2018

Protecting Consumer Data Privacy with Arbitration

Erin O'Hara O'Connor
Florida State University College of Law

PROTECTING CONSUMER DATA PRIVACY WITH ARBITRATION*

ERIN O'HARA O'CONNOR**

** Dean and McKenzie Professor of Law, Florida State University College of Law. Special thanks to participants at the LEC Research Roundtable on the Law and Economics of Privacy and Data Security and at the ILEP Symposium on Secrecy. Thanks also to J. Howard Beales, James Cooper, Robert Jackson, Judith Resnik, Abe Wickelgren & Kathy Zeiler for particularly helpful comments and suggestions. Amy Bhatt provided helpful research assistance.

INTRODUCTION

Businesses, healthcare providers, and others gather, store, and use our data every day. In the process, these entities may end up committing privacy harms. For example, Equifax might fail to utilize proper measures to safeguard your credit information, leaving it vulnerable to hacking. Or a Health Maintenance Organization employee might negligently leave a laptop with your health information on an airplane. Perhaps a retail store decides to sell information about your purchases to a third party without your permission. What should be the consequence of these privacy harms? And what is the best legal mechanism for addressing them?

The privacy regulation question is the subject of vigorous current debate. The widespread gathering of data about consumers and its use in business activities, including behavioral advertising, concerns privacy advocates. Such use of consumer data appears invasive, and even potentially deceptive, leading to calls for more vigorous regulation through the Federal Trade Commission ("FTC"), the states, common law actions, and new legislation.[1] Adding to the consternation of privacy advocates is a rash of reports of security breaches at a variety of retail firms, leading to hackers and other unintended third parties gaining access to consumer information.[2] As a result, an explosion of consumer data privacy legislation has been introduced in Congress recently,[3] and many more legislative

1. *See, e.g.*, Jeri Clausing, *Report Rings Alarm Bells About Privacy on the Internet*, N.Y. TIMES, Feb. 7, 2000, at C10 (noting privacy advocates' arguments that self-regulation is insufficient). A number of privacy organizations have been actively involved in advocacy. *See* Angelique Carson, *Changing Tactics: The Rise of the Privacy Advocates,* THE INT'L ASS'N OF PRIVACY PROF'LS (Sept. 23, 2013), https://iapp.org/news/a/changing-tactics-the-rise-of-the-privacy-advocates/ [https://perma.cc/KP5Z-QYUN] (mentioning, through reference to a single example, the advocacy work of EPIC, the Center for Digital Democracy, Consumer Watchdog, Patient Privacy Rights, US PIRG, and the Privacy Rights Clearinghouse).

2. *See Identity Theft Resource Center Breach Report Hits Record High in 2014*, IDENTITY THEFT RES. CTR., http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html [https://perma.cc/33V3-7DRA].

3. *See, e.g.*, Consumer Privacy Protection Act of 2015, H.R. 2977, 114th Cong. (2015); Data Security Act of 2015, H.R. 2205, 114th Cong. (2015); Consumer Privacy Protection Act of 2015, S. 1158, 114th Cong. (2015); Data Breach Notification and Punishing Cyber Criminals Act of 2015, S. 1027, 114th Cong. (2015); Data Security Act of

proposals have been introduced at the state level.[4] More than half of states now have data disposal laws to ensure that information content is protected, and at least thirteen states have data security laws that regulate how data is stored, maintained, and used.[5] These proposed and enacted laws provide strong evidence that consumer data issues currently rank highly on the agenda of many lawmakers.

On the other side of the debate, pro-business advocates caution that stringent privacy protections can unduly hamstring the development of highly valuable technological innovations to the ultimate detriment of consumers.[6] Bolstering their arguments, some scholars question the extent to which privacy regulations are

2015, S. 961, 114th Cong. (2015); Data Security and Breach Notification Act of 2015, H.R. 1770, 114th Cong. (2015); Personal Data Notification and Protection Act of 2015, H.R. 1704, 114th Cong. (2015); Data Security and Breach Notification Act of 2015, S. 117, 114th Cong. (2015); Personal Data Protection and Breach Accountability Act of 2014, S. 1995, 113th Cong. (2014); Personal Data Privacy and Security Act of 2014, H.R. 3990, 113th Cong. (2014); Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. (2014); Data Security Act of 2014, S. 1927, 113th Cong. (2014); Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (2014).

4. *See State Laws Related to Internet Privacy*, NAT'L CONFERENCE OF STATE LEGISLATURES (June 20, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx [https://perma.cc/5592-D9ZV] (tracking new and proposed state privacy law).

5. *Data Security Laws—Private Sector*, NAT'L CONFERENCE OF STATE LEGISLATURES (Jan. 16, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx [https://perma.cc/78VX-75Z9]. In addition, half of the states prevent employers and/or universities from conditioning work or educational opportunities on having access to student or employee personal internet accounts. *State Social Media Privacy Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (May 5, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-acess-to-social-media-usernanes-and-passwords.aspx [https://perma.cc/49U8-F39M]. Several states have begun to prohibit the private use of GPS tracking systems without the target's consent. Pam Greenberg, NAT'L CONFERENCE OF STATE LEGISLATURES, *Private Use of Mobile Tracking Devices*, 24 LEGISBRIEF, no. 43 (Nov. 2016), http://www.ncsl.org/documents/legisbriefs/2016/lb_2443.pdf [https://perma.cc/jrl6-g7nr].

6. *See, e.g.*, Ed Burns, *Data Collection Practices Spark Debate on Big Data Ethics, Privacy*, SEARCHBUSINESSANALYTICS (Apr. 2014), http://searchbusinessanalytics.techtarget.com/feature/Data-collection-practices-spark-debate-on-big-data-ethics-privacy [https://perma.cc/V5YT-BCS9] (quoting Mike Zaneis, then-Executive Vice President of the Interactive Advertising Bureau, saying "[h]aving Congress or the FTC write prescriptive rules around an industry that is changing every day is the surest way to inhibit growth"); *see also* Jane Yankowitz, *Tragedy of the Data Commons*, 25 HARV. J. L. & TECH. 1 (2011) (arguing that restrictions on the use of anonymized data inhibits advances in research). *See generally* James C. Cooper & Joshua D. Wright, *The Missing Role of Economics in FTC Privacy Policy*, *reprinted in* CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY (Jules Polonetsky, Evan Selinger & Omer Tene, eds.) (forthcoming 2018) (manuscript at 20) (on file with the North Carolina Law Review) (arguing that "consumers would benefit immensely if economics were to play as central a role in privacy regulation as it does in antitrust").

appropriate, given that privacy harms tend to be both subjective and heterogeneous.[7] Subjective harms are not reliably measurable by third parties, which makes it difficult for courts to assess liabilities for breaches and for policy makers to determine appropriate tradeoffs between costs and benefits of particular data use and storage practices.[8] Privacy harms are heterogeneous harms in the sense that rules regarding data use benefit those who value their privacy more highly but not those who attach less value to such protections. In a world where privacy regulations necessarily interfere with technological product and marketing developments, the latter group is not just indifferent to regulation. Rather, they are affirmatively harmed. The presence of substantial costs to consumers in the case of either too much or too little regulation suggests that a careful cost-benefit policy analysis is essential for consumer privacy.

Because industry advocates have so far successfully fought off most new federal legislative proposals, privacy advocates have turned to other regulatory vehicles, including state legislation,[9] private class actions,[10] Federal Communications Commission regulation,[11] and

7. J. Howard Beales III describes the subjective nature of privacy as follows:

> Privacy is one area where such subjective preferences are important. As the FTC's preliminary report noted in 2010, "for some consumers, the actual range of privacy-related harms is much wider and includes . . . the fear of being monitored or simply having private information 'out there.'" Consumers may also feel harmed when information is used "in a manner that is contrary to their expectations," and may have "discomfort with the tracking of the online searches and browsing." Some have summarized these kinds of harms as "creepiness."

The FTC at 100: Views from the Academic Experts: Hearing Before the H. Subcomm. on Commerce, Mfg., & Trade of the H. Comm. on Energy & Commerce, H.R. 113th Cong. 6 (2014) (statement of J. Howard Beales III, Professor of Strategic Mgmt. and Pub. Policy, George Washington Univ. Sch. of Bus.) [hereinafter statement of J. Howard Beales III] (first quoting FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 20 (2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf [https://perma.cc/C2ZQ-RYNU], then quoting Adam Thierer, *The Pursuit of Privacy in a World Where Information Control is Failing*, 36 HARV. J. L. & PUB. POL'Y 409, 417–21 (2013)).

8. *See id.* at 25 (arguing that consumer privacy must be accurately valued because firm behaviors that can interfere with privacy also create value in subsidizing technological improvements, facilitating better consumer decisions, and enabling better monitoring for credit card fraud).

9. *See* NAT'L CONFERENCE OF STATE LEGISLATORS, *supra* note 4.

10. *See infra* notes 56–65 and accompanying text.

11. In 2016, the FCC adopted a regulation that would require internet service providers to obtain the affirmative permission of consumers before selling consumer data. 47 C.F.R. § 64 (2017). In spring 2017, the regulation was repealed. Act of Apr. 3, 2017, Pub. L. No. 115-22, 131 Stat. 88; *see also* Brian Fung, *Trump Has Signed Repeal of the FCC Privacy Rules. Here's What Happens Next.*, WASH. POST: THE SWITCH (Apr. 4, 2017),

Federal Trade Commission ("FTC") enforcement complaints[12] to police consumer data uses. Class action complaints rely on state and federal statutes as well as common law causes of action to recover damages for consumer harms that result from a firm's privacy practices.[13] As is well known, class actions have the advantage of enabling a large number of consumers who have also suffered small damages to aggregate those claims into larger cases that make pursuing legal remedies much more feasible.[14] The downside to class actions is that plaintiffs' attorneys can use them to extract monetary settlements even in cases that lack merit, due to the substantial potential liabilities that a class action poses.[15] Moreover, class action settlements can involve substantial legal fees for plaintiffs' attorneys with relatively modest relief for consumers;[16] thus, they can achieve deterrence, sometimes overdeterrence, without actually effectively compensating harms.

In conjunction with class actions, the FTC has emerged as the primary federal regulator of the commercial use of consumer data over the past twenty years.[17] During the 1990s, industry took on efforts to self-regulate company gathering, use, and security of consumer data. As part of that self-regulatory effort, firms were pressured into providing notice to consumers regarding what the company would do with consumers' data. In fact, between 1998 and 2001, firms underwent a dramatic shift in their use of privacy notices, with virtually no websites listing privacy policies in 1998 to all of the most popular websites displaying privacy notices by 2001.[18] Along the way, the FTC undertook the role of augmenting companies' self-

https://www.washingtonpost.com/news/the-switch/wp/2017/04/04/trump-has-signed-repeal-of-the-fcc-privacy-rules-heres-what-happens-next/?utm_term=.70257b90adcd [https://perma.cc/C4XQ-EE27].

12. For a survey of FTC enforcement actions involving privacy, see Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 600–08 (2014).

13. *See infra* note 66 and accompanying text.

14. 1 WILLIAM B. RUBENSTEIN, NEWBERG ON CLASS ACTIONS § 1:3, at 7, 9 (5th ed. 2011).

15. *See In re* Rhone-Poulenc Rorer Inc., 51 F.3d 1293, 1298–99 (7th Cir. 1995) (discussing the "intense pressure to settle" that people who are involved in class actions face).

16. *See* Deborah R. Hensler & Thomas D. Rowe, Jr., *Beyond "It Just Ain't Worth It": Alternative Strategies for Damage Class Action Reform*, 64 LAW & CONTEMP. PROBS. 137, 138–39, 148–49 (2001) (discussing examples derived from RAND Corporation study of class action settlements).

