

Open Letter: Tech Companies Must Resist Unlawful Subpoenas for User Data

We are sending this letter to the following companies and others that may be receiving subpoenas and other requests for user data from the Department of Homeland Security's (DHS) immigration components: Amazon, Apple, Discord, Google, Meta, Microsoft, Reddit.

Your promises to protect the privacy of users are being tested right now. As part of the federal government's unprecedented campaign to target critics of its conduct and policies, agencies like DHS have repeatedly demanded access to the identities and information of people on your services. Based on our own contact with targeted users, we are deeply concerned your companies are failing to challenge unlawful surveillance and defend user privacy and speech.

The Trump Administration is aggressively targeting social media users engaged in First Amendment activity.¹ We have seen multiple examples of this first-hand. On September 3, 2025, DHS issued a subpoena to Meta seeking to unmask the identities of users who documented immigration raids in California.² DHS issued a similar summons to Meta on September 25, 2025, related to action in Pennsylvania.³ The government withdrew its demands after the users — represented by the ACLU affiliates of Northern California and Pennsylvania—challenged them.⁴ In October 2025, DHS sent Google a subpoena demanding information about a retiree who criticized the agency's policies; in a shocking turn, federal agents later appeared on that person's doorstep.⁵ In another case, Immigration and Customs Enforcement (ICE) issued an April 1, 2025, subpoena to Google in an attempt to locate a Cornell PhD student in the United States on a

¹ See, e.g., EFF, *UAW v. Department of State*, <https://www.eff.org/cases/united-auto-workers-v-us-department-state>.

² *Doe v. DHS*, 3:25-mc-80286, ECF 1-3 (ND Cal. Sept. 18, 2025), <https://www.courtlistener.com/docket/71386144/1/3/j-doe-v-united-states-department-of-homeland-security/> (“DHS subpoena”).

³ *In the Matter of Summons Numbers HSI-PH-2025-082814-001 and HSI-PH-2025-082819-001*, 2:35-mc-80325, ECF 1-4 (ND Cal. Oct. 16, 2025) (“DHS summons”).

⁴ ACLU, *DHS Withdraws Subpoena Seeking to Unmask Instagram Users Who Posted About ICE Raids* (Nov. 25, 2025), <https://www.aclunorcal.org/press-releases/dhs-withdraws-subpoena-seeking-unmask-instagram-users-who-posted-about-ice-raids/>; Ashley Belanger, *DHS keeps trying and failing to unmask anonymous ICE critics online*, *Are Technica* (Jan. 23, 2026), <https://arstechnica.com/tech-policy/2026/01/instagram-ice-critic-wins-fight-to-stay-anonymous-as-dhs-backs-down/>.

⁵ John Woodrow Cox, *Homeland Security is targeting Americans with this secretive legal weapon*, *The Washington Post* (Feb. 3, 2026), <https://www.washingtonpost.com/investigations/2026/02/03/homeland-security-administrative-subpoena/>.

student visa.⁶ The student was likely targeted because of his brief attendance at a protest the year before.⁷ Google fulfilled the subpoena without giving the student an opportunity to challenge it.⁸

We call on companies in receipt of such subpoenas to insist that DHS seek court confirmation that their demands are not unlawful or unconstitutional prior to companies disclosing any user information. We also urge you to notify users about demands for their information with meaningful time to challenge subpoenas on their own. Relatedly, if the government seeks to “gag” you from notifying a user about a demand for their information, you should fight back. We urge you to use your immense resources to defend user privacy in court, if necessary. These steps are not only the right thing to do, they are in line with the existing promises you have made to defend user privacy.

