TechScape: How police use location and search data to find suspects – and not always the right ones

Publication Date: 2023-10-03

Author: Johana Bhuiyan

Section: Technology

Tags: Technology, TechScape newsletter, newsletters

Article URL: https://www.theguardian.com/technology/2023/oct/03/techscape-geofence-warrants

In January 2020, Florida resident Zachary McCoy received a concerning email from Google: local authorities were asking the company for his personal information and he had just seven days to stop them from handing it over. Police were investigating a burglary, McCoy later found out, and had issued Google what's called a geofence warrant. The court-ordered warrant requested the company look for and hand over information on all the devices that were within the vicinity of the broken-into home at the time of the alleged crime. McCoy was on one of his regular bike rides around the neighbourhood at the time and the data Google handed over to police placed him near the scene of the burglary. McCoy was in the wrong place at the wrong time – and for that he had now become a suspect of a crime he did not commit. This was not an isolated incident. From Virginia to Florida, law enforcement all over the US are increasingly using tools called reverse search warrants – including geofence location warrants and keyword search warrants – to come up with a list of suspects who may have committed particular crimes. While the former is used by law enforcement to get tech companies to identify all the devices that were near a certain place at a certain time, the latter is used to get information on everyone who's searched for a particular keyword or phrase. It's a practice public defenders, privacy advocates and many lawmakers have criticised, arguing it violates fourth amendment protections against unreasonable searches. Unlike reverse search warrants, other warrants and subpoenas target a specific person that law enforcement has established there is probable cause to believe has committed a specific crime. But geofence warrants are sweeping in nature and are often used to compile a suspect list to further investigate. A lack of transparency There's also little transparency into the practice. Though many major tech firms such as Apple and Google regularly publish transparency reports identifying the number of requests for user data they get globally, there's been historically little information on how many of those requests are geofence warrants. Responding to pressure from advocacy firms like the Surveillance Oversight Tech Project (Stop) and the Electronic Frontier Foundation (EFF), Google broke out how many geofence warrants it received for the first time in 2021. The company revealed it received nearly 21,000 geofence warrants between 2018 and 2020. The tech giant did not specify how many of those requests it complied with but did share that in the second half of 2020, it responded to 82% of all government requests for data in the US with some level of information. The company has not published an update on how many geofence warrants it received since then and did not respond to requests for comment by the time of publication. Now, Apple has taken steps to publish its own numbers, revealing that in the first half of 2022 the company fielded a total of 13 geofence warrants and complied with none. The difference? According to Apple's transparency report, the company doesn't have any data to provide in response. An Apple spokesperson did not go into detail about how the company avoids collecting or storing time-stamped location

data in such a way that prevents compliance with geofence warrants, but reiterated the company's privacy principles which includes data minimization and giving users control of their data. While Apple's most recent record on responding to government requests for data also includes complying with 90% of US government requests for account information, experts say the newly published numbers on geofence warrants highlight a clear lesson: "If you don't collect [the data] you can't give it to the government or have it breached by hackers," Andrew Crocker, the Surveillance Litigation Director at EFF, said to the Guardian. 'They're putting their users at risk' Though firms like Google say they carefully and thoroughly review each legal request for data, when faced with valid subpoenas or warrants, there's only so much tech companies can do to fight the requests if they have access to the data. As Apple's transparency report shows, the primary way to protect user data from being swept up in broad law enforcement requests is not to collect it in the first place or, at least, encrypt or otherwise protect it from being searched. But tech firms like Google rely heavily on the collection of user data to pad their bottom line and are often unwilling to do what it takes to protect this data even if there are technical workarounds, said Stop director Albert Fox Cahn. "We know [geofence warrants] are a ubiquitous policing tool, and as long as companies make it possible to comply with these sorts of court orders, they're putting their users at risk," Fox Cahn said. "Whether it's Google or Uber or Lyft or payment companies, by segregating their user data in a way which prevents the aggregated location searches, you can keep that data while preventing compliance with a geofence warrant." Google has more recently faced a swell of pressure from US consumers to better protect location and health information in the aftermath of the Supreme Court's reversal of federal abortion protections. In response, the company said it would mask location information when visiting "sensitive locations" such as reproductive care clinics. But, as the Guardian first reported in November 2022, searches for routes to Planned Parenthood locations and directions to abortion clinics on Google Maps were logged as part of their Google activity timeline for months after. Not an isolated case While experts say there's still more Apple can do to protect user data, like making encryption of personal information the default option rather than requiring people to opt in to it, the transparency report may build on mounting pressure competitors including Google are facing to better protect people from sweeping reverse search warrants. "Google has felt some pressure because of the increased scrutiny of geofence warrants," Crocker said. "And I think that is not going away." In the mean time, geofence warrants continue to upend people's lives, especially as public defenders and attorneys are still learning what these legal requests are – and how to fight them. McCoy is among the fortunate few. Rarely do those whose data are being requested through subpoenas or warrants get notice from the company that their information may be handed over – often they come with gag orders prohibiting the company from notifying the subject of the request. After McCoy received the email he contacted an attorney who filed a motion to quash the subpoena and the local police withdrew the warrant. Many others are not so fortunate. If you want to read the complete version of the newsletter please subscribe to receive TechScape in your inbox every Tuesday