17. Solove & Hartzog, *supra* note 12, at 590–606.

18. Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PA. ST. L. REV. 587, 593 (2007).

regulation by enforcing representations and promises that firms make to consumers in their privacy policies.[19] In particular, section 5 of the Federal Trade Commission Act ("FTC Act") gives the FTC authority to prohibit unfair or deceptive acts or practices,[20] and the FTC deemed it deceptive for a company to fail to abide by its own privacy policy representations.[21] Over time, the FTC has gradually moved toward using its section 5 authority beyond merely enforcing the details of the privacy policies in an effort to ensure that firms' privacy efforts comport with industry norms and consumer expectations.[22]

The FTC has extremely limited ability to unilaterally impose monetary liability on firms,[23] but through its authority to "prohibit" unfair or deceptive practices, it can engage in "command-and-control" regulation.[24] Firms fearful of the consequences of FTC enforcement typically respond to enforcement actions against them by entering into settlement agreements with the agency under which the firm agrees to comply with a set of expectations that the FTC might or might not have formal authority to impose.[25] Included in many settlements is an agreement that the firm will refrain from certain business practices for a number of years, during which time the firm agrees to FTC or other external monitoring of its activities.[26] FTC enforcement actions are thus similar to class actions in that they can induce settlement agreements that are not clearly rooted in governing legal principles, and the two mechanisms together contribute to a significant lack of clarity regarding the obligations of similarly situated firms.[27]

19. *Id.* at 599.

20. Federal Trade Commission Act, Pub. L. No. 63-203, ch. 311 § 5, 38 Stat. 717, 719 (1914) (codified as amended at 15 U.S.C. § 45(a)(1) (2012)).

21. Haynes, *supra* note 18, at 599.

22. Solove & Hartzog, *supra* note 12, at 661.

23. *Id.* at 661 & n.59.

24. "Command-and-control" regulation occurs when a government entity mandates or forbids action rather than providing economic incentives to move regulated entities into more desirable activities. For a discussion of the tradeoff, see Jonathan S. Masur & Eric A. Posner, *Toward a Pigouvian State*, 164 U. PA. L. REV. 93, 95, 99 (2015).

25. *See* Solove & Hartzog, *supra* note 12, at 610–19 (discussing the prevalence of FTC settlements and common attributes of FTC settlement orders).

26. *See id.*; *see also* Cooper & Wright, *supra* note 6 (discussing commonality of lengthy monitoring or cease and desist periods).

27. On the lack of clarity regarding FTC guiding policy, see Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 183 (2008); Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 676 (2013).

Moreover, each of these methods of addressing consumer data use and protection is imperfect, in that they can lead to too much or too little effective regulation. In particular, the subjective and heterogeneous nature of harm to consumers makes it highly unlikely that the FTC, lawyer advocates, or courts will accurately assess the value of consumer privacy. What is needed is a mechanism designed to elicit information about the value that consumers place on privacy, which would solve the subjectivity problem, as well as specific information about individual consumer valuation, which would solve the heterogeneity problem.

Markets utilize pricing mechanisms and thus can treat the problem of valuing consumer privacy relatively effectively in many contexts. Indeed, U.S. companies are beginning to use such price mechanisms in the privacy-relevant marketing of their goods and services. Grocery and drug store chains have instituted loyalty programs, under which consumers who are comfortable sharing their purchasing information for purposes of targeted advertising and otherwise pay lower prices for many items than customers who do not participate in the data-sharing programs.[28] In addition, in 2015 AT&T began to offer its GigaPower U-Verse fiber-optic internet access service in Kansas City for two different prices: a higher price for customers who do not want their online browsing tracked for purposes of company-generated targeted advertising and a lower price for customers whose browsing will be tracked.[29] In addition, many companies that are sensitive to consumer concerns about privacy offer products that leave many sharing decisions to the consumers.[30]

However, what happens when privacy decisions are not or should not be left to the marketplace? In some cases, price discrimination or filtering is not feasible for the company. In others, technological or other market changes place pressure on the company to scale back on

28. Martin H. Bosworth, *Loyalty Cards: Reward or Threat?*, CONSUMER AFF. (July 11, 2005), https://www.consumeraffairs.com/news04/2005/loyalty_cards.html [https://perma.cc/5LAY-LWGC].

29. Elizabeth Dwoskin & Thomas Gryta, *AT&T Offers Data Privacy—for a Price*, WALL ST. J.: DIGITS (Feb. 18, 2015, 6:01 AM), http://blogs.wsj.com/digits/2015/02/18/att-offers-data-privacy-for-a-price/ [https://perma.cc/UUT8-7BNV (dark archive)]. AT&T stopped this price discrimination in 2016. Sean Buckley, *AT&T Stops Tracking Internet Activity of GigaPower Customers*, FIERCETELECOM (Sept. 30, 2016, 10:22 AM), http://www.fiercetelecom.com/telecom/at-t-to-sunset-internet-activity-tracking-requirement-for-gigapower-customers [https://perma.cc/A558-MPZU].

30. For example, laptops, smart watches, mobile websites, and other products now commonly contain privacy setting menus. *See* Brian X. Chen, *How to Protect Your Private Data From Prying Apps*, N.Y. TIMES, May 4, 2017, at B6.

prior promises regarding privacy protections, causing potential difficulties for long-term contracts. Separately, sometimes other policy considerations, such as fairness or distrust for consumer choices, should trump these private market decisions.[31] Although no ex post regulatory mechanism can perfectly treat the problems of subjectivity and heterogeneity, this Article conducts a thought experiment into whether a different regulatory policy tool could be more effective than those currently used to treat privacy violations. In particular, this Article explores the possibility of an alternative, informal dispute resolution mechanism that carries the promise of eliciting at least rough information about how consumers value their privacy. Specifically, might the use of an arbitral mechanism, one jointly consented to by a company and FTC, be preferable to both FTC action and private class actions?

Arbitration can at least roughly filter out consumers who place a low value on their privacy because individuals who feel harmed by company actions must file claims to get relief, which will likely entail a cost that low-value consumers would not incur. As long as the financial costs to consumers are kept low or negligible, then consumers who do experience harm should not be discouraged from coming forward, and, assuming that compensation levels reasonably compensate high-privacy-value plaintiffs for their harms, the resulting liabilities can more closely resemble the social value of privacy to a firm's customers. These liabilities can be superior to FTC direct enforcement, which lacks reliable valuation mechanisms. In theory, these liabilities can also be superior to class actions, which could incorporate valuation mechanisms into the claims process, but not in an incentive-compatible manner, at least according to the federal courts that have considered the matter.[32] With FTC oversight, the incentive difficulties could be more reliably managed. And with voluntary participation by firms, companies could be protected from being strong-armed into a liability scheme that leaves them worse off.

Although an arbitration mechanism might cause firms to internalize privacy harms more effectively because only a portion of customers would step forward to file and prosecute claims, the resulting claim filing might not accurately sort high- and low-privacy-value customers. A customer angry with the improper use, sharing, or exposure of her data might be more inclined to file a claim for relief

31. *See* FTC v. Amazon.com, Inc., 71 F. Supp. 3d 1158, 1159–60 (W.D. Wash. 2014) (denying Amazon's summary judgment request regarding billing consumers for unauthorized in-app charges incurred by children).

32. *See infra* notes 62–63 and accompanying text.

while those less concerned about privacy may be less inclined to file a claim. On the other hand, it is also conceivable that some customers who place a high value on their privacy will not bring claims because the opportunity costs of filing the claim are too high or the remedy available too small, while some low-value customers will step forward with claims because their opportunity costs are low and the remedy sufficiently large. Unless one feels comfortable concluding that the high-income, fully employed people in society tend to place a low value on privacy while the lower income and underemployed people place a high value on privacy, the "pricing" mechanism generated with arbitration will create a mismatch. If the point of the pricing is merely to force a company to correctly internalize the costs of privacy violations, this mismatch would not matter if the number of inert high-value claimants is about equivalent to the number of active low-value claimants. Without a reliable pricing mechanism, however, there is no way of knowing consumers' valuations. Indeed, odds are that the mix is not accurate. One could counter that the partial compensation is at least better than either no company liability or full liability for all customers, but without a confident sense of how far off the mark the arbitration scheme is, it does not necessarily represent a policy improvement.

Fortunately, there is a technique that could improve the sorting mechanism for claims in arbitration. In particular, if a private market in plaintiffs' claims insurance were permitted, even encouraged by the FTC, then customers who place a high value on privacy could ensure a right to be compensated for violations through the purchase of ex ante (pre-violation) insurance. Specifically, the insurer, for a premium fee, could agree to represent plaintiffs in the event that they suffer a compensable privacy violation. As part of its offered services, the insurer might also act as a privacy violation monitor. Only those customers who place a high value on privacy would likely purchase such insurance because the premiums would represent a certain financial outlay in return for only a probabilistic future payout. When the insurer also acts as market watchdog, the premium paid by the consumer could also be viewed as a type of donation to a privacy advocate seeking to hold companies accountable. In either case, customers who place a low value on privacy would not be expected to participate. Third-party insurers should be permitted to bring aggregated claims representing those customers who paid premiums prior to the discovery of a privacy violation. Otherwise, aggregated claims should not be permitted in arbitration. If the costs of the privacy violation are small, individual arbitral claims might not be feasible. And, if the harm to a privacy violation is large, then individual claims would be encouraged, further adding to ex ante deterrence.

Part I briefly describes the current FTC enforcement and class action mechanisms. It explains why each mechanism can individually lead to either too much or too little consumer data protections and points out that the concurrent use of the two mechanisms enhances the likelihood of too much data protections. Part II introduces the alternative arbitration enforcement mechanism and demonstrates why, if carefully constructed, it could produce more efficient incentives for companies. Part II also explores a number of complications and potential objections and concludes that none is strong enough to preclude experimentation of the arbitral enforcement mechanism, subject to the potential development of a third-party claims insurance mechanism.

I. FTC ORDERS, CLASS ACTIONS, AND THEIR LIMITATIONS

A. FTC Enforcement Actions

Under section 5 of the FTC Act, the agency is empowered to bring enforcement actions against firms that engage in deceptive or unfair business practices.[33] According to the FTC, a firm's action is deemed deceptive if it engages in "a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[34] In the context of consumer data privacy, a firm's actions are deemed deceptive if the company fails to comply with its own privacy policies, if it fails to take the data security efforts that it represents it takes, or if it fails to clearly disclose material information about the manner in which it will gather, use, and/or store consumer data.[35] In addition, a firm's actions can be deemed deceptive if its privacy notice is buried in documents where consumers are unlikely to find the notice,[36] if it fails to fully disclose the gathering and use of consumer information,[37] or if it fails

33. Federal Trade Commission Act, Pub. L. No. 63-203, ch. 311 § 5, 38 Stat. 717, 719 (1914) (codified as amended at 15 U.S.C. § 45(a)(1) (2012)).

34. Letter from James C. Miller III, Chairman, FTC, to Hon. John D. Dingell, Comm. Chairman on Energy and Commerce, U.S. House of Representatives, at 176 (Oct. 14, 1983), *reprinted in* Cliffdale Assocs., Inc., 103 F.T.C. 110, 174–84 (1984).

35. Solove & Hartzog, s*upra* note 12, at 628–30 (describing "broken promise" cases).

36. *See id.* at 658, 671–72.