ASKS

1. Do not voluntarily disclose user information in response to subpoenas from immigration components of DHS including those issued under 8 U.S.C. § 1225(d), 19 U.S.C. § 1509, or similar authority, without court confirmation that the subpoena is lawful and enforceable.
2. Provide as much prior notice as possible to users before complying with such subpoenas. In the notice, include at least the following: (1) A copy of the subpoena itself; (2) contact information to legal aid organizations. You can include the Electronic Frontier Foundation’s and the ACLU of Northern California’s intake information: info@eff.org; <https://www.aclunorcal.org/get-help/>.
3. If a demand is accompanied by a gag order, confirm that it is court-ordered, seek the reason for the gag order, and strongly consider challenging it.

⁶ Benjamin Leynse, *Immigration Authorities Subpoenaed Amandla Thomas-Johnson’s Personal Email*, The Cornell Daily Sun (Nov. 5, 2025), <https://www.cornellsun.com/article/2025/11/immigration-authorities-subpoenaed-amandla-thomas-johnson-s-personal-email-now-he-says-cornell-is-refusing-to-tell-him-if-his-school-account-was-also-breached>.

⁷ Amandla Thomas-Johnson, *I had to flee the US – as a foreign, Black, pro-Palestinian activist, I tick every box on Ice’s list*, The Guardian (Oct. 5, 2025), <https://www.theguardian.com/commentisfree/2025/oct/05/palestinian-foreigners-protests-campus-ai-ice-trump-us-migrant>.

⁸ Shawn Musgrave, *Google Secretly Handed ICE Data About Pro-Palestine Student Activist*, The Intercept (Sept. 16, 2025), <https://theintercept.com/2025/09/16/google-facebook-subpoena-ice-students-gaza/>.

EXPLANATION

1. Do not voluntarily disclose user information in response to subpoenas from immigration components of DHS including those issued under 8 U.S.C. § 1225(d), 19 U.S.C. § 1509, or similar authority, without court confirmation that the subpoena is lawful and enforceable.

The federal government—and specifically DHS—has a pattern of issuing administrative subpoenas that do not meet the minimum legal requirements. Companies should insist on court intervention before providing information in response to such subpoenas.

By issuing its unconstitutional and unlawful subpoenas like those described above, immigration-related components of DHS have proved that, going forward, their legal process should be heavily scrutinized and fulfilled only after court intervention. Consider the September 3, 2025 subpoena to Meta.⁹ The subpoena was an unconstitutional infringement on users’ expressive rights to anonymously publish and curate information about law enforcement officers engaged in the exercise of their official duties in public places. And the government did not even defend the subpoena when challenged. The subpoena titled “Officer Safety/Doxing” also exceeded the scope of the agency’s authority on its face. The @LBProtest motion to quash, authored by the ACLU of Northern California, provides a detailed legal analysis of the subpoena’s deficiencies.¹⁰ There are similar deficiencies in a September 25, 2025, summons issued under 19 U.S.C. § 1509 to unmask the user behind a Pennsylvania-based account.¹¹ In that case, DHS relied on authority already disclaimed by the agency’s inspector general.¹²

Companies can use the facial defects of similar subpoenas going forward as reason to force immigration-related DHS agencies to seek court intervention. This will require little to no additional investigation by companies themselves.

The September 3, 2025, subpoena and others like it are facially unconstitutional. In order for a government agency to unmask an anonymous user engaging in expressive activity, the government must “convincingly show a substantial relation between the information sought and a subject of overriding and compelling state interest.” *Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 546 (1963). *See also Highfields Cap. Mgmt., L.P. v. Doe*, 385 F. Supp. 2d 969 (N.D. Cal. 2005) (requiring separate showing). Subpoenas that provide no facts—aside from a bare mention of “Officer safety/doxing”—fail that required showing.

⁹ DHS subpoena, *supra* n.2.

¹⁰ Motion to Quash, *Doe v. DHS*, 3:25-mc-80286, ECF 1 (ND Cal. Sept. 18, 2025), <https://storage.courtlistener.com/recap/gov.uscourts.cand.456560/gov.uscourts.cand.456560.1.0.pdf>.

¹¹ DHS summons, *supra* n. 3.

