and even public safety rules by private standards-setting organizations.[8] By the same token, an agreement between competitors to adopt a certain set of privacy practices would at least be subject to review under the antitrust laws.

The next question, then, is what level of review would the antitrust laws apply? There are two basic standards for reviewing joint conduct under the antitrust laws: the *per se* rule, and the rule of reason. Collusion between competitors is "the supreme evil of antitrust,"[9] and accordingly antitrust law treats classic collusive activity like price fixing, bid rigging or customer allocations as illegal *per se. Per se* illegality means that these kinds of collusive activities have "such predictable and pernicious anticompetitive effect, and such limited potential for procompetitive benefit," that they are irrebbutably presumed to violate the law.[10] Accordingly, a prosecutor or plaintiff need only prove that a *per se* illegal activity took place in order to establish that the agreement violated the antitrust laws.

By contrast, most other types of joint activities are reviewed under the more flexible rule of reason, which requires proving that the conduct in question actually harmed competition in light of industry and competitive conditions.[11] Because rule of reason claims often require detailed factual and economic evidence, they may be more difficult to prove than claims involving classic, *per se* illegal conduct. Rule of reason claims also can be defeated with evidence that the activity in question

(describing efforts by "well-entrenched firms . . . [that] may favor barriers to consumer tracking in order to create or raise entry barriers to rivals instead of solely to protect consumers against behavioral tracking. . . . Those firms may be tempted to sail under the consumer protection banner when their predominant interest is instead to disadvantage rivals that are more heavily dependent on advertising . . . .").

5 *Pacific Bell Tel. Co. v. Linkline Communications, Inc.*, 555 U.S. 438, 450 (2009). See generally also U.S Dep't of Justice & Federal Trade Comm'n, *Horizontal Merger Guidelines* (2010) § 1 ("When the Agencies investigate whether a merger may lead to a substantial lessening of non-price competition, they employ an approach analogous to that used to evaluate price competition.").

6 See *Detroit Auto Dealers Association v. FTC*, 955 F.2d 457 (6th Cir. 1992).

7 See *Continental Airlines, Inc. v. United Airlines, Inc.*, 277 F.3d 499 (4th Cir. 2002).

8 See *Allied Tube & Conduit Corp. v. Indian Head, Inc.*, 486 U.S. 492 (1988).

9 *Verizon Communications Inc. v. Law Offices of Curtis V. Trinko, LLP*, 540 U.S. 398, 408 (2004).

10 See generally *State Oil Co. v. Khan*, 522 U.S. 3, 10 (1997).

11 Id.

produced benefits to consumers or to competition that outweighed any harms. Here, the key question is whether a horizontal agreement between competitors not to compete on certain dimensions of privacy would be deemed illegal *per se*, under the theory that it resembles price fixing, or instead whether the more flexible rule of reason would apply.

One possible distinction to draw is that price fixing effectively sets a *floor* on what companies can get out of consumers, whereas an agreement adopting best privacy practices effectively sets a *ceiling* on what companies can get out of consumers. Thus, the argument would go, an agreement adopting a best privacy practice should be reviewed, if at all, under the rule of reason. However, there are two problems with this argument. For one, it has long been settled law that an agreement between competitors that sets *maximum* prices is just as illegal as an agreement that sets *minimum* prices.[12] Therefore, the mere fact that an agreement between competitors might, on its face, be good for consumers does not on its own necessarily salvage that agreement from *per se* illegality. Second, the argument assumes that all varieties of privacy fixing will be good for consumers. This assumption is not necessarily sound. For instance, if Charmed and Doctor Love entered into an agreement that set a *low* bar for user privacy, the law needs to be able to review that agreement under the same legal framework as an agreement that sets a *high* bar for user privacy. The results might be different — that is, an agreement setting a low bar for user privacy might have a more pernicious effect on competition than an agreement setting a high bar — but the overarching legal framework that reviews the agreements needs to be the same.

