‘Geofence’ Warrant Traps Innocent Bike Rider At Scene Of Crime

Police can now get warrants to demand that Google give up ‘geofence’ records of everyone who was near the scene of a crime. Being at the wrong place at the wrong time can get you busted as a suspect and possible arrest. TN Editor

The email arrived on a Tuesday afternoon in January, startling Zachary McCoy as he prepared to leave for his job at a restaurant in Gainesville, Florida.

It was from Google’s legal investigations support team, writing to let him know that local police had demanded information related to his Google account. The company said it would release the data unless he went to court and tried to block it. He had just seven days.

“I was hit with a really deep fear,” McCoy, 30, recalled, even though he couldn’t think of anything he’d done wrong. He had an Android phone, which was linked to his Google account, and, like millions of other

Americans, he used an assortment of Google products, including Gmail and YouTube. Now police seemingly wanted access to all of it.

“I didn’t know what it was about, but I knew the police wanted to get something from me,” McCoy said in a recent interview. “I was afraid I was going to get charged with something, I don’t know what.”

There was one clue.

In the notice from Google was a case number. McCoy searched for it on the Gainesville Police Department’s website, and found a one-page investigation report on the burglary of an elderly woman’s home 10 months earlier. The crime had occurred less than a mile from the home that McCoy, who had recently earned an associate degree in computer programming, shared with two others.

Now McCoy was even more panicked and confused. He knew he had nothing to do with the break-in – he’d never even been to the victim’s house – and didn’t know anyone who might have. And he didn’t have much time to prove it.

McCoy worried that going straight to police would lead to his arrest. So he went to his parents’ home in St. Augustine, where, over dinner, he told them what was happening. They agreed to dip into their savings to pay for a lawyer.

The lawyer, Caleb Kenyon, dug around and learned that the notice had been prompted by a “geofence warrant,” a police surveillance tool that casts a virtual dragnet over crime scenes, sweeping up Google location data — drawn from users’ GPS, Bluetooth, Wi-Fi and cellular connections — from everyone nearby.

The warrants, which have increased dramatically in the past two years, can help police find potential suspects when they have no leads. They also scoop up data from people who have nothing to do with the crime, often without their knowing – which Google itself has described as “a significant incursion on privacy.”

Still confused – and very worried – McCoy examined his phone. An avid

biker, he used an exercise-tracking app, RunKeeper, to record his rides. The app relied on his phone's location services, which fed his movements to Google. He looked up his route on the day of the March 29, 2019, burglary and saw that he had passed the victim's house three times within an hour, part of his frequent loops through his neighborhood, he said.

"It was a nightmare scenario," McCoy recalled. "I was using an app to see how many miles I rode my bike and now it was putting me at the scene of the crime. And I was the lead suspect."

A powerful new tool

The victim was a 97-year-old woman who told police she was missing several pieces of jewelry, including an engagement ring, worth more than $2,000. Four days after she reported the crime, Gainesville police, looking for leads, went to an Alachua County judge with the warrant for Google.

In it, they demanded records of all devices using Google services that had been near the woman's home when the burglary was thought to have taken place. The first batch of data would not include any identifying information. Police would sift through it for devices that seemed suspicious and ask Google for the names of their users.

Kenyon said police told him that they became particularly interested in McCoy's device after reviewing the first batch of anonymized data. They didn't know the identity of the device's owner, so they returned to Google to ask for more information.

Read full story here…