ICE Issued Hundreds of Requests to Major Tech Companies For Personal Data

Documents Reveal ICE Issued At Least 500 Requests to Google, Facebook, and Twitter for Personal Account Information Between 2018-2021

Background:

Administrative subpoenas are a quick, easy way for law enforcement agencies like ICE to request personal account information from private companies, oftentimes without needing a warrant. Companies are not required to produce records in response to an ICE administrative subpoena – sometimes called an immigration enforcement subpoena – unless ICE also has a court order.[1] Below are key findings from administrative subpoena records obtained via a FOIA lawsuit filed by Just Futures Law and the Boston University School of Law's Immigrants' Rights and Human Trafficking Program.

Finding #1:

ICE use of administrative subpoenas implicates major tech companies in the agency's surveillance dragnet and deportation machine. **Between 2018 - 2021, ICE issued at least 500 administrative subpoenas to Google, Facebook, and Twitter requesting that the companies hand over personal account information that the agency can use to target people for arrests and deportations.**[2] ICE directed the companies to provide a wide array of highly sensitive personal account information, such as:

- Names, usernames, screen names, addresses, emails, phone numbers, and birth dates
- IP address information associated with an account over time
- Payment data (e.g. bank account numbers, credit card numbers, deposits, etc.)
- Account status, such as account start date/time and duration/length of service
- Types of services utilized (e.g. text, three-way calling, SMS data, etc.)
- Call records (including local and long-distance phone records detailing the date, time and duration of incoming and outgoing calls)

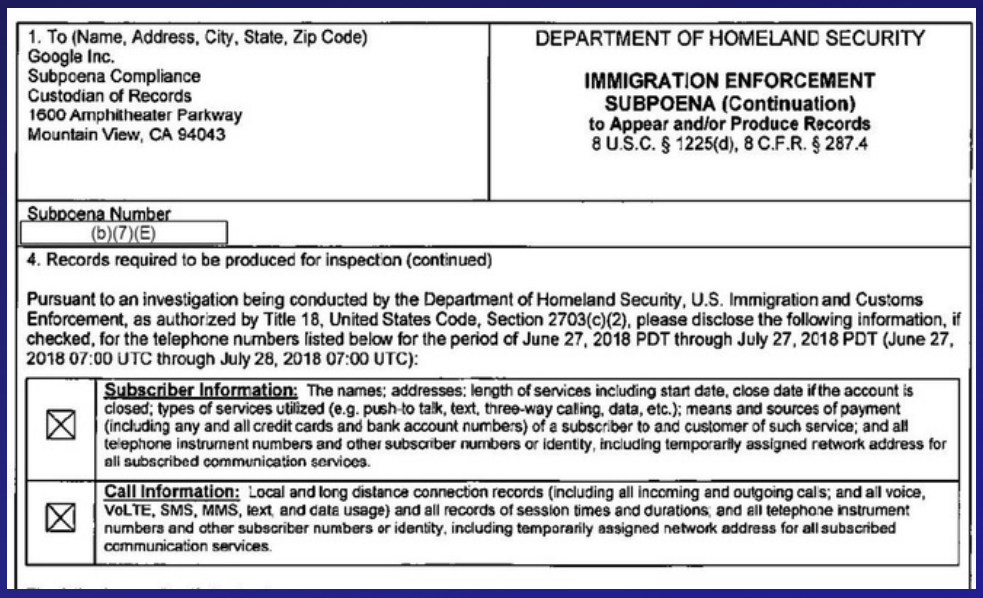
1 Additional background information about ICE use of administrative subpoenas, including guidance for people whose account information is targeted by ICE, is available here: https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/637b9347c01c5f6c2fc3b1b9/1669043016664/JFL+ICE+admin+subpoenas+factsheet+final+edits+%281%29.pdf.

2 The FOIA records show that between January 2018 - March 2021, ICE issued at least 287 administrative subpoenas to Google (including to YouTube), 204 administrative subpoenas to Facebook (which includes Instagram), and 12 administrative subpoenas to Twitter under 8 U.S.C. § 1225(d)(4), 8 C.F.R. § 287.4. However, it is not clear whether these numbers are representative of all administrative subpoenas issued by ICE under 8 U.S.C. § 1225(d)(4), 8 C.F.R. § 287.4 to these companies during this time period, or only a portion of such requests. In addition, ICE has issued subpoenas to tech, telecommunications, and other entities using other purported legal bases.

Finding #2:

Major tech companies have given ICE access to personal account information that the agency can use to target community members. For example:

- In 2020, in response to an ICE administrative subpoena seeking subscriber data and call records associated with two phone numbers, Google provided ICE access to the full name, email address, Google voice number, account start date/time, account ID, and call logs indicating the date, time, duration, and phone numbers for all incoming and outgoing calls and text messages over a 1-month period. The extensive nature of this data sharing suggests that tech companies' cooperation with ICE administrative subpoenas can enable highly invasive ICE surveillance not only of the person the agency is targeting, but also of anyone else that may be communicating with them.