37. *See, e.g.*, Decision and Order at 3–4, Sears Holdings Mgmt. Corp., File No. 0823099, Dkt. No. C-4264, (F.T.C. Aug. 31, 2009), 2009 WL 2979770, at *3–4.

to disclose the consequences of consumer behaviors.[38] Finally, a firm's privacy notices can be deemed deceptive if they contain overly vague statements or promises that fail to properly inform customers of the risks to their privacy.[39]

A firm's actions can be deemed unfair if they fail to comport with sound business practices in a manner that harms consumers.[40] FTC authority here is limited to prohibiting any trade practice that "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."[41] Moreover, the FTC has stated that it will not use this authority to focus on trivial, speculative, emotional, or other subjective harms.[42] Trade practices can be deemed unfair if they fail to disclose or provide information that better enables consumers to make meaningful choices among products or services. And, once a firm has put in place a data privacy policy, it is deemed unfair for that firm to unilaterally impose a retroactive change to that policy that erodes consumers' ability to rely on maintaining their privacy.[43] Moreover, firms are prohibited from using unfair product designs or software settings, by, for example, making installed software nonremovable from the customer's computer.[44] Finally, firms that fail to take reasonable and appropriate measures to secure personal information can be deemed to have committed an unfair trade practice regardless of the promises they make to their customers.[45]

38. *See, e.g.*, Complaint for Permanent Injunction and Other Equitable Relief at 25, FTC v. Frostwire, LLC, No. 1:11-cv-23643 (S.D. Fla. Oct. 7, 2011).

39. *See, e.g.*, Complaint for Permanent Injunction and Other Equitable Relief at 3–4, FTC v. Echometrix, Inc., No. 2:10-cv-05516-DRH-ARL (E.D.N.Y. Nov. 30, 2010).

40. *See* Letter from F.T.C. Chairman & Comm'rs to Hon. John C. Danforth, Member, Consumer Subcomm., Comm. on Commerce, Sci. & Hon. Wendell H. Ford, Chairman, Consumer Subcomm., Comm. on Commerce, Sci., at 1073–74 (Dec. 17, 1980), *reprinted in* Int'l Harvester Co., 104 F.T.C. 949, 1070–76 (1984).

41. 15 U.S.C. § 45(n) (2012).

42. Letter from FTC Comm'rs to Wendell H. Ford & John C. Danforth, *supra* note 40, at 1073 ("Emotional impact and other more subjective types of harm . . . will not ordinarily make a practice unfair. Thus, for example, the Commission will not seek to ban an advertisement merely because it offends the tastes or social beliefs of some viewers. . . .").

43. *See* Gateway Learning Corp., 138 F.T.C. 443, 467–73–50, 2004 WL 5662254, at *5–8 (2004) (determining that it is unfair for a firm to retroactively change its privacy practices as applied to previously collected consumer data).

44. Decision and Order at 2–4, Sony BMG Music Entm't, File No. 0623019, Dkt. No. C-4195 (F.T.C. June 28, 2007), 2007 WL 1942983, at *5–6.

45. Complaint for Civil Penalties, Injunctive and Other Equitable Relief at 8, United States v. Rental Res. Servs., Inc., No. 0:09-cv-00524-PJS-JJK (D. Minn. Mar. 5, 2009);

If, after a non-public investigation, the FTC concludes that a practice is deceptive or unfair, the FTC is authorized to obtain cease-and-desist orders, to require that companies take affirmative remedial actions, and to monitor future activities.[46] Specifically, the FTC issues a proposed complaint containing a description of the alleged violation and an order including the proposed remedy.[47] At that point the company has an opportunity to offer to settle the charges with the proposed order made available for public comment.[48] At the end of the comment period, the FTC can issue a final order.[49] Firms have substantial incentives to settle rather than challenge the complaint and order, because settlement avoids an expensive and public legal battle and does not require that the firm admit wrongdoing. Of the approximately 200 privacy-related complaints issued against companies to date, apparently only three failed to reach resolution in the form of a settlement.[50] In fact, since virtually all firms enter into settlements with the FTC, there are essentially no judicial precedents regarding the FTC's authority and development of de facto privacy policies.[51]

Although FTC authority is indeed significant, the FTC is not generally authorized to issue fines or monetary sanctions to firms engaging in unfair or deceptive trade practices.[52] In a sense, then, its authority consists of creating consumer property rules, or rules that create the right to injunction, rather than liability rules, which only require that a party pay for the damage caused by its actions.[53] In creating property rules, FTC orders tend to direct companies to undertake a line of behavior that affects all of its consumers,

Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 6, *Rental Res. Servs. Inc.*, No. 0:09-cv-00524-PJS-JJK.

46. On the process, see generally *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMM'N (July 2008), http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/556H-4YC2].

47. 15 U.S.C. § 45(b) (2012); 2 AM. BAR ASS'N, SECTION OF ANTITRUST LAW, THE FTC AS AN ANTITRUST ENFORCEMENT AGENCY: ITS STRUCTURE, POWERS AND PROCEDURES 39–40 (1981).

48. AM. BAR ASS'N, *supra* note 47, at 39–40.

49. *Id.*

50. Solove & Hartzog, *supra* note 12, at 610–11.

51. *Id.* at 606.

52. The federal courts accept the FTC's assertion of authority to seek equitable monetary relief for restitution or rescission under Section 13(b) of the Federal Trade Commission Act, but typically privacy violations do not include monetary liability. *Id.* at 611–12, 612 n.124; 15 U.S.C. § 53 (2012).

53. This important distinction originated in 1972. Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1106–10 (1972).

regardless of how individual consumers value data privacy. In creating these property rules, the FTC can also forbid the company from bargaining around the property right through a consumer contract. Instead, the regulation is more "command and control" in nature.

One potential problem with FTC orders is that the subsequent company conduct will tend to apply to all of its customers, despite significant empirical evidence that many people place a relatively low value on privacy.[54] When deciding to bring an enforcement action, the FTC might assume that all consumers will benefit from its enforcement actions, thereby drastically overestimating the proportion of consumers who would be benefitted.[55] This risk comes from the fact that consumers who are unhappy will file complaints, either on their own behalf or through consumer advocacy groups, whereas consumers who place a lower value on privacy will remain inert. If FTC regulatory actions overvalue privacy, those actions increase the cost of firms' business operations, which would have the effect of inefficiently raising prices for all of the company's products, services, and innovations, potentially eliminating some from the marketplace.[56]

Just as the FTC can take actions that overprotect privacy, it can also end up refraining from acting in ways that undervalue privacy. Because consumer harms are both subjective (hard to value monetarily by others) and heterogeneous (the value of privacy varies across consumers), the FTC might choose not to pursue enforcement actions out of a lack of demonstrated harm. Recall that significant nonsubjective harm to consumers is typically a prerequisite to FTC action on grounds of unfairness, and where harms are nonmonetary and diversely experienced, the agency could inefficiently choose not to seek to enjoin firm activities under either prong of its authority.

54. For a review of the empirical literature see Alessandro Acquisti, Curtis Taylor, & Liad Wagman, *The Economics of Privacy*, J. ECON. LITERATURE 442, 462–78 (2016).

55. Recall from the introduction that consumers with low privacy values are affirmatively harmed when FTC regulation forbids the use of technologies that aid those customers.

56. *See, e.g.*, Apple, Inc., F.T.C. File No. 1123108, at 5 (Jan. 15, 2014), https://www.ftc.gov/sites/default/files/documents/cases/140115applestatementwright_0.pdf [https://perma.cc/M446-D4M9] (dissenting statement of Commissioner Joshua D. Wright) ("[P]lacing Apple under a twenty-year order in a marketplace in which consumer preferences and technology are rapidly changing is very likely to do more to harm consumers than it is to protect them."); Testimony of J. Howard Beales III, *supra* note 7, at 17 ("Regulation or enforcement that is too stringent may reduce the risk of the particular privacy harms to which it is addressed, but it increases the risk of precluding innovations that would make everyone's life better.").

Even assuming that the FTC could accurately gauge the aggregate harm to consumers (i.e., it knows how to value both high- and low-privacy-value consumers), it will not know the relevant fraction of high- and low-value consumers, a necessary assessment to determining whether enforcement action is ultimately warranted.

Even if the FTC could reasonably assess consumer value, the cost-benefit calculus requires an assessment of the regulatory costs, which turns in part on forgone products and services, including future innovations, facts that the FTC cannot know. This extra information load on the government stems from the blunt property rights tool afforded it. If the FTC could instead simply require firms to pay for the privacy harms caused by their business practices, then the firm could itself determine whether it makes good business sense to continue its practices despite the potential for harms caused to a portion of consumers. With property rules, FTC decisions can unnecessarily harm either innovation-minded or privacy-minded consumers.

In theory, then, when (1) harms are subjective and heterogeneous, and (2) FTC actions constitute the only form of consumer protection (a counterfactual), then FTC enforcement can lead to (a) overregulation—because the FTC incorrectly overassesses the number of consumers who suffer significant harms when it acts; or (b) underregulation—because subjective and heterogeneous harms can cause the FTC to refrain from acting despite significant injury to consumer privacy. The difficulty is further exacerbated by the fact that even if the FTC accurately gauges aggregate harm, the property-rule solution fails to enable an efficient regulatory mechanism under which firms internalize the costs of their practices for future business decisions.

B. Class Actions

Sitting alongside many possible FTC enforcement actions are private lawsuits alleging state common law and statutory causes of action.[57] Individual privacy harms are typically not large enough to justify the costs of bringing individual lawsuits, but plaintiffs' lawyers can aggregate claims through class action lawsuits.[58] Although plaintiffs can and sometimes do request court orders and injunctive

57. *See, e.g.*, Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1016 (N.D. Cal. 2012) (alleging breach of contract, invasion of privacy, conversion, unjust enrichment, negligence, and state statutory claims); Claridge v. RockYou, Inc., 785 F. Supp. 2d 855, 859 (N.D. Cal. 2011) (alleging contract, tort, and state statutory claims).

58. *See, e.g.*, FED. R. CIV. P. 23.

relief, often the primary remedy pursued and granted is monetary relief.[59] The class action can thus act as a liability regime, and therefore it carries the promise of offering firms the flexibility of determining for themselves whether business practices should continue.

Despite this promise, the class action also fails to produce efficient results. To the extent that settlement is the norm because firms fear their outside exposure and wish to eliminate negative publicity, plaintiffs' attorneys will bring too many lawsuits, causing overdeterrence.[60] The potential overdeterrence problem is exacerbated if every plaintiff in the class is deemed entitled to the damages amount that reflects harm to high-privacy-value customers.

Often, however, defendants seek preliminary termination through certification fights, summary judgment motions, or other means, prior to agreeing to settle class claims. For example, a defendant could seek a determination that plaintiffs' privacy harms are not recoverable because, as subjective harms, they are too speculative. Such an argument might be deemed premature prior to trial[61] or inapt if state statutes specify statutory damages. Several courts, however, have dismissed contract claims on grounds that the privacy harms are too speculative.[62] To the extent that courts are able and willing to eliminate the possibility of plaintiff recovery, class actions could provide too little deterrence.

Part II offers arbitration as a mechanism for sorting high- and low-value consumers in a liability regime. Class actions also could serve this function. Specifically, if a defendant is liable only to the extent that individual plaintiffs collect their promised awards (a "claims-made" approach), then the need to come forward, fill out

59. *See How Do Consumer Class Action Lawsuits Work?*, OHIO STATE BAR ASS'N (June 24, 2016), https://www.ohiobar.org/ForPublic/Resources/LawYouCanUse/Pages/LawYouCanUse-358.aspx [https://perma.cc/ZV45-E33L].

60. *See In re* Rhone-Poulenc Rorer Inc., 51 F.3d 1293, 1298–99 (7th Cir. 1995) (arguing that class actions lead to "blackmail settlements" because defendants "fear . . . the risk of bankruptcy [and] settle even if they have no legal liability," rather than "stake their companies on the outcome of a single jury trial").

61. *See Claridge*, 785 F. Supp. 2d at 861.