Given these considerations, we would argue that the *per se* rule should not apply to claims of horizontal privacy fixing, for the simple reason that it is a new form of competitive restraint that courts and regulators do not yet have substantial experience with. As the Supreme Court has made clear, "[t]he *per se* rule is a presumption of unreasonableness based on business certainty and litigation efficiency,"[13] and "it is only after considerable experience with certain business relationships that courts classify them as *per se* violations."[14] Therefore, a rule of *per se* illegality should only be adopted "once experience with a particular kind of restraint enables the Court to predict with confidence that the rule of reason will condemn it."[15] For these same reasons, each of the other novel forms of agreements described above — the agreement between car dealerships not to open on Saturdays, the agreement between airlines on carry-on sizes, and the standards-setting organization's safety rule — were each reviewed under some form of a rule of reason.[16] And by the same token, we would argue that an agreement between competitors that sets either a high bar or a low bar for user privacy should receive the same rule of reason review.

Today, at least, courts and regulators are not yet in a position to apply *per se* treatment to privacy fixing: they have not yet considered cases of privacy fixing in enough detail to determine whether such agreements tend to unreasonably harm competition or not.[17] Accordingly, no matter how egregious a case of privacy fixing may be — i.e. even if Charmed and Doctor Love had agreed to *maximize* the commercialization of their members' data, no holds barred — we would suggest that a court or regulator review such an agreement under a flexible rule of reason, to allow it to at least consider what corporate efficiencies and consumer benefits might result from such an agreement.[18]

---

12 *Kiefer-Stewart Co. v. Joseph E. Seagram & Sons, Inc.*, 340 U.S. 211, 213 (1951) ("The Court of Appeals erred in holding that an agreement among competitors to fix maximum resale prices of their products does not violate the Sherman Act. For such agreements, no less than those to fix minimum prices, cripple the freedom of traders and thereby restrain their ability to sell in accordance with their own judgment."); see also *United States v. Socony-Vacuum Oil Co.*, 310 U.S. 150, 223 (1940) ("Under the Sherman Act, a combination formed for the purpose and with the effect of raising, depressing, fixing, pegging, or stabilizing the price of a commodity in interstate or foreign commerce is illegal *per se*.").

13 *Atlantic Richfield Co. v. USA Petroleum Co.*, 495 U.S. 328, 348-49 (1990) (italics added and quotation omitted).

14 *Broadcast Music, Inc. v. CBS*, 441 U.S. 1, 9-10 (1979).

15 *Arizona v. Maricopa County Medical Society*, 457 U.S. 332, 344 (1982).

16 *Detroit Auto Dealers Association v. FTC*, 955 F.2d 457, 469 (6th Cir. 1992); *Continental Airlines, Inc. v. United Airlines, Inc.*, 277 F.3d 499, 517 (4th Cir. 2002); *Allied Tube & Conduit Corp. v. Indian Head, Inc.*, 486 U.S. 492, 501 (1988).

17 See generally *International Healthcare Mgmt. v. Hawaii Coalition for Health*, 332 F.3d 600, 603 (9th Cir. 2003) ("Per se categories are not to be expanded indiscriminately to new factual situations.").

18 See *Paladin Associates, Inc. v. Montana Power Co.*, 328 F.3d 1145, 1155 (9th Cir. 2003) ("When a defendant advances plausible arguments that a practice enhances overall efficiency and makes markets more competitive, per se treatment is inappropriate, and the rule of reason applies.").

B. "Predatory Privacy" as Monopolization

Privacy fixing can raise competitive concerns not only by lessening competition between the agreeing firms, but also by creating entry barriers to lessen competition by third-party new entrants. This theory is less akin to price fixing under a Section 1 lens and, instead, is more akin to predatory conduct under a Section 2 lens. In this respect, it is not necessary for there to be a multiplicity of actors to sustain a claim for "predatory privacy," because unlike claims for unlawful restraints of trade, claims for monopolization can apply to the unilateral conduct of a single, powerful firm, as well as to conduct by multiple oligopolists.[19]

To simplify, let us make a small change to the online dating story above. Instead of Charmed and Doctor Love coming to an agreement not to commercialize member data, suppose that Doctor Love unilaterally decided to match Charmed's policy against commercializing member data. In this respect, Doctor Love's decision would fall outside the scope of Section 1 of the Sherman Act, because it was merely a unilateral business decision to follow a competitor's practice rather than a bilateral decision between competing firms.[20] Still, however, Doctor's Love's unilateral adoption of a no-commercialization policy would potentially remain subject to review under Section 2 of the Sherman Act. In that respect, a regulator or an aggrieved competitor might be concerned that Doctor Love's decision to forgo a profitable line of revenue could be motivated by a predatory, monopolistic desire to injure its smaller rivals, rather than a *bona fide* decision to honor its users' privacy.