1. To (Name, Address, City, State, Zip Code)
Google Inc.
Subpoena Compliance
Custodian of Records
1600 Amphitheater Parkway
Mountain View, CA 94043

DEPARTMENT OF HOMELAND SECURITY

IMMIGRATION ENFORCEMENT SUBPOENA (Continuation)
to Appear and/or Produce Records
8 U.S.C. § 1225(d), 8 C.F.R. § 287.4

Subpoena Number
(b)(7)(E)

4. Records required to be produced for inspection (continued)

Pursuant to an investigation being conducted by the Department of Homeland Security, U.S. Immigration and Customs Enforcement, as authorized by Title 18, United States Code, Section 2703(c)(2), please disclose the following information, if checked, for the telephone numbers listed below for the period of June 27, 2018 PDT through July 27, 2018 PDT (June 27, 2018 07:00 UTC through July 28, 2018 07:00 UTC):

☒ **Subscriber Information:** The names; addresses; length of services including start date, close date if the account is closed; types of services utilized (e.g. push-to talk, text, three-way calling, data, etc.); means and sources of payment (including any and all credit cards and bank account numbers) of a subscriber to and customer of such service; and all telephone instrument numbers and other subscriber numbers or identity, including temporarily assigned network address for all subscribed communication services.

☒ **Call Information:** Local and long distance connection records (including all incoming and outgoing calls; and all voice, VoLTE, SMS, MMS, text, and data usage) and all records of session times and durations; and all telephone instrument numbers and other subscriber numbers or identity, including temporarily assigned network address for all subscribed communication services.

Figure 1: Example of ICE Administrative Subpoena issued to Google

- In 2020, in response to an ICE administrative subpoena requesting an expansive list of personal data points associated with a particular Twitter account, Twitter provided ICE an account ID number, email address, phone number, username, display name, IP address information, information detailing the date and time that the account was created, and the type of application used to create the account. ICE could potentially use information such as IP address data, which includes some location information, to identify someone's general whereabouts or movements over time. In addition, ICE can combine phone number data with other surveillance tools to produce more detailed information about the location of a person.

Finding #3:

The records indicate that ICE may be using these subpoenas to target media groups covering migrant issues.

- For example, in 2018, an ICE office located in Mexico City, Mexico issued an administrative subpoena to YouTube (which is owned by Google) requesting names, addresses, network addresses, credit card or bank account numbers, "bill face information," and IP addresses for what appeared to be a media channel on YouTube that covered migrant rights issues. While it is not clear from the FOIA records whether or not YouTube provided the requested records in response, the sweeping nature of this request is alarming.

Finding #4:

The tech platforms that we use on a daily basis – including Gmail, YouTube, Facebook, Instagram, and Twitter – could hand over our personal account information at any time to ICE. ICE can then use this information to target us, without us ever knowing.

- Although big tech companies' compliance with administrative subpoenas is not enforceable without a court order, reports suggest that companies tend to comply. Companies' own transparency reports show that they frequently comply with hundreds of thousands of government data requests worldwide on a regular basis.[3]

- ICE administrative subpoenas to tech companies sometimes included a template demand that the company not notify the person being targeted by the agency – but these attempts to restrict companies from notifying their subscribers are baseless without a court order or specific legal authority. Even if companies notify customers of ICE data requests or refuse to comply with a data request, it is highly concerning that decisions about whether personal account information ends up with ICE remain at the discretion of largely unregulated, multinational tech corporations that themselves have a disturbing track record of privacy and data abuses.

---

3 Transparency reports provided by Google and Meta (parent company of Facebook and Instagram) indicate that companies comply with global government requests for data the majority of the time (see: https://transparencyreport.google.com/user-data/overview?hl=en and https://transparency.fb.com/data/government-data-requests/); Twitter's transparency reporting suggests that the company complies with government requests for information less often than its peers: https://transparency.twitter.com/en/reports/information-requests.html#2021-jul-dec.

Finding #5:

In certain cases, ICE administrative subpoenas requested geolocation data and communications content (e.g. video and image files) associated with accounts.[4] For example, three administrative subpoenas issued by ICE to Facebook in 2018 requested, respectively:

- IP log-in information and "any available geolocation data" for a Facebook account user.
- "All media (videos, images and files) and communications stored in the account(s) of the subscriber(s)... and all files that are controlled by user accounts associated with the subscriber(s)..."
- "All public content photos, videos, wall posts, subscriber information and replies from the date range of November 01, 2017 to present."

Conclusion:

These FOIA records show that ICE has requested highly sensitive personal data from major tech companies and tech companies have handed over this information whether customers are aware of it or not. Administrative subpoenas are just one among many ways that ICE is quietly relying on for-profit corporations to gain access to highly sensitive personal information. For example, data broker LexisNexis sells ICE access to billions of data points on 276 million U.S. residents, and ICE buys access to license plate reader data nationwide from Motorola's Vigilant Solutions. At the same time, recent reports suggest that ICE agents have increasingly abused unrestricted access to personal information gleaned from a variety of sources and that ICE's vast use of administrative subpoenas to a range of entities may in some cases be unlawful.

4 These types of data may fall outside the scope of information provided via an administrative subpoena alone (see: 18 U.S.C. § 2703(c)(2)) and if so, ICE would have been required to accompany these data requests with a court order or other legal process to obtain responsive records. The FOIA records included only one accompanying court order, which required a company not to notify the individual the agency was targeting about ICE's request for their data.