62. *See, e.g.*, *Low*, 900 F. Supp. 2d at 1028–29 (holding that disclosure of personally identifying browsing histories did not cause damages cognizable under contract law); Cherny v. Emigrant Bank, 604 F. Supp. 2d 605, 608–09 (S.D.N.Y. 2009) (holding that alleged disclosure of a customer email address and consequent receipt of unwanted spam emails did not create recoverable harms). *But see In re* Facebook Privacy Litig., 572 F. App'x. 494, 494 (9th Cir. 2014) (mem.) (reversing the district court's determination that the sharing of personally identifiable information with advertisers did not create recoverable harm).

paperwork, show receipts, etc., can be a mechanism for sorting high- and low-value claims even where a single damages amount is assessed across all plaintiffs. Federal judges are hostile to claims-made arrangements, however, because the schemes create problematic incentives.[63] Once the defendant bargains for claims-made liability, the plaintiffs' attorneys bargain for an assessment of attorneys' fees based on the total amount available for recovery rather than the actual amounts recovered because of the delay in determining how much is actually recovered.[64] Under those circumstances neither defendants' nor plaintiffs' attorneys have any incentive to encourage plaintiffs to come forward to receive their awards. In addition, plaintiffs' attorneys sometimes worry that claims-made liabilities will result in the defendant paying too little in damages,[65] and, in any event, it ensures that the defendant has no incentive to help communicate with plaintiffs to increase the likelihood of compensation. To resolve these problems, the lawyers will typically negotiate for a fixed liability pot, with any unclaimed amounts going to a charity or organization formed to combat the type of problem at issue in the lawsuit.[66] Under these circumstances, high- and low-value consumers can be sorted, but the sorting does not affect the firm's ultimate liability, meaning that the prospect of overdeterrence continues.

63. *See, e.g.*, Stewart v. USA Tank Sales & Erection Co., No. 12-05136-CV-SW-DGK, 2014 WL 836212, at *6–9 (W.D. Mo. Mar. 4, 2014) (encouraging "the parties to confer on an alternate settlement proposal that addresses the Court's concerns"); Childs v. United Life Ins. Co., No. 10-CV-23-PJC, 2012 WL 1857163, at *4–5 (N.D. Okla. May 21, 2012) ("[U]nder the circumstances presented here and the flaws in the original notice, the Court finds that additional notice must be given."); Ferrington v. McAfee, Inc., No. 10-CV-01455-LHK, 2012 WL 1156399, at *8–10 (N.D. Cal. Apr. 6, 2012) ("This certainly suggests that . . . extinguishing the . . . class's claims for no consideration would be unfair and unreasonable.").

64. Relatedly, some assert that plaintiffs' attorneys sometimes collude with defendants so that defendants incur low liabilities (with reversionary settlements), plaintiffs' attorneys reap large fees (through clear sailing agreements), and plaintiffs end up with little or nothing. William D. Henderson, *Clear Sailing Agreements: A Special Form of Collusion in Class Action Settlements*, 77 TUL. L. REV. 813, 825–28 (2003).

65. This is particularly likely when plaintiffs suffer small damages, which is common for privacy harms. When plaintiffs suffer small damages, most will decide that it is not worth the effort and expense of claiming the award. Martin H. Redish, Peter Julian & Samantha Zyontz, *Cy Pres Relief and the Pathologies of the Modern Class Action: A Normative and Empirical Analysis*, 62 FLA. L. REV. 617, 618–19 (2010).

66. *Id.* at 634.

C. The Concurrence of FTC Enforcement and Class Actions

Firms are subject to both FTC enforcement and class action lawsuits. The possibility of a class action can alleviate the potential underdeterrence that can result when the FTC chooses not to bring an enforcement action, and, conversely, the FTC enforcement option can alleviate the potential underdeterrence that could result from an unsuccessful class action. Thus, the concurrence of these two mechanisms should shrink the underdeterrence problems that either mechanism alone faces. However, the concurrence of the two actions carries the potential of magnifying the overdeterrence problem that can exist under either mechanism. For example, settling with the FTC could add fuel to the fire of a class action lawsuit, on the grounds that harmed consumers should be compensated because the firm agreed to stop its trade practice. Indeed, when the variety of state, federal, and international enforcement tools are cumulated, overdeterrence becomes increasingly likely.

II. FTC-MONITORED ARBITRATION AS A POTENTIAL SOLUTION

This Part explores whether arbitration, coupled with claims insurance, could improve the regulation of consumer privacy. Recall that FTC enforcement orders or class actions can lead to either underdeterrence or overdeterrence, and the accumulation of enforcement actions can increase potential overdeterrence.[67] Section II.A briefly describes private arbitration and its recent use to replace consumer class actions, and it explores whether arbitration could help calibrate firm incentives to protect privacy. Section II.B discusses the importance of FTC oversight and briefly describes the FTC's prior mixed success with arbitration. Section II.C identifies claims insurance as a mechanism for mitigating a problem inherent in the arbitration scheme. Finally, Section II.D addresses a number of potential objections and complications associated with this alternative mechanism.

A. Arbitrating Privacy Harms

The problem of calibrating deterrence of privacy harms can be mitigated with enforcement schemes designed to better incorporate pricing mechanisms into firms' liabilities. The federal government could experiment with arbitration, where appropriate, as a mechanism likely to more efficiently channel consumer data use.

67. *See supra* Part I.

Arbitration typically entails private dispute resolution.[68] When parties agree to binding arbitration, they usually forfeit their rights to bring their claims to court.[69] Instead, they jointly agree to hire a third party to resolve them,[70] and they often choose the arbitration rules to be applied to their dispute.[71] Federal law and Supreme Court precedent both support this private form of dispute resolution.[72] Private arbitration is a creature of contract, and it is therefore a heterogeneous beast. Most parties anticipate that arbitration will reduce the costs of litigation[73] with reduced discovery,[74] informal hearing procedures,[75] and the use of expert arbitrators rather than generalist judges.[76] Moreover, arbitration allows claimants their "day in court" in the sense that parties' cases are not thrown out on pleading technicalities, and summary proceedings are unusual.[77]

68. CHRISTOPHER R. DRAHOZAL, COMMERCIAL ARBITRATION: CASES AND PROBLEMS 1 (3d ed. 2013).

69. *Id.*

70. *Id.*

71. For an empirical examination of choice of arbitration rules in the arbitration provisions of CEO employment contracts, see Erin O'Hara O'Connor, Kenneth J. Martin & Randall S. Thomas, *Customizing Employment Arbitration*, 98 IOWA L. REV. 133, 163–64 (2012) (finding that of 469 clauses studied, all but eighteen either articulated the governing procedures or chose pre-existing set of procedural rules to govern in arbitration) or Linda J. Demaine & Deborah R. Hensler, *"Volunteering" to Arbitrate Through Predispute Arbitration Clauses: The Average Consumer's Experience*, LAW & CONTEMP. PROBS. Winter/Spring 2004, at 55, 66–69.

72. *See* Federal Arbitration Act, ch. 392, 61 Stat. 669, 670–71 (1947) (codified as amended at 9 U.S.C. §§ 1–7 (2012)); Southland Corp. v. Keating, 465 U.S. 1, 10–16 (1984) (concluding that policy favoring enforcement of arbitration clauses requires that the Federal Arbitration Act be interpreted to apply in state courts).

73. *See* Richard W. Naimark & Stephanie E. Keer, *International Private Commercial Arbitration: Expectations and Perceptions of Attorneys and Business People: A Forced-Rank Analysis,* 30 INT'L BUS. LAW. 203, 203–09 (2002) *reprinted in*, TOWARDS A SCIENCE OF INTERNATIONAL ARBITRATION: COLLECTED EMPIRICAL RESEARCH 43, 45, 49 (Christopher R. Drahozal & Richard W. Mainmark eds., 2005) (surveying the perceptions and expectations of attorneys and their clients in commercial international arbitration).

74. 3 IAN R. MACNEIL, RICHARD E. SPEIDEL & THOMAS J. STIPANOWICH, FEDERAL ARBITRATION LAW: AGREEMENTS, AWARDS, AND REMEDIES UNDER THE FEDERAL ARBITRATION ACT § 34.1 (1994 & Supp. 1999) ("Limitations on discovery . . . remain one of the hallmarks of American commercial arbitration . . . . Avoidance of the delay and expense associated with discovery is still one of the reasons parties choose to arbitrate." (citing William L.D. Barrett, *Arbitration of a Complex Commercial Case: Practical Guidelines for Arbitrators and Counsel*, 41 ARB. J. 15, 19 (1986))).

75. Christopher R. Drahozal, *Why Arbitrate? Substantive Versus Procedural Theories of Private Judging*, 22 AM. REV. INT'L ARB. 163, 173 (2011).

76. *Id.* at 174–75.

77. *See* Mitchell L. Marinello, *Protecting the Natural Cost Advantages of Arbitration,* AM. BAR ASS'N (2008), https://apps.americanbar.org/litigation/litigationnews/practice_areas/corporate_naturalcost.html [https://perma.cc/JA2S-UBC6] ("Careful arbitrators

Finally, for small value claims, some arbitral associations have promulgated expedited procedures that enable claimants to prosecute their claims without incurring the time and expense of meeting in person.[78] Courts have obligations to enforce both private arbitration agreements and awards under international convention as well as federal and state law[79] with limited exceptions.[80]

The arbitration explored here is slightly different from that contemplated under the Federal Arbitration Act ("FAA"). A contractual obligation between the consumer and the company to arbitrate their disputes is generally enforceable under the FAA,[81] but under current law, that contractual arrangement would not eliminate the FTC's authority to bring its own enforcement action.[82] Moreover, the contractual obligation would require the consent of the consumer. The arbitration explored here would replace both private actions and FTC enforcement orders, and it posits a voluntary arrangement made between the firm and the FTC rather than between the firm and the consumer. Despite a lack of consumer consent, an agreement between the firm and the FTC that binds consumers might better protect consumer interests. The FTC is better able to insist on consumer-friendly arbitral attributes than the typical consumer, who does not even read let alone understand the implications of the arbitration agreement,[83] and who typically is presented the arbitration

are wary of motions to dismiss or for summary judgment and often will discourage or even forbid them.").

78. *See, e.g.*, AM. ARBITRATION ASS'N, COMMERCIAL ARBITRATION RULES AND MEDIATION PROCEDURES INCLUDING PROCEDURES FOR LARGE, COMPLEX COMMERCIAL DISPUTES 35 (2017), https://www.adr.org/sites/default/files/commercial_rules.pdf [https://perma.cc/5Z9D-469Y] ("Where no party's claim exceeds $25,000 . . . the dispute shall be resolved by submission of documents, unless any party requests an oral hearing, or the arbitrator determines that an oral hearing is necessary."). Conversely, although typically not present in consumer disputes, some parties choose much more formalized arbitration mechanisms with highly-trained arbitrators; these parties (as well as others) tend to choose arbitration to obtain a neutral decision maker. Drahozal, *supra* note 75, at 174–75.

79. 9 U.S.C. § 201 (2012); Unif. Arbitration Act, §§ 6–7, 7 U.L.A. 25–32 (2009); *see also Arbitration Act*, UNIF. LAW COMM'N, http://www.uniformlaws.org/Act.aspx?title=Arbitration%20Act%20(2000) [https://perma.cc/WRY9-8SU3] (showing states which have adopted the 2000 Uniform Arbitration Act).

80. 9 U.S.C. §§ 1, 10, 11.

81. Southland Corp., v. Keating, 465 U.S. 1, 7, 10–11 (1984).

82. *Cf.* Gilmer v. Interstate/Johnson Lane Corp., 500 U.S. 20, 27–29 (1991) (noting that the EEOC could still prosecute employee's claim notwithstanding clause requiring that the employee bring claims in arbitration).

