wiley

ARTICLE

# E-Commerce—The Next Target of 'Big Data' Class Actions?

*Law360*
January 5, 2016

Not surprisingly, the rise of "big data" has generated a significant amount of class action litigation. To date, however, that litigation—which has focused primarily on data loss or data security breaches—has been only marginally successful. In data security cases, plaintiffs have struggled to demonstrate an actual and imminent injury-in-fact as opposed to a future injury that could result from a third party's misuse of a plaintiff's personal information.

But that may soon change. Late last year, computer science researchers from Northeastern University in Boston published a report purporting to demonstrate that e-commerce websites are using data regarding individuals' online shopping habits to charge different prices and offer different products to different customers.[1] Although it is well known that tracking of consumer preferences by e-commerce sites has occurred for some time and allows those businesses to offer many benefits to customers, the study[2] purported to be the first to examine comprehensively how that data is used by a wide spectrum of e-commerce vendors to engage in two practices—price discrimination and price steering—which arguably result in certain consumers unknowingly paying inflated prices for online products and services.

While "dynamic pricing" has generally not been considered illegal, the inflated prices could expose e-commerce vendors to consumer fraud and unfair trade practices lawsuits in jurisdictions with broad consumer protection statutes. Indeed, a recent White House report on big data and differential pricing discussed the Northeastern report and expressly noted that "differential pricing" could put consumers at risk of harm.[3]

## Authors

Stephen J. Obermeier
Partner
202.719.7465
sobermeier@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

## Practice Areas

Litigation

Privacy, Cyber & Data Governance

Given the existence of a number of jurisdictions with extremely broad and flexible consumer protection statutes, big data analytics seem destined for litigation, including class actions. Fortunately, there are steps businesses, like e-commerce vendors, can take—and defenses they can raise—to help fend off these types of suits.

**The Northeastern Report**

The Northeastern study examined 10 major e-retailers—including Walmart Stores Inc. and Home Depot Inc.—and six hotel/rental car sites—including Travelocity.com LP and Expedia Inc.—to determine whether they implement price discrimination or steering, and if so, what user attributes trigger the so-called "personalization." The report explains that "price steering" occurs when "two users receive different product results (or the same products in different order) for the same query." For example, some customers may be shown more expensive products in response to a search query than others. "Price discrimination" occurs when "two users are shown inconsistent prices for the same product."

Based on the results of searches designed to isolate the existence of personalization run by 300 study participants on the 16 sites, the study concluded:

We find evidence for price steering and price discrimination on four general retailers and five travel sites. Overall, travel sites show price inconsistencies in a higher percentage of cases, relative to the controls, with prices increasing for ... users by hundreds of dollars. Finally, we observe that many ... users experience personalization across multiple sites.

The report also explains what customer attributes resulted in price discrimination and price steering:

We found cases of sites altering results based on the user's OS/browser, account on the site, and history of clicked purchased products. We also observe two travel sites conducting A/B tests that steer users towards more expensive hotel reservations.

More specifically, the results showed, among other things, that some e-commerce companies have been charging higher prices to users on Macs or Android devices. Moreover, users were shown fewer search results in a more expensive price bracket if they used mobile devices to access Home Depot rather than desktop PCs.

The White House report noted that differential pricing is likely still in the early stages: "[a] review of the current practices suggests that sellers are now using big data and digital technology to explore consumer demand, to steer consumers towards particular products, to create targeted advertising and marketing offers, and in a more limited and experimental fashion, to set personalized prices." However, the report also noted that "the combination of differential pricing and big data raises concerns that some consumers can be made worse off," and cited the need to enforce existing laws—including consumer protection laws—and promote transparency.[4]

**Are Consumer Class Actions Based on the Use of Data Analytics on the Horizon?**

At least one way that consumer class actions based on the use of data analytics could manifest themselves is as a consumer fraud or unfair trade practices suit.

It is not unlawful for e-commerce companies to engage in price discrimination or price steering. In fact, such practices can be used to help consumers. As the Northeastern report explains, for example, Cheaptickets and Orbitz Worldwide Inc. price discriminate in favor of their members.

But many members of the public do not like the idea of their private information being used by companies without their knowledge. And to the extent the data is used to increase prices or steer customers away from lower-priced goods and services, consumer displeasure may grow. Add in an aggressive plaintiffs bar looking to break into big data litigation, and broad state consumer protection statutes that all but eliminate an intent requirement, and it is not a stretch to anticipate an increase in consumer class actions based on these practices.

To date, although plaintiffs have brought hundreds of data-related class actions over the last several years, they have had a difficult time prevailing. One of the primary hurdles that plaintiffs have faced is Article III standing. Standing tends to be an issue because typically, data-related class actions have involved data breaches, and a loss of data privacy does not immediately cause injury. Rather, a number of unknown contingencies must occur before a plaintiff suffers an actual injury such as fraud. And instead of waiting for such an injury to occur, plaintiffs have frequently alleged an increased risk of future injury. Courts, however, have often rejected this type of future injury as too speculative to confer standing (though there are exceptions).