An analogue can be drawn to the Supreme Court's decision in *Aspen Skiing*.[21] As its name suggests, that case involved competition for skiing in Aspen. There are four mountains in Aspen that support skiing. Three of these mountains were owned by "Ski Co.," while the fourth was owned by "Highlands." For years, Ski Co. and Highlands teamed up to offer a six-day, all-inclusive pass that allows skiers to visit all four mountains. The product was very popular and profitable for both companies. In 1978, however, Ski Co. ended this product, and instead began to push a six-day pass that only allowed skiers to visit the three mountains owned by Ski Co.

Highlands sued Ski Co. for monopolization. From Highland's perspective, Ski Co.'s decision to terminate the popular, profitable four-mountain pass served no legitimate purpose, but rather was merely an effort by a monopolist to disadvantage its smaller rival. Following a trial, a jury agreed with Highlands and, on appeal, the Supreme Court affirmed the jury's decision. The Supreme Court explained that Ski Co.'s decision to abandon the four-mountain ticket was "a decision by a monopolist to make an important change in the character of the market."[22] In a subsequent decision, the Court elaborated that Ski Co.'s "unilateral termination of a voluntary (and thus presumably profitable) course of dealing suggested a willingness to forsake short-term profits to achieve an anticompetitive end."[23]

Here, by analogy, a decision by Doctor Love to forego a voluntarily, profitable source of revenue might, under the right circumstances, be seen as a similar attempt by an entrenched monopolist to disadvantage its smaller rivals. As *Aspen Skiing* teaches, when a firm "attempt[s] to exclude rivals on some basis other than efficiency, it is fair to characterize its behavior as predatory."[24] Therefore, if Doctor Love's decision to forgo the commercialization of its users' data has the purpose or the effect of making it unprofitable for smaller firms to commercialize their users' data, then Doctor Love's actions could be construed as the predatory actions of a monopolist, in violation of Section 2 of the Sherman Act. (However, this unilateral conduct may well

19 Section 2 of the Sherman Act, 15 U.S.C. § 2, is often thought of as applying exclusively to single-firm conduct. But this is not technically correct: rather, Section 2 applies not only to single-firm conduct but also to "person[s] who . . . combine or conspire with any other person or persons, to monopolize" a relevant market. Therefore, while such cases are not particularly common, agreements between competitors to create or entrench monopolies can be illegal under Section 2. See, e.g. *United States v. American Airlines, Inc.*, 743 F.2d 1114 (5th Cir. 1984) (holding that a solicitation to engage in price fixing constituted an attempt to monopolize under Section 2).

20 See generally *Theatre Enterprises, Inc. v. Paramount Film Distributing Corp.*, 346 U.S. 537, 541 (1954) ("The crucial question is whether respondents' conduct toward petitioner stemmed from independent decision or from an agreement, tacit or express.").

21 *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*, 472 U.S. 585 (1985).

22 Id. at 604.

23 *Verizon Communications Inc. v. Law Offices of Curtis V. Trinko, LLP*, 540 U.S. 398, 409 (2004) (emphasis removed). Note, however, that the *Trinko* Court described *Aspen Skiing* as being "at or near the outer boundary of § 2 liability." Id.

24 *Aspen Skiing*, 472 U.S. at 605 (quotation omitted).

need to be packaged with other purportedly anticompetitive conduct in order to support a Section 2 claim, and would further require that Doctor Love have monopoly power or a dangerous probability of acquiring it.)

To be clear, Doctor Love might have some good arguments in its defense. For one, Doctor Love would surely argue that its decision to adopt a no-commercialization privacy policy was made out of a *bona fide*, procompetitive desire to better serve its customers, rather than out of an anticompetitive desire to disadvantage its rivals. There is certainly support for this defense in theory,[25] but in practice the defense would likely turn on the facts of each particular case.

A more interesting defense that Doctor Love might raise is that its own privacy policy does not actually set an entry barrier for competitors. As long as there are at least some consumers who would rather sacrifice privacy for free content, then there might not be any barrier for competitors to profitably continue targeting those customers. Again, however, this is an empirical question that would likely require some form of evidence to confirm or rebut.