¹² “Management Alert – CBP’s Use of Examination and Summons Authority Under 19 U.S.C. § 1509,” <https://www.oig.dhs.gov/sites/default/files/assets/Mga/2017/oig-18-18-nov17.pdf>.

In addition, these subpoenas are often facially defective under their authorizing statutes because the statutes give officials the power to engage in immigration enforcement, not free ranging investigations of protected speech at issue in their unsupported claims of “doxing.” See 8 U.S.C. § 1225(d)(4)(A); 19 U.S.C § 1509(a). Separately, in an April 1, 2025, ICE subpoena to Google, the agency did not even attempt to fill in the required “title of the proceeding” associated with the subpoena. By leaving this section blank, ICE may have rendered the subpoena facially invalid. 8 CFR § 287.4(b)(2) (“every subpoena issued under the provisions of this section shall state the title of the proceeding”). This requirement demands both that the title of the proceeding appear on the form, but also that a *proceeding actually exist*. The proceeding should be inquired about by companies to understand why the information is being sought.

Finally, companies have the legal right to insist on court intervention. As with many subpoenas, there are no immediate legal consequences if a company refuses to comply with an immigration-related subpoena in the first instance. *United States v. Minker*, 350 U.S. 179, 187 (1956) (noting “there can be no penalty incurred for contempt before there is a judicial order of enforcement”). Specifically, under 8 U.S.C. § 1225(d)(4)(A), immigration officers have the power to issue subpoenas. But companies have the right to “refuse to respond.” § 1225(d)(4)(B). In those cases, immigration officers “may invoke the aid of any court of the United States” and ask the court to “issue an order” requiring the company to respond. § 1225(d)(4). The law only allows for contempt sanctions if a company fails “to obey such order of the court,” not for a company’s failure to comply with the subpoena in the first instance. § 1225(d)(4)(B).¹³

2. Provide as much prior notice as possible to users before complying with such subpoenas. In the notice, include at least the following: (1) A copy of the subpoena itself; (2) contact information to legal aid organizations.

Companies should keep their existing privacy promises and give users enough time and information to meaningfully challenge such subpoenas. Given the apparent current increase in use of DHS subpoenas, notice to targeted users should be prioritized.¹⁴

Many companies have already rightly promised to provide users with advanced notice when receiving legal requests for user information, unless legally prohibited.¹⁵ This allows users themselves to challenge the subpoena. However, at least two users have recently failed to receive this promised notice when it mattered.

¹³ See also ACLU, *Open Letter to College and University General Counsels* (April 17, 2025), <https://assets.aclu.org/live/uploads/2025/04/ACLU-Open-Letter-to-College-and-University-General-Counsels-4.17.25.pdf>.

¹⁴ According to their transparency reports, Google received 28,622 and Meta received 14,520 subpoenas in the first half of 2025—the most since the companies began tracking them. Google and Meta saw a spike of 3,800 and 1,701, respectively, from the prior six-month reporting period. The companies do not break the numbers out by type: civil, trial, grand jury, or administrative.

¹⁵ EFF, *Who Has Your Back? Government Data Requests 2017*, <https://www.eff.org/who-has-your-back-2017>.

On April 1, 2025, Google received an ICE subpoena for user data and fulfilled it on the same day that it notified the user.¹⁶ Despite Google’s existing promise that it will notify users “before disclosing information,”¹⁷ Google provided the user with what it described as “simultaneous notice”—meaning that Google fulfilled the government request at the same time that it notified the user. Worse still, the notice came from a “no reply” email address, and the subpoena itself was not attached. Subsequently, Google explained that its goal is to provide users with advanced notice of legal process. But sometimes when Google misses its response deadline, it complies with the subpoena and provides notice to a user at the same time to minimize the delay for an overdue production.¹⁸ This is a worrying admission that violates its clear promise to users, especially because there is no legal consequence to missing the government’s response deadline. Deceptive acts or practices are sanctionable at the federal and state level.¹⁹ Google should commit to ending “simultaneous notice” as a policy and disclose how often it has deviated from its existing policy.

