Celebrating An Important Victory In The Ongoing Fight Against Reverse Warrants | ACLU

Chad Marlow, Jennifer Stisa Granick ⋮ 6-7 minutes ⋮ 1/29/2024

For years, the ACLU and other privacy advocates have been challenging law enforcement's growing use of reverse warrants. These problematic warrants include, most prominently, reverse location warrants (also known as geofence warrants), which seek location data to identify anyone who was within a defined area during a specific time period. A second type, reverse keyword warrants, demand the identity of every person who entered a certain word or phrase into a search engine during a set timeframe and possibly within a defined geographic area. The constitutionality of reverse warrants is highly suspect because, like general warrants that are prohibited by the Fourth Amendment, they permit searches of vast quantities of private, personal information without identifying any particular criminal suspects or demonstrating probable cause to believe evidence will be located in the corporate databases they search.

Data provided by Google, which is believed to be the most frequent target of reverse warrants due to its extensive collection of customer location data from Android phones and Internet search data from its eponymous search engine, reflects a significant rise in law enforcement's use of reverse location warrants. For example, the number of reverse location warrants Google received from the federal government grew by 1,171 percent between 2018 and 2020, while the number of reverse location warrants issued to Google by state and local law enforcement grew by 813 percent in California, 901 percent in Florida, 1,291 percent in Michigan, 1,867 percent in Missouri, and 5,333 percent in Massachusetts during that same time period. While reverse warrants present a threat to everyone's privacy, they pose an even greater threat to communities of color, low-income communities, and other groups that are already the target of over-policing. Further, in the aftermath of *Dobbs*, the criminalization of abortion has dramatically increased the likelihood of reverse warrants being used to identify people seeking reproductive care.

Fortunately, at the time the Supreme Court overturned *Roe v. Wade*, the ACLU was already fighting against reverse warrants. In 2022, the ACLU's affiliates in New York and Utah were both involved in legislative efforts to prohibit their use. Each of these early efforts provided important momentum to the anti-reverse warrant cause. In 2023, building upon the anti-reverse warrant efforts in Utah and New York, the ACLU launched a nationwide, multistate effort to ban reverse warrants and saw important progress made on bills in California, Missouri, and Delaware.

During the same time period, the ACLU filed a series of friend-of-the-court briefs arguing that reverse warrants were unconstitutional and conducted without sufficient safeguards. Most recently, we collaborated with library groups to tell the Pennsylvania Supreme Court that Google Search queries, which were the target of a reverse keyword warrant, constitute some of the most private data individuals have and must be protected by state and federal Constitutions.

The ACLU also filed a brief in the Fourth Circuit case of *United States v. Chatrie*, the first case where the defendant called witnesses from Google to demystify the technology and cast doubt on the reliability of geofence surveillance. There, we argued that the geofence warrant for Google location data was so overbroad and unjustified that it was patently invalid.

Watching all this unfold, Google recognized it would increasingly be drawn into the reverse warrant fight.. To avoid being repeatedly placed at the center of these fights, Google announced last month that it was changing how Android phones collect and store user location data. Previously, the "Location History" data collected by a user's Android phone would be sent to Google; now, that data will be stored by default on each user's phone in a manner that is not accessible by Google, much in the way iPhones do. This means that going forward, when Google receives a reverse location warrant, it will not have access to the data needed to comply. Given that no other known collector of

location data has Google's broad customer reach, which is needed to make a reverse warrant useful (learning the identities of a tiny fraction of the people within a geofence is generally not helpful to police), it is highly likely law enforcement use of reverse location warrants will decline, at least for the time being. Consequently, far fewer reverse location warrants will turn people who have done nothing wrong into criminal suspects and threaten others who are merely exercising their basic human rights.

While this is unquestionably an important victory for privacy and the many other rights privacy enables, it is not a complete one. The risk presented by reverse keyword searches (which governments can try to use to identify anyone who enters a term like "Planned Parenthood" or "MAGA" into a search engine) remains unimpacted by Google's location data collection changes. Further, the risk that law enforcement will use emerging technologies to circumvent centuries-old constitutional protections, like the prohibition against general warrants, will continue until contemporary legislatures and courts clearly and affirmatively reject such loopholes.

For these reasons, the ACLU will continue to advocate for bans on the use of reverse warrants at the state and federal level, with an enhanced emphasis on the unaltered risks presented by reverse keyword warrants. In court, like our brief in the Pennsylvania Supreme Court, we will continue to assert that these searches, which are akin to reading someone's most complete and intimate diary, are unconstitutional and give police far too much unchecked power.