Another spin on this defense is that Doctor Love's adoption of a no-commercialization privacy policy does not actually force its competitors to follow suit. This defense might raise some interesting factual questions, but it would also raise a number of legal issues as well. One can imagine a range of ways that a new entrant might be impacted by a monopolist's privacy policy, and many of these ways pose a range of intricate legal issues. On one extreme, Doctor Love could hire lawyers and lobbyists to convince a government agency to crack down on its competitors for exploiting sensitive member data, or even to adopt a new regulation that prohibits the practice outright. This might be a very effective tactic for creating a barrier to new entry. But it's also one that is immune to antitrust challenge, because legal representation and lobbying are constitutionally protected rights, subject to limited exceptions.[26]

On the other extreme, Doctor Love might simply advertise to consumers the fact that while it does not seek to profit off of its members' data (anymore), its competitors do. One could imagine these ads being very powerful. Therefore, this too could be a very effective tactic for creating a barrier to new entry. But it is also one that reflects *bona fide* competition between firms, rather than anything anticompetitive. So this tactic should not create any antitrust liability for Doctor Love, because truthful, informative advertising is the essence of competition.[27]

In between these two extremes are more difficult cases. For instance, suppose that Doctor Love uses its clout to pressure an influential industry trade association to adopt no-commercialization as a rule of "online dating ethics" (whatever that means). In that case, there could potentially be antitrust liability, not only for Doctor Love but also for the trade association, if the trade association did not exert adequate controls over the rulemaking process[28] if the rule of ethics was just a subterfuge for protecting an incumbent firm.[29] Likewise, if Doctor Love paid actors to pretend to be consumers outraged at a rival firm's privacy practices in an effort to gin up a faux media controversy, this too might be sufficiently predatory conduct to support an antitrust claim.[30]

Therefore, if predatory privacy is rare, it would be rarer still for predatory privacy to actually be actionable under the antitrust laws. But still, one can imagine a few select sets of circumstances where a company adopted a consumer-friendly privacy policy in an unlawfully monopolistic manner. In these few circumstances, a claim for predatory privacy could conceivably be viable.

25 See id. at 608 (emphasizing "Ski. Co's failure to offer any efficiency justification whatever for its pattern of conduct").

26 See, e.g. *Eastern Railroad Presidents Conference v. Noerr Motor Freight, Inc.*, 365 U.S. 127 (1961); *California Motor Transport Co. v. Trucking Unlimited*, 404 U.S. 508 (1972).

27 See, e.g. *Berkey Photo, Inc. v. Eastman Kodak Co.*, 603 F.2d 263, 287-88 (2d Cir. 1979) ("Advertising that emphasizes a product's strengths and minimizes its weaknesses does not, at least unless it amounts to deception, constitute anticompetitive conduct violative of § 2.").

28 See, e.g. *Allied Tube & Conduit Corp. v. Indian Head, Inc.*, 486 U.S. 492 (1988); *American Society of Mechanical Engineers, Inc. v. Hydrolevel Corp.*, 456 U.S. 556 (1982).

29 See, e.g. *In the Matter of Professional Skaters Association*, FTC Dkt. No. C-4509, 2015 FTC LEXIS 46 (FTC Feb. 13, 2015).

30 See, e.g. *In re Warfarin Sodium Antitrust Litigation*, MDL 98-1232, 1998 U.S. Dist. LEXIS 19555, at *35 (D. Del. Dec. 7, 1998), rev'd on other grounds by 214 F.3d 395 (3d Cir. 2000) (denying motion to dismiss § 2 claim based, in part, on allegations "that defendant's extensive publicity campaign contained false misrepresentations . . . to induce potential customers to avoid purchasing" a competing product).

As an aside, it is worth pausing to distinguish "predatory privacy" as just described from a more classic "predatory pricing" theory. Formally, "predatory pricing" is an exceptionally rare[31] strategy that proceeds in two phases. In phase one, a deep-pocketed firm lowers its prices to below its actual costs, in order to take away business from a smaller rival. Eventually, the smaller rival goes out of business, leaving the deep-pocketed firm with a monopoly.[32] Then, in phase two, the monopolist raises its prices to a supracompetitive level in order to recoup the losses it incurred during phase one.[33] In this light, "predatory privacy" is fundamentally different from traditional "predatory pricing," among other reasons, because customer data is essentially costless for a firm to acquire (at least on a marginal basis), such that the idea of selling customer data below cost is difficult to imagine. There would also be serious obstacles to recoupment, because the FTC takes the position that a failure to keep a promise made to consumers about privacy constitutes a deceptive practice prohibited by under the FTC Act.[34] Therefore, when describing "predatory privacy," we refer primarily to an *Aspen Skiing* type of predation, rather than making a true analogy to predatory pricing.

