Federal Trade Commission's Uber Consent Agreement Designates Geolocation Information as Personal Information

09.01.2017

The Federal Trade Commission (FTC) recently entered a Consent Agreement with Uber that includes "precise geolocation information" in the list of personal information that is to be protected. While the Consent Agreement only applies to Uber, it is reflective of the evolution of the FTC's position on the sensitivity of consumers' location information. Adding precise geolocation information in the definition of personal information will have a significant impact on emerging technologies, such as drones, autonomous vehicles and the Internet of Things (IoT), that will generate or collect geolocation information. It also will affect the growing number of companies that use geolocation information in their business operations.

In its draft complaint, the FTC stated that Uber collects "precise geolocation information" on both drivers and riders from apps loaded on their respective mobile devices. The complaint alleged that Uber also collects "information about the route of the trip from the Driver's mobile device and associates the trip information with the Rider." The FTC alleged that Uber had not taken adequate steps to protect the precise geolocation information and other personal information it collected on drivers and riders, specifically citing a lack of employee training and reasonable access controls. As a result, the FTC alleged that Uber's privacy policy – and other statements made to customers about how their personal information was being protected – were false and misleading.

In August, the FTC published the Consent Agreement entered into with Uber. The Consent Agreement defines personal information to include "precise geolocation data of an individual or mobile device, including GPS-based, WiFi-based or cell-based location information." Under the Consent Agreement, Uber:

- Is prohibited from misrepresenting the extent to which it protects personal information.
- Will establish and implement a comprehensive privacy policy for personal information.
- Will obtain initial and biennial audits of its privacy practices by a third party.

The FTC has been concerned about the privacy issues associated with precise geolocation information for several years. However, this is the furthest step the FTC has taken to define precise geolocation information from a technology standpoint. Moreover, it appears to be the first time that it has publicly included precise geolocation information in the definition of personal information.

Including precise geolocation information in the definition of personal information will affect many types of businesses. For example, technologies, such as drones, autonomous vehicles and the IoT will use GPS, Wi-Fi and cell towers to generate and/or collect geolocation information on mobile devices and individuals. In many instances, this information will easily be associated with other types of information that could be used to identify an individual.

In addition, there is a growing number of businesses that recognize the value of collecting location information on their customers, prospects, assets and employees. It will be incumbent upon those companies to understand whether any precise geolocation information is being collected and how it is being used and stored within the organization. Many companies should consider updating their privacy policies to specifically include what geolocation information is being collected and how it is used. Employee privacy training should now include the sensitivities associated with precise geolocation information. In addition, companies should review vendor and customer agreements under which geolocation information is being transferred or licensed, such as cloud storage agreements, to ensure that they contain adequate privacy protections.

Related People

- Kevin D. Pomfret – 703.760.5204 – kpomfret@williamsmullen.com

Related Services

- Data Protection & Cybersecurity