Subject: Re: Your Location Data Is Being Sold—Often Without Your Knowledge - WSJ

From: "Trystan Kosmynka" [redacted]

Received(Date): Tue, 06 Mar 2018 00:53:14 +0000

To: "Philip Schiller" [redacted], "Sean Cameron" [redacted]

Cc: "Emily Blumsack" [redacted], "Ron Okamoto" [redacted], "C.K. Haun" [redacted], "Eddy Cue" [redacted], "Matt Fischer" [redacted], "Toby Paterson" [redacted], "Craig Federighi" [redacted], "Greg Joswiak" [redacted], "Brian Croll" [redacted], "Josh Shaffer" [redacted]

Date: Tue, 06 Mar 2018 00:53:14 +0000

Privileged and Confidential

We will work with engineering and look into this.

On Mar 5, 2018, at 4:33 PM, Philip Schiller <[redacted]> wrote:

Privileged and Confidential

There appears to be rampant use of location data (based on SDKs that slurp it up after a user approves) far beyond what people think they are allowing just for the app experiences they expect. We should look into his and propose what to do about it (More limited use of the data in terms? Ban any SDKs that are driving this? Force explicit disclosure of the exact uses of the data? Etc)

https://www.wsj.com/articles/your-location-data-is-being-soldoften-without-your-knowledge-1520168400

Your Location Data Is Being Sold—Often Without Your Knowledge

Location-based ads are growing, which means the industry has more ways than ever to track you

Christopher Mims March 4, 2018

Businesses and other locations, in green, where the location-based advertising firm Groundtruth pushes ads to mobile devices. Photo: Kenneth Bachor/The Wall Street Journal

By

Christopher Mims

As location-aware advertising goes mainstream—like that Jack in the Box ad that appears whenever you get near one, in whichever app you have open at the time—and as popular apps harvest your lucrative location data, the potential for leaking or exploiting this data has never been higher.

It's true that your smartphone's location-tracking capabilities can be helpful, whether it's alerting you to traffic or inclement weather. That utility is why so many of us

are giving away a great deal more location data than we probably realize. Every time you say “yes” to an app that asks to know your location, you are also potentially authorizing that app to sell your data.

Dozens of companies track location and/or serve ads based on this data. They aim to compile a complete record of where everyone in America spends their time, in order to chop those histories into market segments to sell to corporate advertisers.

Marketers spent $16 billion on location-targeted ads served to mobile devices like smartphones and tablet computers in 2017. That’s 40% of all mobile ad spending, research firm BIA/Kelsey estimates, and it expects spending on these ads to double by 2021.

The data required to serve you any single ad might pass through many companies’ systems in milliseconds—from data broker to ad marketplace to an agency’s custom

system. In part, this is just how online advertising works, where massive marketplaces hold continuing high-speed auctions for ad space.

A map of the U.S., showing areas of unusually high visits to sites where location-based advertising firm Groundtruth pushes ads to mobile devices. Photo: Kenneth Bachor/The Wall Street Journal

But the fragmentation also is because of a very real fear of the public backlash and legal liability that might occur if there were a breach. Imagine the Equifax breach, except instead of your Social Security number, it's everywhere you've been, including your home, your workplace and your children's schools.

The fix, at least for now, is that with most individual data vendors holding only parts of your data, your complete, identifiable

profile is never all in one place. Giants like Facebook and Alphabet 's Google, which do have all your data in one place, say they are diligent about throwing away or not gathering what they don't need, and eliminating personally identifying information from the remainder.

Yet as the industry and the ways to track us expand, the possibility that our whereabouts will be exposed multiplies. If you've ever felt clever because an app on your phone asked to track your location and you said no, this should make you feel a little less smug: There are plenty of ways to track you without getting your permission. Some of the most intrusive are the easiest to implement.

The spy in your pocket

Your telco knows where you are at all times, because it knows which cell towers your phone is near. In the U.S., how much data service providers sell is up to them.

Another way you can be tracked without your knowing it is through any open Wi-Fi hot spot you might pass. If your phone's Wi-Fi is on, you're constantly broadcasting a unique address and a history of past Wi-Fi connections. Retailers sometimes use these addresses to identify repeat customers, and they can also use them to track you as you go from one of their stores to another.

WeatherBug, one of the most popular weather apps for Android and iPhone, is owned by the location advertising company GroundTruth . It's a natural fit: Weather apps need to know where you are and provide value in exchange for that information. But it also means that app is gathering data on your location any time the app is open—and even when it isn't, if you agreed to always let it track your location. That data is resold to others.

Jack in the Box pushes promotions to apps on potential customers' mobile devices when they are near its stores. Photo: Luke Sharrett/Bloomberg

GroundTruth also says it gathers location data from "over a hundred thousand" other apps that have integrated bits of its code. Company President Serge Matta declined to disclose which apps. App makers agree to harvest location data because it grants them access to GroundTruth's mobile advertising network.

This data is what enables marketers like Jack in the Box to push an advertiser's message to potential customers near its restaurants. A typical engagement includes pushing location-based promotions or coupons through mobile ads, says Iwona Alter, chief marketing officer of Jack in the Box.

Every month GroundTruth tracks 70 million people in the U.S. as they go to work

in the morning, come home at night, surge in and out of public events, take vacations, you name it.

Anonymize, de-anonymize

Companies like GroundTruth try to ensure they aren't tracking or storing data on individuals. Most of what they sell are anonymous blobs of people who fit particular descriptions—"soccer moms who intend to buy an SUV," for example. But they also occasionally hand off location data to a third party, such as LiveRamp, owned by data broker Acxiom , before it is matched up with potentially personally identifying information, such as your complete shopping history at a retailer. LiveRamp is almost like an escrow company for data.

GroundTruth demonstrated its ability to target a mobile ad to a single location by pushing this message to everyone at the

Starbucks where columnist Christopher Mims was working. Ordinarily, these ads would not contain personalized messages or personal information. Photo: Christopher Mims/The Wall Street Journal

Companies like Acxiom could be prime targets for hackers, said Chandler Givens, chief executive of TrackOff, which develops software to protect user identity and personal information. LiveRamp goes to great lengths to mathematically obfuscate our individual identities, said Sheila Colclasure, chief data ethics officer at LiveRamp and Acxiom. But some security researchers fear data brokers like Acxiom might be compromised already, or could be someday.

Acxiom and LiveRamp in the U.S. are governed by federal and state laws that regulate the collection and use of data in the particular businesses their clients are involved in, Ms. Colclasure said. Nearly

every year, a bill comes up in the Senate or House that would regulate our data privacy—the most recent was after the Equifax breach—but none has passed. In some respects, the U.S. appears to be moving backward on privacy protections.

There might never be a breach of our location data. But given the drumbeat of hacks of both companies and governments, it's hard to believe hackers aren't at least trying to compromise such a high-value target.

Write to Christopher Mims at christopher.mims@wsj.com

Corrections & Amplifications

GroundTruth's marketing materials and representatives say the company gets data from "over a hundred thousand" other apps. An earlier version of this article incorrectly attributed this figure to GroundTruth President Serge Matta. (March 4, 2018)

Also, a caption with an earlier version of this column didn’t make clear that GroundTruth’s ads don’t ordinarily contain personalized messages or personal information. (March 5)

Appeared in the March 5, 2018, print edition as 'You’re Being Tracked, and Hackers Loom.'