IV. PROVING THAT A PRIVACY PRACTICE IS ANTICOMPETITIVE

Given that antitrust law could, under the right circumstances, recognize a claim for either privacy fixing or predatory privacy, it is worth considering how such a case might unfold.

As a starting point, even though a niche competitor like Florida Daters might have every incentive to challenge the privacy practices agreement between Charmed and Doctor Love's, we doubt that such a claim could be successful. As a competitor to Charmed and Doctor Love, Florida Daters would arguably lack standing to challenge a horizontal agreement between its competitors.[35] Alternatively, customers of Charmed or Doctor Love might have standing to challenge the restraint — on the theory that they paid a higher membership fee than they would have paid if the firms had sold their data to advertisers — but we doubt that a customer would have much incentive to bring such a case, at least on an individual basis. Even on a class-action basis, consumer claims would seem like a high-risk, low-reward proposition.

An aggrieved advertiser, however, might have both the legal standing and the most practical motivation to bring an antitrust lawsuit. To prove its case, an advertiser would need to show that the agreement between Charmed and Doctor Love not to sell their members' data caused more harm to competition than good. Such a case would likely resemble a classic battle of experts.

As a starting point, the case would require much of the same types of economic evidence about market definition and market power that are needed in all other types of Section 1 or Section 2 cases. In other words, a plaintiff or regulator would likely employ standard economic tools to determine reasonable interchangeability, market share and market concentration to find the contours of the relevant markets and to determine whether the alleged privacy fixer or predator has sufficient market power to be able to plausibly harm competition through its privacy practices. For instance, an economist might be needed to opine as to whether an online dating service with a geographical niche like Florida Daters, or a free dating service like Can't Buy Me Love, is reasonably interchangeable with the services of nationwide, subscription-based dating services like Charmed and Doctor Love. Or, indeed, if "offline," traditional dating services are in the same market as online dating services.

In this respect, an interesting question will be the extent to which the two-sided nature of data markets matter. For instance, imagine that Charmed and Doctor Love had teamed up with, say, a ridesharing application ("Mister Motor") to adopt

31 See *Matsushita Electrical Industrial Co., Ltd. v. Zenith Radio Corp.*, 475 U.S. 574, 589 (1986) ("[T]here is a consensus among commentators that predatory pricing schemes are rarely tried, and even more rarely successful.").

32 It is conceivable that a predatory pricing scheme might be attempted by several oligopolists, rather than by a single monopolist, but for a number of reasons "[s]uch a conspiracy is incalculably more difficult to execute than an analogous plan undertaken by a single predator." Id. at 590.

33 See generally *Brooke Group Ltd. v. Brown & Williamson Tobacco Corp.*, 509 U.S. 209 (1993).

34 See Letter from Jessica Rich, Director, Bureau of Consumer Protection, to Facebook, Inc. and WhatsApp, Inc., April 10, 2014, available at: https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf, at 2-3.

35 See, e.g. *Matsushita Electric Industrial Co. v. Zenith Radio Corp.*, 475 U.S. 574, 583 (1986).

joint policies against commercializing users' data. It is clear that Charmed and Doctor Love operate in a different primary market (online dating) than Mister Motor (ridesharing), but it is also clear that each firm also operates in a common secondary market for the sale of data to advertisers. In such a situation, absent some truly exceptional circumstances, we doubt that any agreement between the online dating services and Mister Motor on privacy practices could even begin to harm competition in the secondary market.

Data markets are immense. Competitors for the sale of data not only include services like Charmed, Doctor Love and Mister Motor, but also search engines, social media sites and, increasingly, data aggregators that purchase data on a wholesale basis and lease or sell it to advertisers or other firms. From a practical perspective, vendors increasingly offer predictive modeling services, such that proxies for data fields that fall under the umbrella of the privacy agreements may be readily available for purchase. For example, machine learning techniques can predict sexual orientation from (say) membership information, donations to charitable causes and so on. Accordingly, barring some truly unique circumstances, we doubt that data markets can be harmed by agreements between firms in different primary markets.

