

This is what happens when ICE asks Google for your user information

March 24 2021, by Johana Bhuiyan



Credit: CC0 Public Domain

You're scrolling through your Gmail inbox and see an email with a strange subject line: A string of numbers followed by "Notification from Google."

It may seem like a phishing scam or an update to Gmail's terms of service. But it could be the only chance you'll have to stop Google from sharing your [personal information](#) with authorities.

Tech companies, which have treasure troves of personal [information](#), have become natural targets for law enforcement and [government requests](#). The industry's biggest names, such as Google, Facebook, Twitter and LinkedIn, receive data requests—from subpoenas to National Security Letters—to assist in, among other efforts, criminal and non-criminal investigations as well as lawsuits.

An email like this one is a rare chance for users to discover when [government agencies](#) are seeking their data.

In Google's case, the company typically lets users know which agency is seeking their information.

In one email The Times reviewed, Google notified the recipient that the company received a request from the Department of Homeland Security to turn over information related to their Google account. (The recipient shared the email on the condition of anonymity due to concern about immigration enforcement). That account may be attached to Gmail, YouTube, Google Photos, Google Pay, Google Calendar and other services and apps.

The email, sent from Google's Legal Investigations Support team, notified the recipient that Google may hand over personal information to DHS unless it receives within seven days a copy of a court-stamped motion to quash the request.

That's a high bar to clear in a short amount of time, said Paromita Shah, co-founder and executive director of immigration rights law firm Just Futures.

"What Google expects you to do is to quash the [subpoena](#) and that would require you to go to federal court," Shah said. "I'd like to know how many people are gonna have the resources and the understanding that they have only seven days to hire an attorney to quash an ICE subpoena in federal court."

The email from Google did not include a copy of the legal request. Upon requesting it, the recipient learned it was an administrative subpoena from the U.S. Immigrations and Customs Enforcement agency. ICE was looking for the names, email addresses, phone numbers, IP addresses, street addresses, length of service such as start date, and means of sources of payment linked in any way to the Google account.

Such requests are not uncommon for Google. From January 2020 to June 2020, Google received nearly 40,000 requests for user information from law enforcement agencies—more than 15,500 were subpoenas, according to an annual transparency report. Of the subpoenas, Google provided "some data" in 83% of cases. For that same period, Facebook received more than 60,000 requests, producing some data in 88% of cases. Twitter received a little more than 3,000 requests and said it had a 59% compliance rate.

Although companies may feel limited in their ability to fight off warrants and court-ordered subpoenas, Shah and immigration advocates argue the tech industry has much more leeway to withhold user information in response to legal requests that did not receive judicial authorization.

In a statement, Google spokesperson Alex Krasov said the company "vigorously" protects users' privacy "while supporting the important work of law enforcement."

"We have a well-established process for managing requests from law

enforcement for data about our users: when we receive a request, we notify users that their information has been requested, push back on overly broad requests to protect users' privacy, and provide transparency around such requests in our transparency report," the statement read.

Subpoenas are one of a handful of legal processes law enforcement agencies deploy to obtain user information, at times in connection with an ongoing criminal or other investigation. Many of these requests come with gag orders, leaving users in the dark until at least a year after the request was issued. Others give users little time or information with which to protect their data.

Law enforcement agencies can gain user information in other ways. Some companies sell user information to data brokers, which in turn sell information to law enforcement agencies, for instance. They're all part of a system that has become available to law enforcement as a byproduct of [tech companies](#)' reliance on a business model of collecting, storing and selling personal information, as well as users' often unconditional willingness to hand over their data.

Administrative subpoenas, such as the one received by the Google user, differ from warrants or court-ordered subpoenas in the type of information they seek and in their enforcement. An administrative subpoena is not self-enforcing—meaning it is simply a legal request and can typically only be enforced by ICE or another issuing agency by going to court if the recipient does not comply. It also has not been signed by a judge and the agency was not required to show probable cause. Unlike a warrant, an administrative subpoena only allows authorities to seek basic subscriber information such as the IP address and how long an account has been active.

