DAVIS GILBERT

Big Data and Big Questions

6th Edition: Trends in Marketing Communications Law

The use of biometric and location data has been on the rise for several years, but the expanded uses of this data must be reevaluated in light of the associated risks and evolving legal regimes. Although the use of biometric data is nothing new in industries such as health and fitness, 2018 saw a broader range of companies collecting information such as eye tracking and facial coding to analyze consumers' reactions to various types of content (and therefore to predict consumer behaviors).

The use of biometric data has been met with substantial legal challenges, in particular under the Illinois Biometric Information Privacy Act (BIPA), which allows for a private right of action for damages. A January 2019 Illinois Supreme Court decision holding that plaintiffs need not prove actual injury to prevail under the BIPA has led to a rash of class actions in Illinois.

Location data usage is also more widespread than ever, providing advertisers with the ability to learn a consumer's general shopping patterns or even the precise moment at which a consumer is in a physical position to make use of a promotion. Companies offering mobile apps may use location data to allow for or improve app performance, but a user's consent to the use of location data for one purpose (e.g., to hail a car or learn the weather) does not constitute consent to use such data for all purposes (e.g., sale of such data to third parties). In January 2019, the provider of a weather app was sued by the city of Los Angeles alleging that the location data it had collected from mobile app users, for the stated purpose of providing relevant weather forecasts, did not adequately notify app users that such data could also be used for marketing purposes.

If the increasingly complicated legal landscape were not enough to merit rethinking the use of biometric and location data, there is also a darker side to this data and the technology used to harness it. Facial recognition and location data have been used to identify and track Muslim populations in China; meanwhile, in the UK and United States, police forces are experimenting with facial recognition technology to identify criminals, despite claims that the technology has high error rates and may be susceptible to racial bias. In January of this year, concern for the misuse of this technology led a group of Amazon's shareholders to urge Amazon to stop selling its Rekognition tool to governments.

If these issues seem distant from the world of data usage for advertising purposes, marketers should note that once these sensitive categories of data have been collected, they are susceptible to access and use for unauthorized purposes. (For example, researchers discovered that the personal information of about 2.5 million individuals in China was exposed due to insufficient precautions taken by a facial recognition technology provider.) Therefore, advertisers who are collecting location and biometric data should do so responsibly, securely, and with a clear focus on offering consumers meaningful notice and a right to consent (or object) to the collection and use of such data.

Key Takeaways

- Interest in sensitive categories of data, such as biometric and location data, continues to grow among advertisers.

- Although data is a powerful tool to optimize consumer experiences with content, it is also susceptible to misuse due to a lack of adequate consent or in the event of a breach or leak.
- While the principles of notice and consent apply to these categories of data, there are other evolving legal requirements that must be observed.

Related People

Richard S. Eisert
Partner/Co-Chair Advertising + Marketing
212 468 4863
reisert@dglaw.com

Gary Kibel
Partner
212 468 4918
gkibel@dglaw.com

Maxine Sharavsky Garrett
Partner
212 468 4845
msgarrett@dglaw.com