Separately, on September 3, 2025, Meta received a CBP/ICE/USCIS subpoena to identify multiple subscriber accounts, but at least one subscriber account did not receive prior notice. The lack of notice to the subscriber was potentially caused by a “technical glitch.”²⁰

Without more transparency from companies, it is impossible to know how often companies fail to give prior notice. And without meaningful notice, people targeted by the government may never have the chance to defend their rights.

It is also important for companies to provide their users with enough information to meaningfully challenge a subpoena in court. Companies like Meta and Google typically do not include a copy of the subpoena at issue in its initial notice to users. And Google sometimes provides notice from a “no reply” email address. This means that if a user wishes to challenge the subpoena, the user must navigate extra steps to even determine what they would be challenging. Companies must provide users with the subpoena itself and contact information for legal resources and further information from the company.

¹⁶ The Cornell Daily Sun, *supra* n.6.

¹⁷ Google, *How Google handles government requests for user information*, <https://policies.google.com/terms/information-requests>.

¹⁸ Google, through outside counsel, provided this information to the Electronic Frontier Foundation.

¹⁹ National Consumer Law Center, *Consumer Protection in the States: A 50-State Evaluation of Unfair and Deceptive Practices Laws* (March 1, 2018), <https://www.nclc.org/resources/how-well-do-states-protect-consumers/>.

²⁰ Shawn Musgrave, *The Feds Want to Unmask Instagram Accounts That Identified Immigration Agents*, *The Intercept* (Sept. 18, 2025), <https://theintercept.com/2025/09/18/dhs-subpoena-ice-instagram-dox/>.

3. If a demand is accompanied by a gag order, confirm that it is court-ordered, seek the reason for the gag order, and strongly consider challenging it.

We understand that immigration authorities sometimes “request” companies “not to disclose the existence of this summons for an indefinite period of time,” attempting to avoid advanced notice to users all together. As you know, these “requests” are not legally binding and companies must continue to refuse them.

If you receive an immigration-related legal process that is accompanied by a legally binding gag order,²¹ you should seek the reason for the gag order from the government and strongly consider challenging them. This will promote user trust and government transparency.

Courts considering the issue have almost uniformly found that nondisclosure orders are prior restraints and/or content-based restrictions. *See In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 881-83 (D. Tex. 2008) (both); *Matter of Grand Jury Subpoena for: [Redacted]@yahoo.com*, 79 F. Supp. 3d 1091, 1091 (N.D. Cal. 2015) (prior restraint); *Microsoft Corp. v. United States Dep’t of Just.*, 233 F. Supp. 3d 887, at 905-907 (W.D. Wash. 2017) (both); *In re Application of the United States of Am. for Nondisclosure Order Pursuant to 18 U.S.C. § 2705(b) for Grand Jury Subpoena #GJ2014032122836*, 2014 WL 1775601, at *2 (D.D.C. Mar. 31, 2014) (both).

To pass constitutional muster, a content-based prior restraints must be necessary to further a governmental interest of the highest magnitude. *See Nebraska Press Ass’n v. Stuart*, 427 U.S. 539, 562-63(1976); *Smith v. Daily Mail Pub. Co.*, 443 U.S. 97, 102(1979). Thus, “[i]f a less restrictive alternative would serve the Government’s purpose,” that alternative must be used. *United States v. Playboy*, (2000) 529 U.S. 803, 813 (2000).

* * *

If you have any question, please reach out to EFF Senior Staff Attorney F. Mario Trujillo (mario@eff.org) and EFF Senior Counsel David Greene (davidg@eff.org).

Signed,

ACLU of Northern California
Electronic Frontier Foundation

February 5, 2026

²¹ A court order is necessary to prevent a company from providing notice to a user. 18 U.S.C. 2705(b).