Exhibit 215

From: [redacted]
To:
Sent: Mon, 15 Apr 2019 16:23:20 -0700
Subject: Re: [Industryinfo] Tracking Phones, Google Is a Dragnet for the Police
Cc: [redacted]

On Mon, Apr 15, 2019, 4:16 PM [redacted] wrote:

> If a taxi driver's path was deemed 'good enough' for law enforcement to ask for & us to release their personal information, that's enough for me to want to ask some questions.
>
> Sure, you should reach out to our lawyercats with questions about how we respond to warrants.

I doubt anyone is going to give you an answer on industryinfo, and I for one will surely not speculate.

> I feel like erring on the side of validating people's expectations for keeping their information away from potentially unreasonable uses by the government is anyone's job who works here.
> [redacted]

> On Apr 15, 2019, at 3:46 PM, [redacted] wrote:
>
> > They did randomly search for people in the area though, in my opinion.
>
> I don't have enough information, from the article or otherwise, to assess that :)
>
> On Mon, Apr 15, 2019 at 3:42 PM [redacted] wrote:
>
> > They did randomly search for people in the area though, in my opinion. The initial phase of the warrant provides anonymized locations of many devices in a given region over an asked-for period of time.
> > From the article:
> > --
> > "Often, Google employees said, the company responds to a single warrant with location information on dozens or hundreds of devices."
> >
> > "This year, one Google employee said, the company received as many as 180 requests in one week. Google declined to confirm precise numbers."
> >
> > "The new orders, sometimes called 'geofence' warrants, specify an area and a time

period, and Google gathers information from Sensorvault about the devices that were there. It labels them with anonymous ID numbers, and detectives look at locations and movement patterns to see if any appear relevant to the crime. Once they narrow the field to a few devices they think belong to suspects or witnesses, Google reveals the users' names and other information."

"The areas they targeted ranged from single buildings to multiple blocks, and most sought data over a few hours. In the Austin case, warrants covered several dozen houses around each bombing location, for times ranging from 12 hours to a week. It wasn't clear whether Google responded to all the requests, and multiple officials said they had seen the company push back on broad searches."

--

I am dubious that 180 times in one week, law enforcement officers had amazingly specific information that would allow them to precisely identify one person's path in a way that wouldn't accidentally ensnare others.

Here's just one instance mentioned in passing of accidentally ensnaring someone looks like: "In Minnesota, for example, the name of an innocent man was released to a local journalist after it became part of the police record. Investigators had his information because he was within 170 feet of a burglary. Reached by a reporter, the man said he was surprised about the release of his data and thought he might have appeared because he was a cabdriver. "I drive everywhere," he said."

[redacted]

On Apr 15, 2019, at 3:29 PM, [redacted] wrote:

My point was that the warrant requires some initial evidence to obtain, which in this case is footage of the person's vehicle linked with the crime; it's not like they were fishing for any random person who happened to be in the area, which I agree would've been far more scary.

On Mon, Apr 15, 2019 at 3:19 PM [redacted] wrote:

I don't think the headline is what's scary here though. It's the geofence warrant.

[redacted]

On Apr 15, 2019, at 2:48 PM, [redacted] wrote:

Something no one in this thread has mentioned yet is the fact that the crime

was committed with the person's car, and the police had actual footage putting the car in that location. The explanation given here is:

> Last month, the police arrested another man: his mother's ex-boyfriend, who had sometimes used [redacted] car.

What makes this even stranger is, if the ex-boyfriend was driving the car, then why was his location in the area? To that, they give the following answer:

> his investigation found that [redacted]ad sometimes signed in to other people's phones to check his Google account.

While it's easy to see a headline like this and reach directly for the panic button, I think the actual circumstances here are fairly unique.

On Monday, April 15, 2019 at 2:37:07 PM UTC-7, [redacted] wrote:

> Moving to [redacted] is for the GMM release process.

On Mon, Apr 15, 2019 at 2:31 PM [redacted] wrote:

> [redacted]

Cross-posting this thread to the Google Maps Mobile discussion group for visibility.

