Venmo did what with my data? My location was shared when I paid with the app

February 24 2020, by Jefferson Graham

Credit: CC0 Public Domain

Many of us have ditched cash and, instead, use smartphone apps like Venmo to pay for goods and services.

The app is free, it takes just a second to initiate and finish a transaction. I don't have to write a check or pull out some cash. It's great.

But you know what, there's no such thing as free.

I discovered this week that when I opened PayPal-owned Venmo to pay my personal trainer and made sure to click "private," yet the app recorded my GPS location (home address) and the trainer's name, and sent it off to Braze, a third-party data collection firm.

Think about that for a minute. You use the app to pay your bill, and, in return, some company you've never heard of now has your address and associations. How icky is that?

"How would the CEO of PayPal feel about his home address and contacts being shared with third-party data collection firms?" asks Patrick Jackson, the Chief Technology Officer for security firm Disconnect.

Probably just like I did—a little sick to the stomach.

Jackson took control of my iPhone this week to help me understand just how badly I was being tracked. His firm Disconnect was able to see which companies were sharing my information when I used apps.

It was worse than you could imagine.

Our digital privacy and what we can do to tackle the onslaught from all these firms that want to snoop into our lives takes a big spotlight Monday, with the annual RSA conference, which is devoted "to stand against cyberthreats around the world."

And nowhere are cyber threats more prevalent than on our smartphones. Just ask Amazon CEO Jeff Bezos, whose phone is believed to have been hacked by the crown prince of Saudi Arabia, via the Whatsapp communications app. Or Hillary Clinton's 2016 campaign manager John Podesta, who clicked a malicious link in an e-mail sent by Russians.

Firms not disclosing sharing our data with third parties

Here at home, it's all our personal data getting sent to these data collection firms, a practice not disclosed by the companies whose logos are all over our smartphones.

Take the seemingly innocuous Solitaire app that many people use to waste a few minutes with a game that many of us have been playing since the first PCs. My version is from the Chinese company Zenjoy, and Jackson found that it sent device information to Chartboost, a San Francisco based data collection firm. It knew what kind of phone I used, who my carrier is, that I played the game while wearing earbuds, and via a digital fingerprint, it could follow me to other devices.

"You, as a user, have no idea any of this is happening," Jackson says. Nor "the level of detail we're giving up to these companies."

Noom shared e-mail address

Also this week, I signed up for a "free" trial of weight loss app Noom,

and it responded apparently by sending off my e-mail address and device information to the data collection firm Mixpanel.

Noom is an app that costs $59 monthly to use. I do expect it to mine my data: what foods I'm eating, my levels of exercise activity and the like. I don't expect it to share this info with a company like Mixpanel, whose mission is to "analyze user behavior."

Did I sign up for this? Because I don't remember that happening.

Solitaire and Venmo, though, are "free." We all make a bargain with these types of apps. We don't pay to use them in exchange for the companies learning about our habits and preferences.

The problem is, we trust a big company like PayPal with our data, but how do we feel about Braze, Mixpanel and other companies of the same ilk?

"Now they know who you are, where you live and who you're sending money to, and how safe is that information?" Jackson asks. "What happens to that data?"

What is Braze?

And good luck to the consumer who could figure out exactly what Braze is, based on its own description. The company calls itself "a comprehensive customer engagement platform that powers relevant and memorable experiences between consumers and the brands they love."

Got it?

We reached out to Venmo, Noom and ZenJoy, but only got a response, sort of, from Venmo.

It declined to answer why it shared my home location and association with Braze. It also declined to answer whether the PayPal app also shares such information with Braze.

PayPal did say it works with third-party service providers "who assist us in providing services to you" or to provide fraud detection. "Our contracts dictate that these service providers only use your information in connection with the services they perform for us and not for their own benefit."

There's nothing in there about what consumers are giving up by using Venmo.

PayPal acts differently than Venmo

Despite the practices of a PayPal unit to distribute our personal information to a data collection firm, the parent company apparently acts differently. We made three payments on the PayPal app from our home location, and it responded differently than Venmo. It grabbed what Jackson calls "minor" information like device type and the amount of time spent on the app. "PayPal is definitely less chatty with third parties than Venmo," says Jackson.

Would you be bothered by Venmo's home address and associate share, Noom Coach's e-mail address forward and your Solitaire game passing on that you play the game with earbuds ion?

If so, scream loud and clear that this type of behavior isn't acceptable, says Jackson.

"When the companies get called out, they switch their behavior," he says.

What about it Apple?

Another big concern, he says, is Apple, which regularly touts its different approach to privacy and tells consumers it's less grabby than Facebook and Google.

Yet everything that happened on my iPhone was allowed to happen by the company that makes the phones. Sure, all of this also happens on Android phones, but Google, which makes Android software, doesn't have billboards and full-page ads touting its different, pro-consumer approach to privacy.

As Apple said on one recent campaign, "What happens on your iPhone, stays on your iPhone."

Not exactly.

Just ask Venmo, Noom and ZenJoy if my information is still on my iPhone and not shared with their third-party partners.

"Tell Apple it's not OK," Jackson says. "They have a big hammer. They could stop the data collection overnight if they wanted to."

Apple has its developer conference in June where it regularly updates the iOS operating system. Now here's a new feature I'd really like to see: an end to consumer tracking in apps. What do you say Tim Cook and company?

In response, Apple says, "We are always improving and considering how to best ensure our users are consenting to the data collected by apps."

In other tech news this week

Oculus Quest sold out—the popular Oculus Quest virtual reality system that was so hot to get over the holidays is an even tougher ticket now. Due to production problems caused by the effects of the coronavirus on manufacturing and shipping, Facebook has grayed out the buy buttons on its website, and the unit is not for sale on Amazon or Best Buy either. Facebook says it's working as fast as it can to get the units available to consumers again.

Ring doorbells now enforce two-factor authentication. After months of reports of hacks on Ring doorbells, the Amazon-owned company says Ring owners are now required to use two-factor authentication to log in to their accounts. Earlier this month, Ring began offering as a default two-factor authentication, which requires you to input a passcode sent via email or text when you log into your account. Now, its use is mandatory.

UCLA dropped a controversial facial recognition plan to monitor students. The idea was to have the University of California Los Angeles use facial recognition as a way to gain access to buildings, to prove authenticity and to deny entry to people with restricted access to the campus, matching their faces against a database. Advocacy group Fight for the Future says UCLA was the first major university exploring using facial recognition to monitor students. The group had tested facial recognition software and found that "dozens" of student-athletes and professors were incorrectly matched with photos from a mug shot database, "and the overwhelming majority of those misidentified were people of color."

app.html