83. *See* Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1174, 1179 (1983); Amy J. Schmitz, *Consideration of "Contracting Culture in Enforcing Arbitration Provisions*, 81 ST. JOHN'S L. REV. 123, 166 (2007) ("[C]orporations usually draft these form [arbitration] provisions knowing that consumers

agreement on take-it-or-leave-it terms.[84] Moreover, the arbitration explored here would be subject to FTC oversight and monitoring, which should provide further consumer protections. Admittedly, however, the scheme proposed here does not leave the arbitration choice to the consumer, and thus it potentially interferes with consumer autonomy. Because the arbitral mechanism discussed here would bind non-contractual parties as well as government enforcement agencies, it does not fall within current statutory schemes for the enforcement of arbitration agreements. Thus, Congressional legislation likely would be needed to implement this scheme, a complication that is discussed further in the next Part.

Consumer arbitration is common in the United States, but it remains controversial,[85] and it is not supported in some other countries.[86] Courts scrutinize arbitration clauses to make sure that they are not unconscionable,[87] but so long as the arbitration clauses are found in valid contracts and do not contemplate unfair procedures, they will be enforced.[88] One reason that consumer arbitration is controversial in the U.S. is that firms can use it to circumvent potential class action liability.[89] As a result, in May 2016, the Consumer Financial Protection Bureau ("CFPB") proposed a rule that would prohibit certain consumer financial product and service providers from using a pre-dispute arbitration agreement that

generally do not read or understand these provisions."); Jean R. Sternlight, *Creeping Mandatory Arbitration: Is It Just?*, 57 STAN. L. REV. 1631, 1648 (2005) ("Empirical studies have shown that only a minute percentage of consumers read form agreements, and of these, only a smaller number understand what they read." (citing Alan M. White & Cathy Lesser Mansfield, *Literacy and Contract*, 13 STAN. L. & POL'Y REV. 233 (2002))).

84. *See* David S. Schwartz, *Enforcing Small Print to Protect Big Business: Employee and Consumer Rights Claims in an Age of Compelled Arbitration*, 1997 WIS. L. REV. 53–56 (1997).

85. *See* STEVEN C. BENNETT, ARBITRATION: ESSENTIAL CONCEPTS 161–66 (2002) (discussing this controversy); Jean R. Sternlight, *Consumer Arbitration*, *in* ARBITRATION LAW IN AMERICA: A CRITICAL ASSESSMENT 127, 128–30, 140–51 (2006)).

86. Sternlight, *supra* note 85, at 139–40.

87. DRAHOZAL, *supra* note 68, at 129–36. With FTC oversight of this arbitration, court review might be unnecessary.

88. *See* David Horton, *The Shadow Terms: Contract Procedure and Unilateral Amendments*, 57 UCLA L. REV. 605, 622 (2010) ("By 1991 . . . the Court had left open just two avenues to contest arbitration clauses. First, a plaintiff could, theoretically, show that the lack of judicial forum would thwart her ability to vindicate statutory rights—though the Court had made clear that this would require forceful, specific proof. Second, arbitration clauses remained susceptible to the same defenses that applied to any contract, such as unconscionability." (footnote omitted)).

89. *See, e.g.*, Theodore Eisenberg, Geoffrey P. Miller & Emily Sherwin, *Arbitration's Summer Soldiers: An Empirical Study of Arbitration Clauses in Consumer and Nonconsumer Contracts,* 41 U. MICH. J.L. REFORM 871, 884 (2008) ("[E]very consumer contract with an arbitration clause also included a waiver of classwide arbitration.").

worked to bar the consumer from filing or participating in a class action against it.[90]

In general, however, U.S. courts must facilitate arbitrations, even when they prevent class actions. In *AT&T Mobility LLC v. Concepcion*,[91] the Supreme Court struck down California's refusal to enforce AT&T's arbitration clause on grounds that the clause was unconscionable because plaintiffs were denied a class proceeding.[92] Importantly for present purposes, AT&T's arbitration clause was designed to make arbitration both fair and feasible for any plaintiff who wished to file an individual complaint against the company.[93] Specifically, in addition to other favorable features, AT&T agreed to pay all costs for nonfrivolous claims; arbitration was to occur in the claimant's home county; all legal remedies were available in arbitration; and, in the event that the consumer received an award higher than what AT&T last offered in settlement, AT&T agreed to pay a minimum recovery of $7500 and twice the claimant's attorney's fees.[94] The *Concepcion* decision is controversial and has generated considerable criticism on grounds that arbitration can potentially be used to erode consumers' substantive rights.[95]

Whatever the relative merits of the *Concepcion* critiques,[96] this low-cost structure for resolving consumer disputes may be especially well-suited for handling subjective and heterogeneous harms, including privacy harms. As long as the financial costs of bringing an arbitration action are minimized or eliminated and the procedures adopted are fair to consumers, those plaintiffs who highly value their

90. Arbitration Agreements, 81 Fed. Reg. 32,830, 32,830 (proposed May 24, 2016). The implementation of this rule was abrogated by Congress following the 2016 elections. Act of Nov. 1, 2017, Pub. L. No. 115-74, 131 Stat. 1243 (voiding the CFPB's arbitration rule).

91. 563 U.S. 333 (2011).

92. *Id.* at 338, 340, 352.

93. *Id.* at 336–37.

94. *Id.* at 337.

95. *See, e.g.*, Karen Weise, *Consumer Protection Faces a 'Tsunami' in Court*, BLOOMBERG BUSINESSWEEK (Apr. 27, 2012), https://www.bloomberglaw.com/document/M35HLE3HBS3K [https://perma.cc/4WNB-NYLE] (quoting legal commentators describing the case as the most harmful in the history of consumer law, with the potential to virtually end class actions against businesses); Jean R. Sternlight, *Tsunami:* AT&T Mobility LLC v. Concepcion *Impedes Access to Justice*, 90 OR. L. REV. 703, 704 (2012) ("[I]f not legislatively limited, this case will substantially harm consumers, employees, and perhaps others.").

96. I have elsewhere defended *Concepcion* on the grounds that California's effective national control of the class waiver issue should be preempted in favor of federal treatment. Erin O'Hara O'Connor & Larry E. Ribstein, *Preemption and Choice-of-Law Coordination*, 111 MICH. L. REV. 647, 700–01 (2013).

privacy will have an incentive to bring claims. Those who place a low value on their privacy will not bring claims, but segregation of high- and low-value plaintiffs is desirable for more efficient pricing of privacy harms.

Granted, this arbitration scheme only allows for a binary sorting between plaintiffs, whereas consumers may value data privacy along a continuum. If so, under the binary sorting, pure-efficiency pricing is not possible. Nevertheless, the binary sort could prove surprisingly effective in the context of privacy harms. Available empirical evidence seems to indicate that when it comes to valuing privacy, people seem to lie along a bimodal distribution.[97] Some people value privacy very highly, whereas others seem to care little about privacy.[98] If consumer preferences are bimodal, then it is possible for a binary sorting mechanism to sort the two groups effectively. Of course, the effectiveness of this arbitral mechanism is highly sensitive to structure, including especially the costs and benefits of proceeding to arbitration and the remedies consumers can obtain there. But, if its features are carefully calibrated, *Concepcion*-type arbitration can "price discriminate" on the basis of subjective value, creating economic incentives that are more efficient than the present legal mechanisms used to protect privacy.

Consider the following example. Suppose that consumers entered into a relationship with Company A, receiving its goods and/or services, and thereafter A sold the consumers' data to a third party for use in behavioral marketing. Suppose further that at the time that this relationship formed, A's privacy policy stated that the consumers' information would not be shared with third parties. Alternatively, A's privacy policy could have stated that the consumers' information could be shared with third-party contractual affiliates, but it did not make clear that the company might sell the data to affiliates for use in behavioral marketing. In the first example,

97. *See* Patricia A. Norberg, Daniel R. Horne & David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, 41 J. CONSUMER AFF. 100, 101 (2007) (examining the "discrepancy between individuals' intentions to protect their own privacy and how they behave in the marketplace").

98. *See, e.g.*, Alessandro Acquisti, Leslie K. John & George Loewenstein, *What is Privacy Worth?,* 42 J. LEGAL STUD. 249, 252 (2013) (finding that consumer research subjects valued privacy more highly when anonymity was the default or initially-presented option than when disclosure was the default or first option); Jacob T. Biehl, Eleanor G. Rieffel & Adam J. Lee, *When Privacy and Utility are in Harmony: Towards Better Design of Presence Technologies,* 17 PERS. & UBIQUITOUS COMPUTING 503, 506–07 (2013) (finding that privacy preferences in the context of automatic detection of individuals' presence in the workplace tended to be distributed bimodally).

the company might be subject to both private suit and to FTC enforcement action for deception. In the second example, the company might be subject to private suit and to FTC enforcement action for both deceptive and unfair trade practices. Under this proposal, an arbitration scheme could displace both private and public actions in both examples. As an efficiency matter, the scheme works best when the privacy harms are heterogeneous and hard to forecast and where there are potential offsetting commercial benefits to consumers from A's actions.

In short, *Concepcion*-type arbitration can be superior to FTC enforcement actions because it enables the sorting of consumer harms and the pricing rather than outright prohibition of activities that produce such harms, thus leaving greater product/service flexibility for companies. And it can be superior to class actions because it does not lump all consumers together for damage-assessment purposes. As a result, subjective harms can be legally recognized and vindicated without over-deterring corporate conduct. A problem exists with this "sorting" mechanism, however, in that, at best, it only imperfectly sorts consumers. No doubt some consumers who place a high value on privacy but face high opportunity costs to their time will still not bring claims, whereas some consumers who place a low value on privacy but who face low opportunity costs would bring their claims. It is possible that the two mismatched groups would serve to cancel one another out, and calibration of the rules for recovery can help to mitigate this problem. Nevertheless, the mismatch, and some potential effects, will likely remain. Section II.C below explores one possible market mechanism that carries the potential of alleviating this weakness.

B. The Importance of FTC Oversight and Voluntary Participation by Firms

Because arbitral mechanisms can be unfair to consumers, the FTC should oversee and monitor the proposed arbitration to ensure it is consumer-friendly. Courts typically oversee the fundamental fairness of arbitration with a variety of doctrines applied to the enforcement of arbitration agreements and awards.[99] However, because the scheme envisioned here would also displace administrative orders, the FTC should play a much more active oversight role. Consumer protections are particularly important

99. DRAHOZAL, *supra* note 68, at 106–52 (examining general contract law defenses to arbitration agreements).

under the proposal because FTC-approved arbitration would take away consumer litigation rights even without the consumers' consent to arbitration. Whatever the effectiveness of consumer consent to arbitration in other contexts, it might well be wholly absent here.

Specifically, in order to replace both class actions and FTC enforcement orders, the FTC would have to approve the basic structure, applicable procedural rules (which could be adapted from any number of off-the-rack procedural rules promulgated by private arbitral organizations), and cost allocations. FTC oversight could provide the opportunity to introduce an arbitral mechanism that is more fair to consumers than that seen in the context of purely private arbitration. At a minimum, a record of the arbitrated dispute and the basis of a consumer's claim should be publicly available. The arbitral mechanism might even include an affirmative obligation to notify the company's consumers, in order to ensure that high-value consumers will have knowledge about their own claims. Consumers can be given more liberal rights of discovery as well as other rights that protect their ability to vindicate claims.

FTC-approved consumer arbitration already exists for many automobile purchasers. The Magnuson-Moss Warranty Act [100] provides a set of obligations that manufacturers must comply with when entering into a warranty with the consumer. [101] The Act encourages the use of informal dispute resolution mechanisms and directs the FTC to prescribe rules setting forth minimum standards for dispute resolution programs utilized by companies and described in their warranties.[102] Pursuant to this direction, the FTC promulgated such minimum standards, which include an annual audit of the program to ensure its compliance with the guidelines.[103] Several of the leading automobile manufacturers have instituted the Automobile Warranty Arbitration Program, which handles consumer disputes regarding automobile warranties.[104] The program is administered by

100. Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, Pub. L. No. 93–637, 88 Stat. 2183 (1975) (codified as amended at 15 U.S.C. §§ 2301–12 (2012)).

