



CARDOZO

Benjamin N. Cardozo School of Law

LARC @ Cardozo Law

---

AEJ Blog

Journal Blogs

---

4-16-2016

## The Fight Against Uber's Privacy Infringement

Alexa Shore

*Cardozo Arts & Entertainment Law Journal*

Follow this and additional works at: <https://larc.cardozo.yu.edu/aelj-blog>



Part of the [Law Commons](#)

---

### Recommended Citation

Shore, Alexa, "The Fight Against Uber's Privacy Infringement" (2016). *AEJ Blog*. 103.  
<https://larc.cardozo.yu.edu/aelj-blog/103>

This Article is brought to you for free and open access by the Journal Blogs at LARC @ Cardozo Law. It has been accepted for inclusion in AELJ Blog by an authorized administrator of LARC @ Cardozo Law. For more information, please contact [larc@yu.edu](mailto:larc@yu.edu).

# The Fight Against Uber's Privacy Infringement

BY [ALEXA SHORE](#) / ON APRIL 16, 2016

As of July 15, 2015, Uber updated its privacy policy, which caused customers to delete the app from their cellular phones immediately. Uber implemented two main changes with its new privacy policy. It now gives the company the ability to access users' location data and the capability of sending ads and promotions to users' address books from their mobile phones. In its policy, Uber explains that it utilizes elaborate software to track consumer's precise locations, allowing the company to track users even when the app is shut off, deleted, or when the GPS function is turned off. Furthermore, Uber's privacy policy does not indicate when or if this information of past location data will be deleted.

As a result, Uber consumers are appalled because the company can trace not only users' whereabouts, but also every single location that they've ever traveled since the first download of the app. Users have almost zero privacy after the app is downloaded. That lack of privacy is the enormous cost an Uber consumer pays to have the ability to quickly request a car to go wherever they need to be. Thus, once the app is downloaded, Uber can locate exactly where a user is forever.

Companies have constantly been facing issues in utilizing technological platforms and running applications while still interpreting the law correctly and avoiding privacy infringement of their customers. This problem arises because of the growing amount of sophisticated technology that consumes our advanced world today.

In order to try to fix this particular issue, the Electronic Privacy Information Center ("EPIC") filed a complaint against Uber on June 22, 2015, on behalf of thousands of American Uber consumers who feel as if their privacy is being invaded through Uber's recently updated privacy policy. EPIC focuses on emerging privacy and civil liberties and is a leading consumer advocate before the Federal Trade Commission ("FTC"). EPIC has a specific interest in protecting consumer privacy and has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers.

In response to EPIC's complaint, the FTC should cease the unfair and deceptive data collection practices which Uber imposed on consumers in July 2015. Through the lens of the Federal Trade Commission Act ("FTC Act"), Uber should be liable this time for unfair and deceptive practices in or affecting commerce.

For the FTC to conclude this, it must first define exactly what an "unfair" and "deceptive" practice is. According to the Federal Trade Commission Act, a trade practice is unfair if it "causes or is likely to cause substantial inquiry to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to

consumers or to competition.” Uber’s IP address tracking practice constitutes an unfair business practice because it is likely to cause substantial injury to consumers, which is not reasonably avoidable by consumers themselves. Consumers must completely delete the app or quit using Uber’s services to stop the company from collecting their IP addresses, however it is not clear that such actions would mean that Uber will not be able to locate the consumer after.

Also according to the FTC Act, an act or practice is deceptive if it “involves a representation, omission, or practice that is likely to mislead the consumer acting reasonably under the circumstances, to the consumer’s detriment.” There are three elements to a deception claim. First, there must be representation, omission, or practice that is likely to mislead the customer. The relevant injury for this factor is not whether the act or practice actually misleads the customer, but rather whether it is likely to mislead the customer. Second, the act or practice must be considered from the perspective of a reasonable consumer. When interpreting the second factor, the FTC will look at the totality of the act or practice and ask questions such as, “How clear is the representation? How conspicuous is any qualifying information? How important is the omitted information? Do other sources for the omitted information exist? How familiar is the public with the product or service?” Finally, the representation, omission, or practice must be material. Essentially, the information must be important to customers.

Moreover, Uber’s statement in its privacy policy that it will “take appropriate measures to protect [users’] personal information” is extremely deceptive and false, for that matter. Industry experts have identified that Uber’s data collection of intimate customer details is valuable to unauthorized third party users and is likely vulnerable to attacks.

Clearly, Uber is in violation of the FTC Act in that it engaged in a deceptive practice when it stated that “users will be in control” of their privacy settings in the most recently updated privacy policy. Users are not truly in control of the data they disclose to Uber because the company retains the ability to track users even if they choose not to share location data, exit the app, or even delete the app. Users could not reasonably know that they are not truly in control of what data they want to share with Uber. In all, Uber should be liable for deceptive representation in its policy in that users will be able to opt out of targeted advertising, when really they are not. This inconsistency is to users’ detriment and material in that they may not have downloaded the service in the first place had they known Uber could access their contact lists and send promotional messages.

The moral of the story is that companies need to be careful about accessing consumer data without a customer’s consent or expressly informing them. This way, companies will not be held liable for threatening users’ privacy rights, diminishing personal safety of consumers, allowing unauthorized parties to access users’ information, posing a direct risk of consumer harm, and participating in unfair and deceptive trade subject to investigation by the FTC, among several other federal agencies.

Sources:

1. <http://www.consumeraffairs.com/news/epic-fail-for-ubers-new-privacy-policy-ftc-asked-to-block-deceptive-data-collection-062315.html>
2. <http://www.internetontrial.com/privacy-law/uber-policy-raises-privacy-concerns/>
3. <http://lawstreetmedia.com/news/uber-users-beware-tracking-software/>
4. <http://www.scribd.com/doc/269425673/UBER-Complaint>

*Alexa Shore is a second-year law student at Benjamin N. Cardozo School of Law and a Staff Editor of the Cardozo Arts and Entertainment Law Journal. Alexa worked at Estee Lauder Legal during summer 2015 and is looking forward to pursuing a career in trademark and intellectual property.*