Forbes / Tech

BETA

DEC 24, 2014 @ 03:04 PM 4,997

BEWARE: The Dangers Of Location Data

Danielle Citron, CONTRIBUTOR

FULL BIO

Opinions expressed by Forbes Contributors are their own.

This week, California Attorney General Kamala Harris HRS -1.06% advised her constituents to disable their phones' automatic location identifier. Consumers likely don't know that their phones continuously collect their location data for reasons that have nothing to do with the routing of their calls and e911 requirements. Her advice is to turn off the default, the always on setting, and turn it on for specific uses. You want to let Yelp YELP -0.71% ! know where you are--sure, give the app permission for a specific moment in time. Otherwise, turn it off.

That is wise advice. If consumers keep the always-on setting for their geolocation data (that is, the street and city where a phone is located as it changes moment to moment), they are opening themselves up to mischief and far worse. Geolocation data tells us intimate, revealing details about people's lives--their visits to drug treatment clinics, psychiatrists, prospective employers, and more. As AG Harris told USA Today, "Broadcasting your location can sometimes expose you and your family to risk of theft or physical harm. . . For instance, you may be unknowingly revealing your location if your phone is 'geo-tagging' your photos. ... Sharing a 'selfie' without disabling geo-tagging can be dangerous, especially for victims of stalking or domestic abuse." Companies can sell geolocation data to data brokers, further filling their dossiers with information about consumers' medical conditions, religious affiliations, and more.

Consumers may well be giving mobile apps access to their geolocation data without ever having given specific permission. Indeed, most mobile apps are not transparent about the fact that they collect geolocation data. Most mobile app companies say that they only collect geolocation data after getting express consent from consumers, but that is not the case. As the FTC's Director of the Bureau of Consumer Protection Jessica Rich testified this past summer before a Senate Privacy, Technology, and Law subcommittee hearing, companies often claim that they have an opt-in approach to geolocation data but do not follow it in practice. The Flashlight app and

Snapchat cases show that opt-in standard is not the norm. For instance, Snapchat transmitted geolocation information from users of its Android app, even though its privacy policy claimed it did not track users or access such information. The developer of a flashlight app failed to disclose that its app transmitted the device's location to third parties, including mobile ad networks. The company and its manager agreed to an order that prohibits them from misrepresenting how consumers' information is collected and shared. Crucially, the company must obtain consumers' affirmative express consent before collecting, using, and sharing their geolocation data.

As privacy scholars Daniel Solove and Woodrow Hartzog powerfully argue, the FTC's consent decrees establish common law set of principles. Recent FTC settlements in cases involving CyberSpy Software, Flashlight app, and Snapchat app make clear that geolocation data is the third rail. Be careful before collecting it and take certain steps if you do. Geolocation data is especially revealing about our lives. It is subject to serious abuse, from domestic abuse and stalking to theft and discrimination. Mobile apps and other entities should get express consent from consumers before collecting it. They should not share it with any entity without consumer consent. I'll have more to say about the criminal consequences of stalking apps later but for now there is much consumers and mobile app providers need to do to respect privacy.