101. *Id.* §§ 102–108, 88 Stat. at 2185–89.

102. *Id.* § 110(a), 88 Stat. at 2189.

103. FTC Informal Dispute Settlement Procedures Rule, 16 C.F.R. § 703.7 (2017).

104. The FTC makes available the most recent audit of this arbitration program, which includes a general discussion of the program. *See* CLAVERHOUSE ASSOCS., 2015 AUDIT OF THE NATIONAL CENTER FOR DISPUTE SETTLEMENT (AUTOMOBILE WARRANTY ARBITRATION PROGRAM) 3–4 (2015), https://www.ftc.gov/system/files/documents/reports/2015-audit-national-center-dispute-settlement-automobile-warranty-arbitration-program/2015_ftc_national_audit.pdf [https://perma.cc/UFX4-39ZP].

the National Center for Dispute Settlement,[105] which undergoes the annual FTC-mandated audit in order to remain approved.[106]

The arbitration program standards applicable under the Magnuson-Moss Warranty Act are designed for companies to adopt ex ante, so that the warranty agreement between the company and the consumer actually contains an arbitration clause.[107] Moreover, the approved arbitral mechanism must be nonbinding, according to the FTC's rules.[108] In contrast, the proposed mechanism for privacy claims would be binding, meaning that the consumers lose their rights to bring class actions. Also in contrast to automobile arbitration, a privacy-claim arbitral mechanism could, at least in theory, be either put in place ex ante (prior to any privacy violation) or ex post (as a settlement technique for FTC enforcement actions, to be used in lieu of FTC enforcement orders). Companies heavily enmeshed in the gathering and storage of data (i.e., Google, Facebook, etc.) might obtain generalized approval for specific types of future claims/actions, much as the automobile manufacturers have done for warranty disputes. Other companies might not be able to forecast a significant likelihood of FTC enforcement actions. In order for the arbitral scheme to work for them, the target companies would have to negotiate with the FTC for an arbitral mechanism after complaints/investigations materialize. Presumably these ex post arbitral schemes could benefit from the guidance provided by ex ante mechanisms. Alternatively, the FTC could set up its own arbitral

105. *See id.* at 4. Other major American automobile manufacturers utilize the Better Business Bureau ("BBB") Auto Line arbitration program. *See* Agency Information Collection Activities, 82 Fed. Reg. 8614, 8615 (Jan. 26, 2017) (identifying the two arbitration programs operating under the FTC's Dispute Resolution Rule as the National Center for Dispute Settlement and the BBB Auto Line program); *see also Participating Auto Manufacturers*, BETTER BUS. BUREAU, https://www.bbb.org/autoline/bbb-auto-line-process/participating-auto-manufacturers/ [https://perma.cc/R99S-Q47P] (listing over two dozen participating manufacturers).

106. *See* 16 C.F.R. § 703.7(a).

107. *Cf.* Cunningham v. Fleetwood Homes of Ga., Inc., 253 F.3d 611, 622 (11th Cir. 2001) (holding that the failure to disclose in the warranty a term or clause requiring the utilization of an informal dispute resolution mechanism "contravenes the text, legislative history, and purpose of the Magnuson-Moss Warranty Act").

108. 16 C.F.R. § 703.5(j). Binding arbitration is, however, not precluded by the regulations as long as both parties agree to it. *See* Rules, Regulations, Statements, and Interpretations Under Magnuson-Moss Warranty Act, 40 Fed. Reg. 60,167, 60,211 (Dec. 31, 1975) (clarifying that a warrantor and a consumer could agree to submit their dispute to binding arbitration either after the Mechanism has rendered a decision or instead of proceeding under the Mechanism, but that binding arbitration may not be mentioned in the written warranty).

mechanisms that companies could opt into as part of its settlement with the FTC or as part of the company's contract with consumers.

FTC oversight can prevent a number of potential problems that might arise for company-instituted arbitration. When enforcing arbitration agreements in consumer contracts, courts often seek to ensure that firms do not fashion unfair processes,[109] and the FTC should assume that role under this scheme. In addition, courts are sometimes concerned about a potential repeat-player effect, which can arise when the company participates in repeated arbitrations but the consumers each participate only once.[110] To obtain the firm's repeat business, arbitrators' determinations might unduly favor the firm.[111] Potential repeat-player problems could be handled by having the FTC refer complaining consumers to a panel of potential lawyers who routinely handle claims in arbitration. In fact, if a given advocate represents multiple consumers who file similar claims against a firm, then the advocate could possibly aggregate those claims in order to achieve cost efficiencies. Alternatively, the FTC could decertify those arbitrators who show a bias in favor of company rulings. Making public the arbitration claims and rulings can help defuse the potential for repeat player bias. If the FTC sets up its own arbitration, it could hire consumer-friendly arbitrators.

Furthermore, if a firm faces liability only to the extent that consumers are willing to file claims, the firm might have little incentive to alert consumers to the presence of the arbitration scheme. In order to overcome this difficulty, the FTC might require that the company widely distribute information about the arbitration option to consumers, at least once an FTC investigation and complaint indicates that remedial actions might be warranted. The FTC could also notify consumers of active arbitrations on its websites.

109. *See* DRAHOZAL, *supra* note 68, at 690.

110. *See* Mercuro v. Superior Court, 116 Cal. Rptr. 2d 671, 678–79 (Cal. Ct. App. 2002) (striking the arbitration clause and noting that employer's choice of arbitral forum resulted in only eight available arbitrators, which created a potential repeat player effect).

111. For discussions of a possible repeat player effect, see Lisa B. Bingham, *Employment Arbitration: The Repeat Player Effect*, 1 EMP. RTS. & EMP. POL'Y J. 189, 209–10 (1997); Lisa B. Bingham, *On Repeat Players, Adhesive Contracts, and the Use of Statistics in Judicial Review of Employment Arbitration Awards*, 29 MCGEORGE L. REV. 223, 238–39 (1998); Sarah Rudolph Cole, *Incentives and Arbitration: The Case Against Enforcement of Executory Arbitration Agreements Between Employers and Employees*, 64 UMKC L. REV. 449, 472–79 (1996); Alexander J.S. Colvin, *An Empirical Study of Employment Arbitration: Case Outcomes and Processes*, 8 J. EMPIRICAL LEGAL STUD. 1, 14–15 (2011). The repeat-player problem can be mitigated by, for example, using a large pool of arbitrators or enlisting arbitration-experienced advocates to represent consumer interests.

Consumer advocates also might have a financial incentive to notify consumers of potential claims.

Finally, the FTC might impose rules designed to ensure that consumers do not face overly-large costs to bringing claims. While opportunity and financial costs can operate as a valuable mechanism for sorting consumers who place high and low values on privacy, sorting requires that the effective costs to arbitration be low enough to attract high-privacy-value consumers. Thus, costs would need to be carefully scrutinized. Indeed, one requirement of the automobile warranty arbitration is that the consumer bear no financial costs to arbitrate.[112] Perhaps overall administrative costs can be reduced with aggregated claims options through insurance and/or by enabling single arbitrators to handle multiple similar claims individually.

Voluntary participation by firms is equally important. Assuming that the FTC seeks to oversee arbitration in the best interest of consumers,[113] it would ensure that arbitrations are procedurally fair to, and protect the substantive rights of, consumers. However, excessive consumer rights could impose dispute resolution costs on firms that are so large that the overdeterrence problem mentioned earlier is not actually alleviated. If firms retain the right to opt into or out of an FTC-approved program, then any resulting arbitration mechanisms should be Pareto-superior[114] to current legal enforcement mechanisms. Mechanically, firms could seek approval for proposed arbitration schemes, followed by FTC feedback and pushback, followed by a firm's decision whether to participate in an arbitral scheme as shaped by the FTC. A credible threat not to participate in the FTC-shaped arbitration could enable a firm to negotiate to a mutually agreeable position with the FTC. Note that legal rules,

112. 16 C.F.R. § 703.3(a). However, this rule has been interpreted to allow for some costs to be placed on consumers, including "initially notifying the Mechanism of the dispute, . . . provid[ing] the information needed by the Mechanism to fairly resolve the dispute[,] . . . . developing and submitting any rebuttal evidence," and obtaining copies of any "Mechanism records relating to the dispute." *See* Rules, Regulations, Statements, and Interpretations Under Magnuson-Moss Warranty Act, 40 Fed. Reg. 60,019, 60,204 (1975) (codified at 16 C.F.R. § 703). "Except for the cost of notifying the Mechanism and the cost of complying with reasonable requests for necessary information," all other costs able to be placed on the consumer are voluntary costs and "the Mechanism will still render a decision" even if the consumer decides not to bear the costs. *Id.*

113. Consumer protection is the FTC's charge, although agency capture theorists might challenge this assumption. For a discussion of agency capture in industries charged with consumer protection, see Rachel E. Barkow, *Insulating Agencies: Avoiding Capture Through Institutional Design*, 89 TEX. L. REV. 15, 64–78 (2010).

114. Pareto-superior policies make some people better off without harming others. *See* David S. Bullock, *Are Government Transfers Efficient? An Alternative Test of the Efficient Redistribution Hypothesis*, 103 J. POL. ECON. 1236, 1237 (1995).

which force firms into court, would not achieve this important corporate buy-in.

C. Third-Party Insurer/Monitors

As mentioned in Section II.A above, the central problem with using arbitration to effectively price privacy is that the sorting mechanism will be imperfect. In particular, some decisions to file (or not to file) claims in arbitration will be motivated by the consumer's opportunity costs as reflected in employment, wages, and other matters rather than by the degree to which the consumer actually values privacy. One way to treat this problem is to enable higher earning consumers to obtain higher arbitration awards than those awarded to lower earning consumers. Perhaps some privacy violations would naturally lead to such damage patterns (i.e., identity theft or loss of reputation/income), but categorically awarding damages based on the income of the claimant seems problematic due to perceived class discrimination.

An alternative mechanism that could alleviate the mismatch between claims and privacy valuations would be claims insurance made available to consumers prior to the privacy violation(s) in question. With claims insurance, a third-party insurer would offer to prosecute arbitral claims on behalf of consumers for a premium paid prior to any actual privacy violations that affect the consumer. In the event that the arbitral mechanism becomes available to plaintiffs who were harmed by violations, the insurer would undertake a duty to bring claims on behalf of insured consumers and to pay over to consumers some or all of any amounts collected on behalf of the consumer. Ex ante, consumers are much more likely to purchase such insurance based on their valuation of privacy protections rather than based on opportunity costs. Indeed, to the extent that opportunity costs do influence the ex ante insurance decision, it will be in the direction of having high-privacy-value, high-opportunity-cost individuals be more inclined to pay the premium.

Claims insurers might also advocate for greater substantive privacy protections on behalf of their customers. With strong reputations as privacy advocates, the insurers can attract more high-privacy-value customers. Indeed, it is conceivable that some firms wishing to signal that they respect consumer privacy might facilitate the insurer's services or even offer to pay the insurance premiums on behalf of the customers. However, this type of signaling will require a regulatory regime that preserves the firm's growth and innovation possibilities.

If the third-party insurer files claims on behalf of all its consumers, perhaps the insurer should be permitted to aggregate these claims. With a sufficiently successful insurance option, the aggregated claims could begin to resemble a class claim. Nevertheless, the insurer's aggregated or "class" claim would have the advantage of including only high-privacy-value plaintiffs. As a result, the difficulties posed in the class actions described above would not be present.

