

I'm not a robot



Google law enforcement guide

Google provides a dropdown list for users to change the language of their site, featuring 65 options including Afrikaans and many others. Transparency Report Help Center notes that various laws allow governments worldwide to request user information for civil, administrative, criminal, and national security purposes. Each request is carefully reviewed by Google to ensure compliance with applicable laws. If a request seeks too much information, we try to narrow it down or object to providing any data at all. For more information on how Google handles government requests, please see our policies. The laws governing notification of account holders vary by jurisdiction. See our policies for notifying users in how Google handles government requests. When notified via email, Google will not request personal information like passwords or social security numbers. If you receive such a request, it's likely a scam; report it to us immediately. We require all user information requests be sent directly to Google and do not permit "back door" access by governments. Our legal team reviews each request, and we strive for transparency in handling government requests. For more information, see our policies. Google does not sell personal information to anyone, including government agencies. We remain committed to protecting users' information against improper demands and will continue to oppose overly broad or legally objectionable requests. Google reviews every legal request to ensure it satisfies applicable laws and has a track record of pushing back against overbroad demands, including objecting to some entirely. In California, Google asks U.S. state law enforcement officials to attest their requests don't pertain to abortion-related investigations. A government request is when an agency asks Google to disclose info about someone using its services. Most are in criminal investigations but can also be for civil or admin cases. We're revealing stats on these demands. Preservation requests only apply to info Google has at the time, not future-generated data. We report preservation requests separately from user data disclosures. If a government comes back with a legal order, we account for those in the appropriate category. Given article text here As we continually refine our processes and update our data, we aim to provide accurate reports despite the possibility of minor errors. The reporting period from July 2020 to December 2020 excluded requests withdrawn due to COVID-19 before processing. To showcase more information, early time periods might not include new insights. Our disclosure practices began in July 2010 for user information request percentages and January 2011 for numbers of users/accounts requested. This number includes all accounts subject to a government request, even if it's the same account specified multiple times or an existing non-existent one. We've also reduced over-inclusiveness but prioritize greater accuracy. Some requests may not be included, such as when information is anonymized or aggregated, or based on other criteria. If we partially objected to a request but produced user information, that's reflected in the percentage. Conversely, if no information was produced, it doesn't affect the percentage. The MLAT (Multilateral Legal Arrangement Treaty) facilitates cooperation between countries on legal matters like criminal investigations. Google carefully reviews each government request to ensure compliance with applicable laws and limits excessive information requests when necessary. Notifying account holders' rights varies by jurisdiction. For more details, see our policies on handling government requests for user information and notifying users according to local laws. Google processes government requests for user data. If you receive an email asking for sensitive information, be cautious and report it. We require direct access to our systems and review each request thoroughly. Our policies outline how we handle such requests. We don't sell personal info to governments. Instead, we provide an online system for verified agencies to submit secure requests. You can also use Google Takeout to export your content. Government agencies often request information from Gmail, YouTube, Google Voice, and Blogger. This data may include subscriber info, sign-in IP addresses, email content, video upload details, private messages, and blog post comments. We narrow down broad requests whenever possible. Our goal is to protect user privacy while complying with applicable laws. Google has consistently pushed back against government demands for user data, objecting to some requests entirely. The company also requires U.S. state law enforcement officials to attest that their requests do not pertain to abortion-related investigations. Governments can ask Google for information in criminal or civil cases, but preservation requests only apply to information already stored. We are revealing statistics on these demands, excluding those withdrawn due to COVID-19. Our goal is to provide a comprehensive dataset of all government requests from countries we have processed. We receive various types of government requests, including those with multiple identifiers resolving to a single user account. To avoid over-inclusiveness, we've taken steps to minimize this issue, but have decided that a more comprehensive approach is better. However, there are instances where we exclude accounts from the count, such as when information is anonymized or aggregated, or when accounts aren't specifically identified by a request but are based on other criteria. Even if we object to a request in part, if we produce any user information in response to a government request, that request gets reflected in our percentage. On the other hand, if we didn't produce any information at all