Thus, in addition to proving market definition and market power, a regulator or plaintiff will also be required to prove, one way or another, that the defendant's privacy practices have actually harmed (or were intended to harm, or otherwise pose some danger to) competition. Plainly, if a defendant were to turn over some smoking gun — such as a strategy presentation to the board of directors explaining how adopting a no-commercialization privacy policy will create a barrier to new entry — then this evidence may assist in proving an antitrust claim. But absent this sort of "hot" document, it might require some innovative forms of economic evidence to prove that a privacy practice has harmed competition.

In this respect, a key issue at any trial would be whether the agreement foreclosed the advertiser from obtaining the data it wanted from other sources, such as from competing online dating sites like Florida Daters, from non-competing services like Mister Motor, from search engines or social media sites, or from third-party data aggregators. In this respect, the defendants' expert would likely be able to opine that advertisers have a wide array of options for obtaining consumer data. However, the advertiser's expert might be able to opine that online data sites are irreplaceable sources of data about things like dating histories and sexual orientations, and that these sorts of highly sensitive data are uniquely valuable to advertisers. The trier of fact would have to weigh these arguments to determine whether the agreement harmed competition.

Ultimately, if the advertiser proved its case, it would also need to show damages to collect any money. A damages estimate might take the form of calculating the advertiser's lost income from being deprived of the ability to run advertisements based on users' dating histories and sexual orientations, offset in part by the advertiser's ability to run advertisements based on information that was available from other sources, such as users' ages and locations. In the age of big data and machine learning, such estimates will have to be benchmarked against the cost of buying probabilistic data for ad targeting. One can imagine a counterfactual world where the aggrieved plaintiff may reasonably be able to buy data generated from predictive modeling software that uses proxies for fields such as sexual orientation to achieve a near-equivalent level of ad targeting.

V. CONCLUSION

It remains to be seen whether privacy fixing or predatory privacy will take off as a new area of antitrust litigation or enforcement. That said, as big data gets bigger and bigger, it stands to reason that these issues will only increase in importance. In the meantime, we would close with four observations.

First, absent truly extraordinary circumstances, we suggest that Section 1 "privacy fixing" liability should only attach for agreements between companies that compete horizontally in non-data markets. It is very difficult to imagine a scenario where an agreement between an online dating site and a ridesharing application to adopt the same privacy policies could unreasonably harm competition. Even though both firms might each have vast amounts of sensitive data about their respective members, the markets for data are so large and unconcentrated, and have such low entry barriers, that it is exceedingly unlikely that any restraint between the two firms would lessen competition in any way.

Second, we expect that any private lawsuits over privacy fixing or predatory privacy would likely come from aggrieved advertisers. Competing firms are unlikely to have antitrust standing to challenge their rivals' privacy practices. And as long as companies tend to adopt high bars for their privacy practices, consumers are unlikely to file lawsuits complaining that these bars are harming rivals or creating barriers for new entrants. Advertisers, however, could have both the standing and the motivation to file a lawsuit for privacy fixing or for predatory privacy.

Third, because it is relatively uncommon for companies to adopt privacy policies in direct collaboration with their competitors, the most likely target for a privacy fixing or predatory privacy claim might well be a standards-setting organization or trade association that tries to adopt a best privacy practice or a rule of ethics for an entire industry. Therefore, when such organizations wade into discussing privacy topics, they should recognize the competitive concerns and potential antitrust risks. Whenever possible, such standards-setting organizations and trade associations should make sure to apply procedures and safeguards to prevent their decisions from becoming hijacked by private interests.[36] For instance, such organizations might consider requiring supermajority votes before any policies are adopted, basing decisions on outside expert judgments rather than industry interests, and describing any best practices as "recommendations" rather than as strict requirements.

Finally, companies should take heart that any good-faith attempts to advocate to the government for new laws or for better law enforcement are constitutionally protected and usually will not create antitrust liability. Therefore, companies with strict privacy policies should not be discouraged from lobbying for similar standards across the industry. That said, the competitive implications of privacy practices raise some tricky questions for law enforcement agencies like the FTC, which is simultaneously charged with promoting competition and with protecting consumers. It is for the policymakers at the FTC to decide how to balance these two important societal values. But the first step in striking the right balance is to recognize that competition and privacy can conflict, and that what's best for consumers' privacy may not be best for consumers' wallets.

36 See generally *Allied Tube & Conduit Corp. v. Indian Head, Inc.*, 486 U.S. 492, 505 (1988).