If the insurer is permitted to aggregate its customers' claims, then arbitrators could perhaps charge claimants at least modest administrative fees to help cover the costs of arbitration. These fees could help to discourage low-privacy-value, low-opportunity-cost plaintiffs from free-riding off the efforts of the privacy advocates after an aggregate claim has been filed. At the same time, if the costs are sufficiently modest, some high-privacy-value consumers who did not purchase insurance on the front end could file claims once a company's privacy violation has become apparent. Under such a scheme, it is at least theoretically possible that the high-privacy-value consumers purchase insurance, leading to feasible claims prosecution, or add their claims after the fact, and the low-privacy-value consumers are effectively foreclosed from asserting claims.

Note that under a third-party insurance scheme, the insurance effectively serves as the pricing mechanism, while the arbitration is merely a consumer-friendly forum, which serves to substitute away from the overdeterrence problems associated with the conjunction of class actions and FTC enforcement orders. If the arbitration scheme were available after an FTC investigation determined that the company had committed a privacy violation, these are the very cases where both FTC actions and class action claims are currently likely, and this conjunction represents the greatest risk of overdeterrence. The proposed arbitration mechanism corrects the overdeterrence problem by eliminating the conjunction, effectively substituting property-rule FTC enforcement for liability rules, and preventing class awards from assuming that all customers place a high value on privacy.

Even if the overdeterrence problem can be corrected, or at least substantially ameliorated with the proposed arbitration, what about the potential for underdeterrence? Under the current enforcement regime, underdeterrence can result from a number of sources, including inevitable budget constraints and other scarce resources for the FTC. Currently, class actions are available to supplement FTC enforcement efforts, thereby helping to ameliorate underdeterrence problems. To help ease the potential for underdeterrence, the pre-negotiated arbitration scheme should replace consumer class actions even in cases where the FTC has not filed a complaint against the company. In short, insurers and harmed consumers should have independent enforcement authority. If so, then the class arbitration would serve to lessen both overdeterrence (by sorting claimants) and underdeterrence (by providing investigation and enforcement independent of the FTC).

The question remains whether there can be a market for third-party claims insurance. In order for such a market to exist, there must be (1) an absence of legal barriers to the offering of such insurance (fueling the supply side); (2) an absence of, or ability to eliminate the risks of adverse selection and moral hazard;[115] and (3) a sufficiently large pool of high-privacy-value consumers who are willing to purchase the insurance (fueling the demand side). Assuming no legal barriers to the offering of claims insurance,[116] are there adverse selection or moral hazard problems? Adverse selection problems[117] do not really apply to consumers, who are not exhibiting risks relevant to the insurance premium.[118] Moral hazard problems[119] could arise under our proposed scheme if consumers who purchase claims insurance are less likely to take measures to protect their own privacy in situations where both firms and consumers should take care to protect privacy. Presumably either the scope of the claims coverage or

115. *See, e.g.*, Tom Baker, *Containing the Promise of Insurance: Adverse Selection and Risk Classification*, 9 CONN. INS. L.J. 371, 373–74 (2003).

116. In the United States, this is called a prepaid legal service plan. *See generally* John R. Dunne, *Prepaid Legal Services Have Arrived*, 4 HOFSTRA L. REV. 1 (1975) (describing the advent and development of prepaid legal services); Brian Heid & Eitan Misulovin, *The Group Legal Plan Revolution: Bright Horizon or Dark Future?*, 18 HOFSTRA LAB. & EMP. L.J. 335 (2000) (discussing the details and recent growth of prepaid group legal plans which allow the spreading of legal services among many to make them more affordable).

117. Adverse selection refers to the "theoretical tendency for low risk individuals to avoid or drop out of insurance pools." Baker, *supra* note 115, at 373.

118. The result of adverse selection is that insurance pools, absent countervailing efforts by administrators, tend to contain a disproportionate percentage of high-risk individuals. *Id.* In the context of insurance claims, however, consumers presumably do not possess asymmetric information about the risk that firms they deal with will violate consumer privacy rights. As a result, all consumers theoretically share equally in the information that firms may violate consumer privacy rights, thereby rending all consumers "at-risk."

119. Moral hazard refers to the "change in incentives that can result from insurance protection." *Id.* There tends to be an inversely proportional relationship between protection and risk, whereby "[r]isks that pose a very high degree of moral hazard typically are not insurable at all," such as intentional harm. *Id.* at 374.

the applicable rules applied to the privacy claim could take into account the mutual care issue, where it is present.[120]

The most pressing potential impediment to the rise of a third-party insurance market is the possibility that too few consumers value privacy highly enough to purchase such insurance. The greater the number of consumers who are willing to purchase the insurance, the cheaper the premium, given that aggregation of consumer claims in arbitration should reduce the costs per consumer of prosecuting future claims. Available empirical evidence indicates that although consumers often express opinions that suggest they place a high value on privacy, in practice consumers tend to be willing to pay relatively little for privacy protections.[121] At the same time consumer willingness to sign away privacy rights appears to be heavily contingent on the framing of the issue.[122] Specifically, consumer willingness to share data can turn on the playfulness of the website design or the specific pieces of information over which consumers are given control.[123] One way that third-party insurers might be able to induce consumers to purchase the insurance is to overcome consumer ignorance of the risks they face by calling to mind specific risks to consumers.[124]

Plaintiffs' claims insurance does not seem to exist in the U.S., although that is likely due to the fact that contingency fees serve to minimize risks for plaintiffs.[125] In Germany, where contingency fees are not permitted, plaintiff-side litigation insurance is common.[126]

120. *See id.* at 373–74 (explaining that insurers often require the consumers to relinquish control, such as over the settlement and defense of claims, or retain "coinsurance" to protect from moral hazard problems). It helps that the claims coverage conceived here gives the insurer, rather than the consumer, control over the litigation decision. *See id.*

121. Acquisti et al., *supra* note 54, at 41; Norberg et al., *supra* note 97, at 103, 118.

122. *See* Somini Sengupta, *Letting Down Our Guard*, N.Y. TIMES, Mar. 31, 2013, at BU1.

123. *Id.* (explaining, for example, the increased willingness to provide identifying information such as date of birth on Facebook).

124. *Cf.* Timothy Morey, Theodore Forbath & Allison Schoop, *Customer Data: Designing for Transparency and Trust*, HARV. BUS. REV. (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust [https://perma.cc/KLV7-HPLC] (noting that consumers are typically ignorant of the specific types of data sharing and uses to which they are subject).

125. *Cf.* Samuel R. Gross, *We Could Pass a Law . . . What Might Happen if Contingent Legal Fees were Banned*, 47 DEPAUL L. REV. 321, 330–35 (1998) (discussing the relationship between contingent fees and plaintiffs' litigation insurance).

126. Forty percent of West German households studied in 1979 had purchased insurance covering at least some legal expenses. Erhard Blankenburg, *Legal Insurance, Litigant Decisions, and the Rising Caseload of Courts: A West German Study*, 16 LAW & SOC'Y REV. 601, 605 (1981–82).

Additionally, the costs to providing claims insurance would be smaller where fee shifting is permitted, a common feature in private arbitration [127] that could be incorporated into FTC-approved arbitration mechanisms. In the end, the development, or not, of a claims insurance market could itself provide useful empirical evidence of the extent to which consumers actually value privacy protection.

D. *Other Complications and Objections Considered*

What are other potential objections to such an arbitration scheme? Even if arbitration could work well in some circumstances, are there circumstances where it should not be used? This Section considers possible objections and complications and concludes that, while some may limit the circumstances in which the proposed scheme could be feasibly implemented, none provide compelling arguments against experimentation.

1. Arbitration Schemes Risk Potential Underdeterrence

If too few consumer claims are filed in arbitration, privacy violations would be underdeterred.[128] This potential problem should be treated within the arbitration scheme rather than rejecting arbitration altogether. If significant numbers of consumers who claim to place a high value on their privacy nevertheless fail to come forward, the problem could result either from costs associated with the arbitration or a failure to effectively inform consumers of their right to redress. Arbitration costs can be addressed over time by tailoring the cost structure of the arbitration. Information problems can be addressed through joint efforts by the firm, the FTC, and

127. *See* O'Hara O'Connor et al*., supra* note 71, at 164–66 (evaluating an empirical study of arbitration clauses in CEO employment contracts and finding that many either provided for or assumed the possibility of attorney fee-shifting).

128. For an example of this charge, see the CFPB's recent report to Congress on the use of arbitration clauses in consumer financial instruments. CONSUMER FIN. PROT. BUREAU, ARBITRATION STUDY: REPORT TO CONGRESS, PURSUANT TO DODD-FRANK WALL STREET REFORM & CONSUMER PROTECTION ACT § 1028(A) app. A, at 7 (2015) ("[C]ritics argue that arbitration clauses . . . may undermine deterrence and leave widespread wrongdoing against consumers unaddressed."). The CFPB presents findings indicating that litigation outcomes are more successful for consumers than are individual arbitration outcomes. *Id.* § 1, at 11–15. The development of a claims insurance market under the proposed scheme could produce better incentives because it would allow aggregation, similar to class actions, without enabling plaintiffs' attorneys to demand damages for low-privacy-value plaintiffs. *See* Thomas H. Koenig & Michael L. Rustad, *Fundamentally Unfair: An Empirical Analysis of Social Media*, 65 CASE W. RES. L. REV. 341, 370 (2014) ("[P]redispute arbitration clauses . . . discourage filings—therefore shielding [companies] from any accountability for breach of [terms of use], tort claims, intellectual property rights, privacy violations, or other causes of action.").

plaintiffs' advocate/lawyers to disseminate information about firm violations and the arbitration option. If, notwithstanding well-drafted arbitration schemes and significant efforts to disseminate information, many consumers fail to step forward to exercise their rights through arbitration, through insurance schemes or otherwise, it may be reasonable to conclude that the passive consumers do not, in fact, value their privacy at sufficiently high values to register their grievances and collect compensation. That revelation would not be one of underdeterrence but rather of overprotection of privacy with formal legal rules. If there are specific contexts where underdeterrence seems particularly likely or costly, the FTC might refuse to displace its regulatory authority or may refuse to permit the use of the arbitral scheme.

2. Privacy Should Be Protected via Property Rules, Not Liability Rules

Privacy advocates might object to the use of liability rather than property rules to protect privacy on grounds that consumers who value privacy at high levels will not be satisfied with ex post monetary awards when that privacy is violated. After all, the creepiness or loss of dignity associated with privacy violations may be incommensurable with money.[129] Although this objection could limit the political feasibility of this arbitration scheme, it should not displace experimentation altogether. As some scholars have pointed out, one difficulty with obtaining consumer consent for the use of data is that consumers often do not know until after the fact whether they will object to particular uses of their data simply because it is too hard to imagine all possible data uses at the time that consent is obtained.[130] In this world where consumers cannot forecast future privacy harms, even high-value consumers might agree to liability rules, which can judge corporate actions after the fact, when it is known how the information was used, and by whom.

129. Julie E. Cohen, *Examined Lives: Information Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1398 (2000); Clyde W. Summers, *Individualism, Collectivism and Autonomy in American Labor Law*, 5 EMP. RTS. & EMP. POL'Y 453, 483 (2001).

130. *See* Andrew W. Bagley & Justin S. Brown, *Limited Consumer Privacy Protections Against the Lawyers of Big Data*, 31 SANTA CLARA COMPUTER & HIGH TECH. L. J. 483, 496–97, 518–19 (2014) ("[C]onsenting [consumers seem] to be making a long-term commitment to the control of their data by other parties for uses that are unimaginable at the time of consent.").