On Mon, Apr 15, 2019 at 2:23 PM [redacted] wrote:

> Merely carrying a cell phone enters you into that territory, as the police have been using cell-tower location data for many years.
> Specifically with Google, #2 "location history" is what you are concerned about. NYT has a discussion on how to disable it:

https://www.nytimes.com/2019/04/13/technology/google-sensorvault-location-tracking.html

On Monday, April 15, 2019 at 2:19:00 PM UTC-7, [redacted] wrote:

> I think this is where the problem lies.
> I'd want to know which of these options (some?

all? none?) enter me into the wrongful-arrest lottery.

And I'd want that to be very clear to even the least technical people.

[redacted]

On Apr 15, 2019, at 2:13 PM, [redacted] wrote:

It looks to me you're mixing a few things:

1) **Device-level location**: that's the "Location" on the quick settings or "Location Services", that enables your device to use GPS & other info to obtain the device's location. Naturally, if you turn that off, you can get the phone's location, and can't use navigation, or find your location on Maps.

2) **Google account Location History**: this is the "Location history" toggle you find in your Google account settings, and enables recording of your location history in your Google Activity. If you disable this, everything still seems to work (expect products/features that use your location history, naturally).

3) **Your Timeline**: this is the Google Maps feature that takes your location history and converts to your "itinerary", with places you visited and activities. Turning this off has no impact on your Location History

Google Maps doesn't need (1) enabled to work (I just tested it), but it does need (1) enabled to (duh) have your location. It doesn't need (2) enabled to work, or (3).

> What else won't work without Location services? Navigation? Play store? Netflix? GPS tracking?

Location services IS GPS tracking. I just tested and all of that work with location services disabled,

> except for navigation as, naturally, you won't have your location to be able to navigate.

In practice, only (1) and (2) matter.

On Mon, Apr 15, 2019 at 2:00 PM [redacted] wrote:

> On Mon, Apr 15, 2019 at 4:13 PM [redacted] wrote:
>
> > Is there an internal document anywhere that lists all of the cases where location information is recorded when the user has opted-out of location sharing?
>
> If you disable the Location toggle on Android (it's available in Quick Settings), there are no such cases. The phone doesn't localize, so no location data is stored, because no location data is generated.
>

Speaking as a user, WTF? More specifically I **thought** I had location tracking turned off on my phone. However the location toggle in the quick settings was on. So our messaging around this is enough to confuse a privacy focused Google-SWE. That's not good.

Second, after turning off the Location toggle, I go to maps. Now it can't find my location and prompts me to turn location services back on. That's **two** fails:

Fail #1: Maps refuses to take No for an answer. Although I turned off location services 20 seconds earlier, Maps is trying to make me second guess my conscious decision. This is the "Not Now, maybe later" antipattern that we still can't seem to wean ourselves off of. What else won't work without Location services? Navigation? Play store? Netflix? GPS tracking?

Fail #2: *I* should be able to get *my* location on *my* phone without sharing that information with Google. This may be how Apple is eating our lunch. I'm not an iOS expert by any means, but it seems Apple does not rely nearly as heavily as we do on transmitting user-identified information into the cloud into order to work with it. They're much more likely to leave the user's data on the user's devices.

--
[redacted]

--
--
[GOOGLE CONFIDENTIAL]

You received this message because you are subscribed to the Google Groups "Industryinfo" group.
To unsubscribe from this group, send email to
[redacted]
For more options, visit this group at
[redacted]

--

[redacted]

--
You received this message because you are subscribed to the Google Groups
[redacted]
To unsubscribe from this group and stop receiving emails from it, send an email to [redacted]
[redacted]
To post to this group, send email to [redacted]
To view this discussion on the web visit
[redacted]

--

--
[GOOGLE CONFIDENTIAL]

You received this message because you are subscribed to the Google Groups "Industryinfo" group.
To unsubscribe from this group, send email to
[redacted]
For more options, visit this group at
[redacted]

--
[redacted]

--
--
[GOOGLE CONFIDENTIAL]

You received this message because you are subscribed to the Google Groups "Industryinfo" group.
To unsubscribe from this group, send email to
[redacted]
For more options, visit this group at
[redacted]