Some civil rights and legal groups worry that federal agencies such as ICE could use legal processes such as administrative subpoenas to gain

access to user info to expand surveillance on U.S. residents.

In a freedom of information request, a coalition of groups are asking ICE how many of these requests it has sent to Google, Facebook, and Twitter, pointing out these platforms "contain large amounts of personal data about their users including real-time location, address, and communication data."

"ICE administrative subpoena requests to technology companies for such information would invade the most intimate and personal information about our daily lives, such as location, address and communication," the request, filed by Boston University School of Law Immigrants' Rights and Human Trafficking Program, Just Futures Law, and the Mijente Support Committee, says.

An ICE official said the agency does not routinely send administrative subpoenas to tech companies for noncriminal, civil immigration purposes. The agency also pointed to previous uses of administrative subpoenas to compel the New York Department of Corrections and Community Supervision—in a city whose sanctuary laws prohibit agencies from assisting in federal deportation efforts—to provide ICE with information on several people. In a press release about the use of administrative subpoenas, ICE said it uses "statutorily-authorized immigration subpoenas to obtain information as part of investigations regarding potential removable aliens."

Critics say they are concerned about how hard it is for users whose information is the subject of administrative subpoenas to stop companies such as Google from sharing it, Shah says.

"Google is making it harder to opt out because they put the burden on the person to file a motion to quash," she said. "And that's very typical of corporations. It's really hard for users to opt out of anything, unless you

take extra steps or go to special portals to opt out."

In a letter to Google's Chief Legal Officer Kent Walker, a coalition of immigrant rights groups argued the company should not turn over any information unless the ICE request is accompanied by a judicial order and to reconsider its policy so that "the subscriber has an opportunity to be heard." Google did not respond to specific questions about whether the company will reconsider its policy.

"Providing location data to ICE can cause irreparable harm because ICE uses such information to conduct home raids, incarcerate noncitizens, deport individuals and their families, and tear apart communities," the letter from Immigrant Legal Rights, Mijente, Just Futures Law, and several university immigrant rights clinics says.

While ICE's use of this nonjudicial process has become a concern for those who believe it's been used to "install confusion" about the legal weight it carries, administrative subpoenas are actually one of the more transparent ways law enforcement can request user information from tech companies.

That's partly because such requests don't unilaterally come with gag orders.

The agency would have to go to court to get a gag order, a move that could expose the administrative subpoena—which is a low-cost tool because it doesn't require going to court—to challenges, said Electronic Frontier Foundation staff attorney Andrew Crocker.

(Authorities can request in their administrative subpoenas—as ICE did in this case—that a company not share the information with the user, but it's simply a request.)

Other law enforcement requests, including warrants and National Security Letters, on the other hand, often come with gag orders because notifying the user could interfere with investigations.

In those cases, a user would not be notified. National Security Letters—a type of administrative subpoena issued primarily by the FBI—come with a default gag order that is required to be revisited twice in the course of an investigation, Crocker said. Examples published by Google show one National Security Letter sent to the company in July 2016 that was only disclosed last month, and another that was issued in March 2020 and released in February. In both cases, the subscriber whose information would be requested would have no idea it was handed over until it was disclosed.

Because of this, it's important for providers such as Google to act as a check on [law enforcement](#), Crocker said.

"Otherwise you just don't know what the process is that's been used to get a hold of private stuff," he said. "When you compare that to the way it happens in the real world, if the police want to search your house, they have to get a warrant to do that and then they break your door down or knock. But you know that they're in your house and then they're actually required to give you a list of everything they take."

2021 Los Angeles Times.

Distributed by Tribune Content Agency, LLC.

Citation: This is what happens when ICE asks Google for your user information (2021, March 24) retrieved 20 June 2024 from <https://techxplore.com/news/2021-03-ice-google-user.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.