3. Actual Fraud/Intentional Deceit Should Still Be Enjoined

The arbitration scheme works best in cases where it is important to carefully calibrate firm incentives such as unintentional disclosure of private consumer information. Instances in which overdeterrence is less problematic, such as intentional wrongdoing, may be better regulated by the current regulatory scheme. In cases alleging fraud or intentional deception, however, the FTC or other enforcing plaintiff should be required to show fraudulent intent on the part of the target firm, and that intent must be present at the time that the firm issued its disclosures, privacy policies, etc. These are standard elements of common law fraud,[131] so the limitation is in no way radical. But the important point is that the FTC should not be able to claim "deception" or "unfairness" without satisfying the elements of common law fraud, in cases where the arbitration scheme is not permitted.

4. Protection of Health Information Should Not Require Affirmative Action by Patients

Consumer preferences may be significantly less heterogeneous regarding the use and dissemination of at least some forms of health information, and, on average, patients appear to highly value protection of their health information.[132] Without heterogeneous preferences, the problems associated with consumer valuation are somewhat mitigated, and with high valuations, the potential overdeterrence problem is also mitigated. Under these circumstances the case against the current regime of FTC enforcement orders and class actions fades.

Yet, perhaps arbitration mechanisms should at least be considered as an option for those health privacy violations that trigger very different responses across patient populations. For example, while a healthy majority of patients might be uncomfortable sharing their mental health histories and problems, patients might face heterogeneous preferences about the disclosure of other conditions

131. *See* RESTATEMENT (SECOND) OF TORTS § 525 (AM. LAW INST. 1977).

132. Joy L. Pritts, *The Importance and Value of Protecting the Privacy of Health Information: The Roles of the HIPAA Privacy Rule and the Common Rule in Health Research*, DIVISION OF MED. OF THE NAT'L ACADS. OF SCI. ENGINEERING, & MED. 1, 5–8 (2008) http://iom.nationalacademics.org/~/media/Files/Activity%20Files/Research/HIPAAandResearch/PrittsPrivacyFinalDraftwed.ashx [https://perma.cc/BAC6-5J2B] (discussing the importance of protecting the privacy of health information by reviewing public attitudes toward the privacy of health information and discusses the value that privacy serves in the health case context).

like ear infections or headaches. In these circumstances, heterogeneous preferences and the possibility of overdeterrence for some health data uses are present, indicating that the arbitration mechanism could improve matters.

Moreover, many of the security breach issues for medicine are similar to those found in the general commercial context. Medical records routinely contain Social Security numbers, addresses, and next of kin, and access to insurance information facilitates the filing of fraudulent claims, making medical data every bit as valuable to hackers as commercial data.[133] In fact, healthcare organizations accounted for nearly half of all major data breaches in 2014,[134] which suggests that differential treatment across the board may not be warranted.

5. Security Beaches Cause Externalities by Encouraging Hacking of All Firms, and Arbitration is Unlikely to Capture that Cost

Incentives to hack may be present regardless of the incidence of actual breaches. That said, firms with more highly-valued information should make more efforts to protect consumer data from potential hackers. A well-constructed arbitration scheme should be able to sort these firms from those with low-value information. Moreover, a well-constructed arbitration scheme should be better able to value consumer privacy, especially in the face of heterogeneous consumer privacy values. Security breaches capture a lot of press attention, and they cause widespread concern among consumers, at least in the short term.[135] For these reasons it may not be politically feasible to relegate

133. Caroline Humer & Jim Finkle, *Your Medical Record is Worth More to Hackers than Your Credit Card*, REUTERS (Sept. 24, 2014, 2:25 PM), http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924 [https://perma.cc/D8D7-3UM9].

134. Greg Slabodkin, *2014 Was Landmark Year for Health Data Breaches,* HEALTH DATA MGMT. (Dec. 26, 2014, 7:46 AM), http://www.healthdatamanagement.com/news/2014-Landmark-Year-for-Health-Data-Breaches-49505-1.html [https://perma.cc/CAQ9-4FXB].

135. *See, e.g.*, Melanie Eversley & Kim Hjelmgaard, *Target Confirms Massive Credit-Card Data Breach*, USA TODAY (Dec. 19, 2013), https://www.usatoday.com/story/news/nation/2013/12/18/secret-service-target-data-breach/4119337/ [https://perma.cc/SU3P-9WP9]; Greg Farrell & Patricia Hurtado, *JP Morgan's 2014 Hack Ties to Largest Cyber Breach Ever*, BLOOMBERG BUSINESSWEEK, (Nov. 10, 2015), https://www.bloomberg.com/news/articles/2015-11-10/hackers-accused-by-u-s-of-targeting-top-banks-mutual-funds [https://perma.cc/PW7Y-DHUV (staff uploaded archive)]; Gordon Kelly, *eBay Suffers Massive Security Breach*, *All Users Must Change Their Passwords*, FORBES (May 21, 2014), https://www.forbes.com/sites/gordonkelly/2014/05/21/ebay-suffers-massive-security-breach-all-users-must-their-change-passwords/ [https://perma.cc/92C9-UGGN]; Jeff John Roberts, *Home Depot to Pay Banks $25 Million in Data Breach Settlement*, FORTUNE

claims involving data security breaches to the more private forum of arbitration. On the other hand, public attention to company behaviors can be achieved through other mechanisms. For example, perhaps political issues can be handled by calling firm leaders to explain themselves to Congressional committees, with testimony aired by C-SPAN and other news channels. If so, public shaming can provide additional incentives for companies to take care, suggesting that arbitration could potentially work here too.

6. The Arbitration Scheme Would Require Congressional Action and Therefore Could Flounder Politically

The proposed arbitration might well require congressional action. Current FTC authority does not extend to the imposition of monetary liability, and although the FTC presumably could promise to refrain from section 5 enforcement actions in return for any number of firm promises, its oversight role in the arbitration scheme likely would require congressional action. Current and past arbitration schemes monitored by the FTC were affirmatively authorized and directed by Congress in the Magnuson-Moss Warranty Act,[136] so they do not provide precedent for FTC authority to institute or manage the arbitration of privacy claims. Moreover, if the arbitration scheme works to displace class actions, congressional authorization could similarly be required. Currently, individual arbitration can replace class actions under the FAA, but that statute's operation requires an agreement to arbitrate between the parties,[137] whereas the proposed arbitration scheme would operate even in the absence of consumer agreement. As a consequence, separate statutory authorization would be required.

Several consumer privacy statutes have, of late, been thwarted in Congress, and this one could also flounder. Industry advocates have killed recently proposed statutes that stalled in congressional

(Mar. 9, 2017), http://fortune.com/2017/03/09/home-depot-data-breach-banks/ [https://perma.cc/Z5PV-PQFF (staff-uploaded archive)]; Jonathan Stempel & Jim Finkle, *Yahoo Says All Three Billion Accounts Hacked in 2013 Data Theft*, REUTERS (Oct. 3, 2017), http://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1 [https://perma.cc/KB5U-LTAT]; Gillian B. White, *A Cybersecurity Breach at Equifax Left Pretty Much Everyone's Financial Data Vulnerable*, THE ATLANTIC (Sept. 7, 2017), https://www.theatlantic.com/business/achrive/2017/09/Equifax-cybersecurity-breach/539178/ [https://perma.cc/KR4U-AAT4].

136. Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, Pub. L. No. 93-637 § 110(a), 88 Stat. 2183, 2189–90 (1975) (codified as amended at 15 U.S.C. § 2310(a) (2012)).

137. *See* 9 U.S.C. §§ 2–4 (2012).

committee.[138] Unlike other bills, however, this proposal circumvents the status quo only if companies agree to arbitration. Because this scheme costs firms nothing unless they affirmatively choose to participate, proposed legislation should experience less industry resistance. To the extent this proposal threatens to replace the current tools for privacy advocates, however, it could fail to garner the requisite support for passage. On the other hand, with the promise of FTC oversight and the prospect of greater protection for high-privacy-value consumers, a carefully formulated proposed scheme could become a grand bargain between industry and privacy advocates.

7. Arbitration Might Be a Poor Forum for Law Creation

Arbitration is not generally viewed to be a superior forum for the development of law because it is typically closed to the public and an arbitrator's decision generally does not create precedent.[139] Privacy law is underdeveloped and must pay very careful attention to technological advances, so one might conclude that privacy law needs to advance considerably before an arbitration option could perform well.[140] This critique suggests, at a minimum, that privacy arbitrations should be open to the public and arbitrators should be required to follow FTC statements about sound privacy policy. Public participation and FTC evaluation of the legal principles developed in arbitration can both help to steer legal development in healthy, carefully-deliberated directions. Because the arbitrators can develop an expertise in the area of privacy, their decisions might well prove superior to those of generalist judges. And if the firms want assurances of predictable legal rules, the arbitrators could adopt a system of precedent. The inability of firms to appeal the arbitrator's decision might cause the firms to be wary of agreeing to the arbitration scheme, so perhaps an option to appeal to the FTC

138. *See, e.g.*, John Brodkin, *For Sale: Your Private Browsing History*, ARS TECHNICA (Mar. 28, 2017), https://arstechnica.com/tech-policy/2017/03/for-sale-your-private-browsing-history/ [https://perma.cc/DZA8-6J5H] (quoting U.S. Representative Mike Doyle as stating that many companies rely on lobbying efforts to defeat privacy bills); Kate Tummarello, *'Big Data' Lobbyist: Congress Doesn't Want Online Privacy Law*, THE HILL (Aug. 19, 2014), http://thehill.com/policy/technology/215457-big-data-lobbyist-congress-doesnt-want-online-privacy-law [https://perma.cc/XS8D-A6BZ] ("A lobbyist for one of the top companies that trades in consumer data is confident that Congress won't set rules for how online marketers use information about consumers."); *see also supra* note 3.

139. Christopher R. Drahozal, *Is Arbitration Lawless,* 40 LOY. L.A. L. REV. 187, 207–14 (2006).

140. Special thanks to Robert Jackson for identifying this critique.

Commissioners could be incorporated.[141] In any event, more careful thought on this front is highly advisable.

CONCLUSION

A critical missing component of the regulation of consumer data use is a pricing mechanism. The FTC, consumer advocates, and plaintiffs' attorneys all correctly assert that privacy protection is an important goal of sound government policies, but translating that norm into the realm of consumer data use is difficult. Privacy harms are subjective, and consumers seem to vary significantly in their attitudes toward many uses of consumer data. The subjective nature of privacy harms can lead the FTC and the courts to not impose damages or restrictions on firm behavior, even when that the firm's actions cause harm. When the government does regulate consumer data use out of a commitment to privacy, it likely ends up overregulating firm behavior, given that consumer harm is heterogeneous. Without an effective pricing mechanism, the risk of any one government actor's decision causing overdeterrence or underdeterrence remains significant. Given that multiple government actors can effectively regulate firm behavior, the overdeterrence risk seems more likely.

This Article offers a separate regulatory possibility that could incorporate a pricing/sorting mechanism into consumer redress for privacy harms: FTC-approved mandatory arbitration of consumer claims that would replace both FTC enforcement orders and class action litigation. In particular, the arbitration mechanism proposed here would seek to set an effective "price" for redress, in terms of both opportunity costs and out-of-pocket expenses, that would enable high-privacy-value consumers to bring claims while foreclosing those by low-privacy-value consumers. The sorting mechanism here is imperfect, however, because it would have a tendency to also sort claimants according to the opportunity costs of their time rather than solely according to their preferences regarding privacy. A third-party consumer claims insurance mechanism, under which the third party obtains an ex ante premium from the consumer and, in return, agrees to prosecute claims on behalf of the consumer in the event of a firm privacy violation, could work to more effectively sort the high- and low-privacy-value consumers. A question remains whether such a

141. Of course, this option might add to the FTC's administrative burden, but arbitration fees paid by the companies could enable the hiring of support personnel to assist.

complicated mechanism is viable. Experimentation with the FTC-approved arbitration should nevertheless proceed to make room for the possibility of a regulatory regime that, at least in some quarters, might substantially improve the pricing of privacy.