

Broad Minnesota Warrant Seeks Data on All Users Who Googled Fraud Victim

COVINGTON

Article By

[Moriah Daugherty](#)

[Covington & Burling LLP](#)

[Inside Privacy](#)

- [Communications, Media & Internet](#)
- [Minnesota](#)

Tuesday, April 11, 2017

A **Minnesota** state court on February 1, 2017, issued an unusually broad [search warrant](#) directed to **Google** in connection with a wire fraud case. The warrant seeks a broad set of data about all users who searched on Google for a specific person between December 1, 2016 and January 7, 2017. The warrant became public after a researcher [published an article discussing the warrant application and judge's order](#).

The warrant was issued in connection with a fraud case. According to the warrant, in January 2017, an individual contacted Spire Credit Union and requested \$28,500 be transferred from the victim's line of credit to the victim's savings account, and then to an account at another bank. That individual provided Spire with the victim's name, date of birth, and social security number—and faxed to the bank a fraudulent passport purporting to belong to the victim. While the faxed passport included biographical data on the victim, it also included a picture of an unknown man who appeared to be a similar age as the victim.

According to the warrant application, Google image searches of the victim's name returned photographs of that unknown man, whereas searches on other search engines (Bing and Yahoo) did not return the same images. Investigators initially sent Google an administrative subpoena requesting subscriber information for all persons who ran a Google search for the victim's name. But Google did not comply, according to the warrant application, because "the request had to do with content"

rather than subscriber information and thus could not be sought by subpoena. Investigators then sought the warrant.

As issued, the warrant seeks a broad range of user and subscriber information for persons who used Google to search for the victim's name, including the users' names, addresses, telephone numbers, dates of birth, and social security numbers. It also seeks information associated with each such user's Google account, including the users' email addresses, payment information, and account information. Finally, the warrant seeks information about the device and network used by each individual that ran such a search, including Internet Protocol ("IP") addresses and media access control ("MAC") addresses.

The geographic scope of the warrant is not clear from the face of the document. Although the warrant contains a formulaic limitation on its scope, stating it seeks information "located in the city or township of Edina, Minnesota," the warrant also lists the place to be searched as Google's headquarters in Mountain View, California.

The breadth of the warrant raises questions about the permissible scope of warrants under the Fourth Amendment. Google has refused to comply with the warrant, [telling a Minnesota newspaper](#), that it "will continue to object to this overreaching request for user data, and if needed, will fight it in court. We always push back when we receive excessively broad requests for data about our users."

© 2019 Covington & Burling LLP

Source URL: <https://www.natlawreview.com/article/broad-minnesota-warrant-seeks-data-all-users-who-googled-fraud-victim>