TECHCRUNCH: FEB 3, 2026 Zack Whittaker is the security editor at TechCrunch.

The Department of Homeland Security has been quietly demanding tech companies turn over user information about critics of the Trump administration, according to reports.

In several cases over recent months, Homeland Security has relied on the use of administrative subpoenas to seek identifiable information about individuals who run anonymous Instagram accounts, which share posts about ICE immigration raids in their local neighborhoods. These subpoenas have also been used to demand information about people who have criticized Trump officials or protested government policies.

Unlike judicial subpoenas, which are authorized by a judge after seeing enough evidence of a crime to authorize a search or seizure of someone's things, administrative subpoenas are issued by federal agencies, allowing investigators to seek a wealth of information about individuals from tech and phone companies without a judge's oversight.

While administrative subpoenas cannot be used to obtain the contents of a person's emails, online searches, or location data, **they can demand information specifically about the user, such as what time a user logs in, from where, using which devices, and revealing the email addresses and other identifiable information about who opened an online account.** But because administrative subpoenas are not backed by a judge's authority or a court's order, it's largely up to a company whether to give over any data to the requesting government agency.

Administrative subpoenas are not new; the use of these self-signed demands by Trump officials to seek identifiable information about people who are critical of the president's policies has raised alarm.

Bloomberg reported last week that Homeland Security sought the identity of an anonymous Instagram account called @montocowatch, which says its goal is to share resources to help protect immigrant rights and due process across Montgomery County in Pennsylvania. This comes amid an ongoing federal immigration crackdown across the United States, which has drawn widespread protests and condemnation. Homeland Security lawyers sent an administrative subpoena to Meta demanding it turn over personal information of the person who runs the account, citing a non-Homeland Security employee who claimed to receive a tip that ICE agents were being stalked.

The American Civil Liberties Union, representing the account owner, said there was no evidence of wrongdoing and that recording police, sharing that recording, and doing so anonymously is legal and protected under the First Amendment. Homeland Security withdrew its subpoena without providing an explanation.

The ACLU called the subpoena "part of a broader strategy to intimidate people who document immigration activity or criticize government actions."

Bloomberg reported the effort to unmask the @montcowatch account was not an isolated incident, referencing at least four other cases where Homeland Security officials used administrative subpoenas in efforts to identify the people running Instagram accounts publishing content critical of the government. Those subpoenas were also withdrawn after the account owners sued to block the attempt.

Tech companies have in recent years published transparency reports that detail how many government demands for data they receive. But most do not break out how many judicial and administrative subpoenas they receive over a period of time, even though the two kinds of demands are fundamentally different.

When asked by TechCrunch, Meta spokesperson Francis Brennan did not say if Meta provided Homeland Security any data involving @montcowatch or if the company was asked to provide information about the account another way.

A new report by The Washington Post on Tuesday found that an administrative subpoena was also used **to seek information from Google** about an American retiree within hours of him after sending a critical email to Homeland Security's lead attorney Joseph Dernbach. The retiree's home was later visited by federal agents inquiring about the email.

The Post described the retiree as someone critical of Trump during his first term, who attended a No Kings rally last year, regularly attends gatherings and protests, and wrote criticisms to lawmakers, all actions protected under the First Amendment.

Within five hours of emailing the Homeland Security lawyer — who was named in an article about the case of an Afghan the U.S. was trying to deport and whose email address is listed on the Florida Bar's website — the retiree received an email from Google, according to The Washington Post. The email notified him that his account had been subpoenaed by the Department of Homeland Security.

The subpoena demanded to know the day, time, and duration of all his online sessions, his IP address and physical address, and a list of each service he used,

and any other usernames and identifiable information relating to his account, such as his credit card, driver's license, and Social Security numbers.

Two weeks later, Homeland Security agents were on his doorstep, asking him questions about the email that he sent to Dernbach, which the agents conceded broke no laws.

Google spokesperson Katelin Jabbari told TechCrunch the company pushes back against overbroad or improper subpoenas, "as we did in this instance," referring to the subpoena referenced in The Washington Post's reporting.

When asked by TechCrunch, Homeland Security assistant secretary Tricia McLaughlin would not say why the U.S. was seeking information about people who have been critical of the Trump administration and accounts documenting ICE activity, or say for what reason the subpoenas were withdrawn.

"HSI has broad administrative subpoena authority under 8 U.S.C. § 1225(d) and 19 U.S.C. § 1509(a)(1) to issue subpoenas," said McLaughlin, referring to Homeland Security Investigations, an investigative unit within ICE.

Not all companies are able to hand over data about their customers. For instance, information that is end-to-end encrypted and can only be accessed by obtaining a person's phone or devices. That said, many companies are still able to provide large amounts of information about their users, including where they log in, how they log in, and from where, which may allow investigators to unmask anonymous accounts.

End-to-end encrypted messaging apps, like Signal, have long championed how little data it collects about its users. The messaging app responds to occasional legal demands by stating that it is unable to produce user datathat it does not have to begin with.

The reliance on U.S. tech giants is another reason why European countries and ordinary consumers are seeking to rely less on American tech giants, at a time when chief executives and senior leaders at some of the largest U.S. tech companies are overtly cozying up to the Trump administration.