due to objections or lack of responsive user data, that request isn't included in the percentage. A Mutual Legal Assistance Treaty (MLAT) is an agreement between countries defining how each will assist in legal matters like criminal investigations. Through an MLAT, a government can ask another country for assistance in obtaining information from companies within that country. We carefully review each request to ensure it satisfies applicable laws. If a request asks for too much information, we try to narrow it and may object to producing any information at all. For more information on our policies regarding government requests, see Google's Transparency Report. The laws governing when a provider like Google can notify the account holder vary by jurisdiction. We notify users about legal requests via email, but we will not ask for personal information such as passwords or social security numbers in these emails. If you receive an email from us asking for this type of information, it is likely a scam and should be reported to us. Requests for user information must be sent directly to Google and not through any back door access by the government. Our legal team reviews each request, and we've taken the lead in being as transparent as possible about government requests for user information. For more information on our policies regarding government requests, see Google's Transparency Report. We do not sell personal information to anyone, including government agencies. We remain committed to protecting our users against improper demands for their personal information and will continue to oppose overly broad or legally objectionable demands. **Using Google Takeout for Archived Content & Understanding Government Information Requests** Utilize Google Takeout to create an archived file of your content from most Google services, sharing it with anyone you choose. For government agencies, Google requires valid legal process (except in emergencies) before producing requested information. **Commonly Requested Services: Examples of Disclosable Information** * **Gmail** + Subscriber Info: name, account creation details, associated emails, phone number + Non-Content Info: sign-in IP addresses, email header info (non-content) + Content: email content (if requested and available) * **YouTube** + Subscriber Registration Info + Sign-in IP Addresses & Time Stamps + Video Upload IP Address & Time Stamp + Private Video Copies & Associated Info + Private Message Content * **Google Voice** + Subscriber Registration Info + Sign-up IP Address & Time Stamp + Telephone Connection Records + Billing Information + Forwarding Number + Stored Text Messages & Voicemail Content * **Blogger** + Blog Registration Page Info + Blog Owner Subscriber Information + IP Addresses & Time Stamps for Specific Posts/Comments + Private Post + Comment Content **Google's Review Process & Pushback Against Overbroad Requests** Google meticulously reviews each legal request to ensure compliance with applicable laws. With a history of challenging overly broad or inappropriate demands, including objections to certain requests, Google also adheres to California AB 1242 by requiring U.S. state law enforcement to attest that their requests don't pertain to specific abortion-related investigations. **Understanding Government Requests for User Information** * **Context:** Mostly criminal investigations, but also civil/administrative cases * **Preservation Requests:** Setting aside specific information while awaiting legal process; only applies to existing info at the time of request. Reported separately, as no user data is disclosed in response. **Note:** The original text's structure and some details were modified for clarity and brevity while maintaining the core information and message. We include disclosures related to government requests in our legal process category. Our goal is to present a comprehensive data set covering all user information demands from government agencies. The global report includes categories of government requests from countries we have processed or completed at the time of publication, excluding US national security laws, which are detailed separately. We cannot guarantee error-free data but continually work to improve internal processes and correct or update our data for timely and accurate reports. For July 2020 through December 2020, we excluded withdrawn matters due to COVID-19 prior to processing. We seek new ways to show more information and insights: early time periods may not include this new information. We began disclosing user information request percentages in July - December 2010 and the number of users or accounts requested starting January - June 2011. The "accounts" column reflects the total number of accounts subject to a government request, which is not necessarily an aggregate count of unique users due to factors like duplicate requests for the same account or non-existent accounts. We aim to reduce over-inclusiveness but err on the side of caution. We include instances where information is anonymized, aggregated, or based on other criteria in the request. Even if we objected to a request partially, any produced user information gets reflected in the percentage. Requests with no responsive user information are excluded. Given article text here Google provides e-discovery assistance on complex criminal cases to defense teams nationwide. Before transitioning to private practice, Mr. Ellis spent 13 years as a trial attorney and supervisory attorney with Federal Defenders of San Diego, Inc. He also functions as a digital forensic consultant and expert. The diagram shows wireless access points as orange dots and the estimated range of location sources depicted by grey spheres. The radius for Maps Display has its largest impact from the location information source. Typically, GPS offers the smallest sphere while Cell