

Subscribe

Sign In

FORBES INNOVATION CYBERSECURITY

PREMIUM

Feds Ordered Google To Unmask Certain YouTube Users. Critics Say It's 'Terrifying.'

In two court orders, the federal government told Google to turn over information on anyone who viewed multiple YouTube videos and livestreams. Privacy experts say the orders are unconstitutional.

Thomas Brewster Forbes Staff

Senior writer at Forbes covering cybercrime, privacy and surveillance.

Follow

Mar 22, 2024, 04:55pm EDT



The government orders show an "unconstitutional" overreach by the government, multiple privacy experts said. AFP VIA GETTY IMAGES

Federal investigators have ordered Google to provide information on all viewers of select YouTube videos, according to multiple court orders obtained by *Forbes*. Privacy experts from multiple civil rights groups told *Forbes* they think the orders are unconstitutional because they threaten to turn innocent YouTube viewers into criminal suspects.

In a just-unsealed case from Kentucky reviewed by *Forbes*, undercover cops sought to identify the individual behind the online moniker “elonmuskwhm,” who they suspect of selling bitcoin for cash, potentially running afoul of money laundering laws and rules around unlicensed money transmitting.

In conversations with the user in early January, undercover agents sent links of YouTube tutorials for mapping via drones and augmented reality software, then asked Google for information on who had viewed the videos, which collectively have been watched over 30,000 times.

The court orders show the government telling Google to provide the names, addresses, telephone numbers and user activity for all Google account users who accessed the YouTube videos between January 1 and January 8, 2023. The government also wanted the IP addresses of non-Google account owners who viewed the videos. The cops argued, “There is reason to believe that these records would be relevant and material to an ongoing criminal investigation, including by providing identification information about the perpetrators.”

“No one should fear a knock at the door from police simply because of what the YouTube algorithm serves up.”

Albert Fox-Cahn, executive director at the Surveillance Technology Oversight Project

The court granted the order and Google was told to keep the request secret until it was unsealed earlier this week, when it was obtained by *Forbes*. The court records do not show whether or not Google provided data in the case.

In another example, involving an investigation in New Hampshire, the Portsmouth Police received a threat from an unknown male that an explosive had been placed in a trashcan in a public area. The order says that after the police searched the area, they learned they were being watched over a YouTube live stream camera associated with a local business. Federal

investigators believe similar events have happened across the U.S., where bomb threats were made and cops watched via YouTube.

They asked Google to provide a list of accounts that “viewed and/or interacted with” eight YouTube live streams and the associated identifying information during specific timeframes. That included a video posted by Boston and Maine Live, which has 130,000 subscribers. Mike McCormack, who set up the company behind the account, IP Time Lapse, said he knew about the order, adding that they related “to swatting incidents directed at the camera views at that time.”

Again, it’s unclear whether Google provided the data.

“With all law enforcement demands, we have a rigorous process designed to protect the privacy and constitutional rights of our users while supporting the important work of law enforcement,” said Google spokesperson Matt Bryant. “We examine each demand for legal validity, consistent with developing case law, and we routinely push back against overbroad or otherwise inappropriate demands for user data, including objecting to some demands entirely.”

The Justice Department had not responded to requests for comment at the time of publication.

Privacy experts said the orders were unconstitutional because they threatened to undo protections in the 1st and 4th Amendments covering free speech and freedom from unreasonable searches. “This is the latest chapter in a disturbing trend where we see government agencies increasingly transforming search warrants into digital dragnets. It’s unconstitutional, it’s terrifying and it’s happening every day,” said Albert Fox-Cahn, executive director at the Surveillance Technology Oversight Project. “No one should fear a knock at the door from police simply because of what the YouTube algorithm serves up. I’m horrified that the courts are allowing this.”

He said the orders were “just as chilling” as geofence warrants, where Google has been ordered to provide data on all users in the vicinity of a crime.

Google announced [an update in December](#) that will make it technically impossible for the tech giant to provide information in response to geofence orders. Prior to that, a California court had [ruled](#) that a geofence warrant covering several densely-populated areas in Los Angeles was unconstitutional, leading to hopes the courts would stop police seeking the data.

“What we watch online can reveal deeply sensitive information about us—our politics, our passions, our religious beliefs, and much more,” said John Davisson, senior counsel at the Electronic Privacy Information Center. “It’s

fair to expect that law enforcement won't have access to that information without probable cause. This order turns that assumption on its head.”

MORE FROM FORBES

MORE FROM FORBES

Google Just Killed Warrants That Give Police Access To Location Data

By **Cyrus Farivar**

MORE FROM FORBES

This \$4 Billion Car Surveillance Startup Says It Cuts Crime. But It Likely Broke The Law.

By **Thomas Brewster**

MORE FROM FORBES

Experian Is Trying To Force WhatsApp To Hand Over User Data In An 'Odd' Court Battle

By **Thomas Brewster**

MORE FROM FORBES

AT&T And T-Mobile Are Giving Cops Geofenced Location Data, Even Though It's Inaccurate

By **Thomas Brewster**

Follow me on [Twitter](#). Check out my [website](#). Send me a secure [tip](#).



Thomas Brewster

Follow

I'm a senior writer for Forbes, covering security, surveillance and privacy. I'm also the editor of The Wiretap newsletter, which has exclusive stories on real-world surveillance and all the biggest cybersecurity stories of the week. It goes out every Monday and you can sign up here: <https://www.forbes.com/newsletter/thewiretap> I've been breaking news and writing features on these topics for major publications since 2010. As a freelancer, I worked for The Guardian, Vice, Wired and the BBC, amongst many others. Tip me on Signal at +1 929-512-7964. **Read Less**

[Editorial Standards](#)

[Print](#)

[Reprints & Permissions](#)

ADVERTISEMENT

