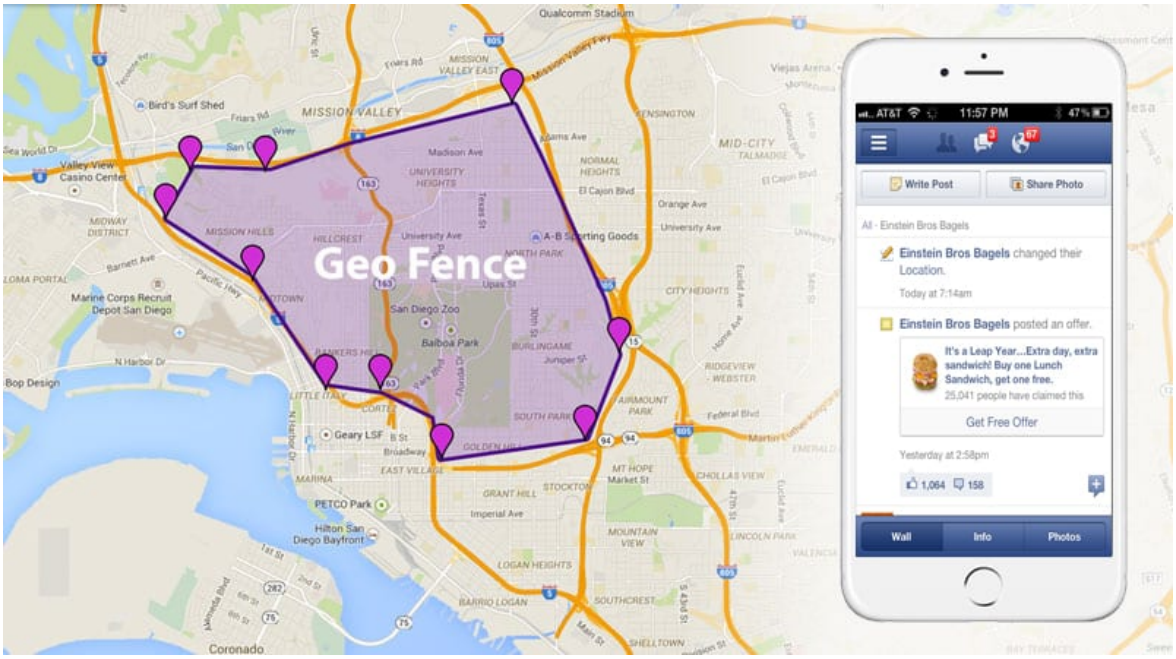

Police Use ‘Geofence’ To Find Anyone Close To A Crime Scene

You could be inadvertently caught up in a police investigation if you happened to be close to a crime scene. It is your cell phone that rats on you as Big Tech firms collect location data. When police figured this out, they went to court to get the data in order to find perpetrators. TN Editor

Police increasingly ask Google and other tech firms for data about who was where, when. Two judges ruled the investigative tool invalid in a Chicago case.

In 2018, 23-year-old Jorge Molina was arrested and jailed for six days on suspicion of killing another man. Police in Avondale, Arizona, about 20 miles from Phoenix, held Molina for questioning. According to a police report, officers told him they knew “one hundred percent, without a doubt” his phone was at the scene of the crime, based on data from Google. In fact, Molina wasn’t there. He’d simply lent an old phone to the man police later arrested. The phone was still signed into his Google account.

The information about Molina's phone came from a geofence warrant, a relatively new and increasingly popular investigative technique police use to track suspects' locations. Traditionally, police identify a suspect, then issue a warrant to search the person's home or belongings.

Geofence warrants work in reverse: Police start with a time and location, and request data from Google or another tech company about the devices in the area at the time. The companies then typically supply anonymous data on the devices in the area. Police use their own investigative tools to narrow down this list. Then they may ask for more specific information—often an email address or a name of the account holder—for a phone on the narrower list.

Critics say the process is an invasion of privacy, often subjecting many people to an unconstitutional search. Now, in a rare step, two judges have denied requests for geofence warrants and questioned whether they complied with Fourth Amendment protections for searches. Lawmakers and activists see the court opinions as steps toward a potential ban on the practice.

"This is as clear as day a fishing expedition that violates people's basic constitutional rights," says New York state assemblymember Dan Quart. Earlier this year, Quart and state senator Zellnor Myrie introduced bills that would prevent authorities from using data gathered from geofence warrants. "It should never be used in a courtroom."

Though relatively new, the practice is becoming increasingly common. Google reported a 1,500 percent increase in requests in 2018 compared with 2017. *The New York Times* reported the company received as many as 180 requests per week last year. Privacy experts tell WIRED that it isn't just Google. Apple, Uber, and Snapchat have all received similar requests.

"This is a tactic that really can be targeted at literally any company," says Albert Fox Cahn, founder and executive director of the Surveillance Technology Oversight Project, a nonprofit civil liberties organization. The New York legislation would bar law enforcement from obtaining location data from tech companies or any of the nameless data brokers

collecting the data from seemingly innocuous apps. The legislation would also prevent law enforcement from bypassing geofence warrants and buying location data directly, as the Secret Service did, a Vice report uncovered.

Read full story here…