Sites generally provide the largest. For example, a map display radius for GPS is usually just a few meters but can be over 1000 meters for Wi-Fi. A recent trend involves law enforcement using Google's Sensorvault technology to gather data on individuals present in a specific area at a particular time. This method was initially designed for targeted advertising but has been exploited by authorities to investigate crimes. According to Google, it received 982 geofence warrants in 2018 and over 11,000 in 2020. A three-step warrant process is currently in place, agreed upon between Google and the Department of Justice's Computer Crime and Intellectual Property Section (CCIPS). This involves: 1. **Initial Search:** Upon receiving a geofence warrant, Google searches location history data to identify users with devices within the specified area during the given timeframe. The list includes anonymized user identifiers, device locations, and source information. 2. **Additional Requests:** Law enforcement can request more detailed location data beyond the initial request without geographical limits. This can include compelling Google for additional location coordinates that exceed the original request's time and scope. 3. **Account Identification:** If deemed relevant to an investigation, law enforcement can compel Google to provide account subscriber information such as email addresses associated with accounts and user-provided names. In practice, it appears that law enforcement often skips this step in favor of moving directly to the final analysis. The process has evolved over time, as seen in past examples like "In the Matter of the Search of information stored at premises controlled by Google." Law enforcement agencies have been seeking information about specific Google accounts in various investigations, often involving location data from different time periods. For instance, during a bank robbery on October 13, 2018, authorities were looking for "all Google accounts" within a 30-meter radius around the specified coordinates. Similarly, in another case, law enforcement sought location information for "all Google accounts" between March 1 and 2, 2018, within a geographical box containing specific coordinates. Recently, Google has requested that law enforcement submit Geofence warrants, which are convex polygons in shape. These warrants aim to capture the mobile devices of suspects based on their proximity to the crime scene or surrounding areas. However, the impact of such geofences can be extensive, potentially capturing not only suspects but also innocent individuals who happen to be in the vicinity. A hypothetical example illustrates this concept. Suppose a crime occurs in the parking lot of a strip mall. To increase the chances of capturing the suspect's mobile device, authorities might create a geofence that includes storefronts and surrounding areas. However, this approach could lead to unintended consequences, as it may also capture the devices of people who are not connected to the offense, such as those living in nearby apartments or driving by during the relevant time period. In practice, law enforcement agencies have obtained Geofence warrants with varying Maps Display Radii, which indicate the range within which a device is likely to be located. For instance, one location might be captured with a radius of 5 meters, while another location could be derived from a Cell Site with a much larger radius of 1000 meters. Here's a rewritten text based on the original one: In the initial stage, we'll expand our research and investigate if Suspect One's device was also present in the area north-east of the primary search location. Subsequently, Stage Three will involve obtaining subscriber information from Google for accounts that match their geofence warrant criteria. This process typically yields results such as: As technology advances and consumer privacy concerns evolve, law enforcement agencies are continually adapting to obtain users' location data. However, utilizing Google geofence warrants raises several Fourth Amendment issues; future posts will delve into the legal implications surrounding these warrants. Beyond the legal challenges, individuals encountering Google location warrants should be aware of the limitations of this data and the lack of clear explanations from Google regarding their methodology for determining location information. Interestingly, it appears that Google is more likely to have comprehensive knowledge about Android users' location history compared to iPhone users, as approximately 52% of mobile devices on US networks are iOS-based (Source: Statista). According to Google's policies, most Android devices utilize Google Location Services (GLS) or Google Location Accuracy, which periodically collect and anonymize location data to enhance accuracy. In some cases, this may result in a value of 100 meters being assigned, indicating that the user is likely within a 100-meter radius of their saved coordinates. The collected data includes device numbers, latitude and longitude coordinates, timestamps, map display radii, and the origin of location information, whether it's derived from Wi-Fi, GPS, or cell tower signals. [viii] Id. at 17 [ix] Id. [x] The case of Google Geofence warrants under the Fourth Amendment is well-explained in "In the Matter of the Search of: Information Stored at Premises Controlled by Google." Additionally, for more information on the topic, see EFF's articles about geofence warrants and their potential violation of the Fourth Amendment rights.

Google geofencing law enforcement guide. Google law enforcement phone number. Google law enforcement request. Google law enforcement guidelines. Google for law enforcement. Google llc law enforcement guide. Google voice law enforcement guide. Google gmail law enforcement guide. Google law enforcement contact.