The Northeastern report demonstrates that price discrimination or price steering cases — as opposed to data loss cases — may be another story. To the extent, for example, a consumer challenges an e-commerce retailer's use of personal data to charge higher prices or to steer the consumer away from lower-priced products as deceptive under state consumer protection laws, that consumer may have an easier time establishing an injury and be able to avoid the standing issues that have undermined so many previous data-related suits.

**E-Commerce Retailers Can Take Steps to Reduce Their Risks of Being Subject to Consumer Class Actions Based on the Use of Data Analytics**

Notwithstanding the potential risks of using data analytics, e-commerce vendors are not likely to discontinue the practice, as it can be useful to both the vendors and their consumers. But vendors do have several ways to protect themselves from potential consumer class actions.

***Terms of Use and Privacy Policies***

Foremost, e-commerce vendors can be explicit about the use of data analytics in their privacy policies and terms of use, and even in search interfaces. A consumer generally consents to such policies by clicking

through certain buttons or windows when purchasing a product or signing up for a service, and courts have generally upheld these so-called "click-wrap" agreements so long as the consumer has actual or constructive notice of the terms. The key to any such policy would be to provide conspicuous notice of the terms and explicitly articulate in a clear, simple and concise manner the types of data collected and how the data will be used. It may also be desirable to notify consumers that while it may result in hindering a vendor's ability to best respond to consumer preferences, they can disable various features on their Web browsers to prevent data collection altogether.

Even a perfectly crafted privacy policy may not be a silver bullet, however. A policy could be attacked as unconscionable and not binding. First, privacy policies could be challenged because they provide little or no room for bargaining. This alone could be used to try and establish procedural unconscionability, especially if the policy contains technical language or carefully-worded disclaimers. And although substantive unconscionability would likely be more difficult to prove, one-sided terms—i.e., terms that allow for consumers to be charged higher prices—combined with procedural unconscionability could be enough to render a privacy policy unenforceable.

Because privacy policies are subject to such challenges, it would also be advisable for e-commerce vendors to include in their privacy policy an arbitration clause establishing that any dispute would be adjudicated in individual arbitration (as opposed to class litigation or arbitration). The U.S. Supreme Court repeatedly has held that such clauses are enforceable, and individual arbitration can be a good way for both parties to resolve small-value disputes without large and costly class litigation.

***Other Defenses in Litigation***

To the extent an e-commerce vendor does find itself in class litigation based on the use of data analytics, it would likely have several defensive moves available.

A defendant's primary focus would be on avoiding class certification. Individual data use suits are likely to be costly and hard to maintain outside the class action vehicle—especially in cases involving potentially small price differentials. Because plaintiff's ability to obtain class certification is often, for all practical purposes, dispositive, defendants will have to stave off class certification. In the price discrimination and steering contexts, the merits and/or damages may be sufficiently individualized to render class certification unachievable. For instance, an e-commerce vendor facing a consumer class action on price steering would have strong arguments that different search results for different individuals would result in vast factual disparities among potential class plaintiffs, as well as varying degrees of price differentials. Indeed, even the same individual using different devices could face different search results and prices. And for these same reasons, it would be similarly difficult to establish a class in a disparate impact case. In several data cases, courts have refused to certify a class when there are numerous individualized inquiries.[5]

E-commerce vendors would also have several defenses on the merits. At least with respect to price steering, e-commerce vendors would have good arguments that there is nothing false or misleading about the practice. If personalization simply affects the order in which products are presented to a consumer—such that the

consumer would be able to view all options by scrolling through all of the search results—there is a solid argument that a consumer is not misled or has not suffered any kind of loss. Indeed, this would be no different than a grocery store putting cheaper, generic products on the bottom shelves. Similarly, to the extent that privacy settings and preferences are variable, an e-commerce company could argue that consumers' option to adjust the privacy settings on their Web browsers prevents any claim of price steering or price discrimination. This argument would be particularly strong if notification of that possibility was included in a privacy policy.

**Conclusion**

Some consumer advocates are wary about business practices involving big data, particularly the algorithms used to steer customers to goods, services, information and opportunities. Companies using big data analytics to shape customers' experiences and behavior should consider how their practices and contracts can help shield them from future suits.

---

[1] http://www.washingtonpost.com/posteverything/wp/2014/11/03/if-you-use-a-mac-or-an-android-e-commerce-sites-may-be-charging-you-more/; http://www.ibtimes.co.uk/look-out-you-might-be-charged-more-if-you-shop-online-using-mac-android-device-1474431.

[2] "Measuring Price Discrimination and Steering on E-commerce Web Sites," http://www.ccs.neu.edu/home/cbw/pdf/imc151-hannak.pdf.

[3] White House Council of Economic Advisors, Big Data and Differential Pricing, 19, 2 (Feb. 2015), available at https://www.whitehouse.gov/blog/2015/02/06/economics-big-data-and-differential-pricing.

[4] More recently, a study published on Technology Science demonstrated that The Princeton Review charges different prices for its online tutoring based on the zip code used when ordering the service. See "Price Discrimination in The Princeton Review's Online SAT Tutoring Service," http://techscience.org/a/2015090102/.

[5] See, e.g., *In re Hulu Privacy Litig.*, No. C 11-03764 LB, 2014 WL 2758598, at *16 (N.D. Cal. June 17, 2014).