Does a law enforcement agency in the U.S. have to use legal process to compel Google to provide user data or will a phone call be enough?
The government needs legal process—such as a subpoena, court order or search warrant—to force Google to disclose user information. Exceptions can be made in certain emergency cases, though even then the government can't force Google to disclose.

What kinds of emergency cases?
Sometimes we voluntarily disclose user information to government agencies when we believe that doing so is necessary to prevent death or serious physical harm to someone. The law allows us to make these exceptions, such as in cases involving kidnapping or bomb threats. Emergency requests must contain a description of the emergency and an explanation of how the information requested might prevent the harm. Any information we provide in response to the request is limited to what we believe would help prevent the harm.

What types of legal requests does Google receive from U.S. government agencies?
By far the most common is the subpoena, followed by search warrants. A federal statute called the Electronic Communications Privacy Act, known as ECPA, regulates how a government agency can use these types of legal process to compel companies like Google to disclose information about users. This law was passed in 1986, before the web as we know it today even existed. It has failed to keep pace with how people use the Internet today. That's why we've been working with many advocacy groups, companies and others, through the Digital Due Process Coalition, to seek updates to this important law so it guarantees the level of privacy that you should reasonably expect when using our services.

What's the difference between a subpoena, a search warrant and a court order under ECPA? And what information can a government agency get from Google with each?
It's complex, but here's a summary of the different forms of legal process covered by ECPA:

Subpoena
Of the three types of ECPA legal process for stored information, the subpoena has the lowest threshold for a government agency to obtain. In many jurisdictions, including the federal system, there is no requirement that a judge or magistrate review a subpoena before the government can issue it. A government agency can use a subpoena to compel Google to disclose only specific types of information listed in the statute. For example, a valid subpoena for your Gmail address could compel us to disclose the name that you listed when creating the account, and the IP addresses from which you created the account and signed in and signed out (with dates and times). Subpoenas can be used by the government in both criminal and civil cases.
On its face, ECPA seems to allow a government agency to compel a communications provider to disclose the content of certain types of emails and other content with a subpoena or an ECPA court order (described below). But Google requires an ECPA search warrant for contents of Gmail and other services based on the Fourth Amendment to the U.S. Constitution, which prohibits unreasonable search and seizure.

**ECPA Court Order [i.e. an order under 18 U.S.C. § 2703(d)]**

Unlike an ECPA subpoena, obtaining an ECPA court order requires judicial review. To receive an ECPA court order, a government agency must present specific facts to a judge or magistrate demonstrating that the requested information is relevant and material to an ongoing criminal investigation.

With such a court order, a government agency can obtain the same information as a subpoena, plus more detailed information about the use of the account. This could include the IP address associated with a particular email sent from that account or used to change the account password (with dates and times), and the non-content portion of email headers such as the "from," "to" and "date" fields. An ECPA court order is available only for criminal investigations.

**Search Warrant**

The threshold is higher still for an ECPA search warrant. To obtain one, a government agency must make a request to a judge or magistrate and meet a relatively high burden of proof: demonstrating "probable cause" to believe that contraband or certain information related to a crime is presently in the specific place to be searched. A warrant must specify the place to be searched and the things being sought. It can be used to compel the disclosure of the same information as an ECPA subpoena or court order—but also a user's search query information and private content stored in a Google Account, such as Gmail messages, documents, photos and YouTube videos. An ECPA search warrant is available only in criminal investigations. ***

**What are Wiretap, Pen Register and Trap and Trace Orders, and How Do They Differ from Other ECPA Legal Process?**

Some US federal and local government agencies can ask courts to require companies to disclose user information in real-time. In contrast to subpoenas or search warrants, which are used to obtain information created in the past, these types of court orders look to collect information that doesn’t exist yet. They fall into two categories: wiretaps and pen register and trap and trace orders.

**Wiretap**

A wiretap order requires a company to hand over information that includes the content of communications in real-time. Of all the government requests than can be issued under ECPA, wiretap orders are the hardest to obtain. To satisfy legal requirements, a government agency must demonstrate that: a) someone is committing a crime listed in the
Wiretap Act, b) the wiretap will collect information about that crime, and c) the crime involves the telephone number or account that will be tapped. The court must also find that ‘normal’ ways to investigate crime have failed (or probably would fail), or are too dangerous to attempt in the first place. There are limits on how long a wiretap can run and requirements to notify users who have been tapped. **

**Pen Register, and Trap and Trace**

A pen register or trap and trace order requires a company to hand over information about a user’s communications (excluding the content of communications themselves) in real-time. With such an order, a government can obtain “dialing, routing, addressing and signaling information.” This could include the numbers you dial on your phone to reach someone or an IP address issued by an ISP to a subscriber.

It’s easier for a government agency to get a pen register or trap and trace order than a wiretap orders or search warrant. To obtain one, the requesting agent has to certify that information likely to be obtained will be “relevant to an ongoing criminal investigation.” Google believes this standard is too low, and has been working with the Digital Due Process coalition to make sure the court has a meaningful role in determining when these orders are issued.

**What kinds of data do you disclose for different products?**

To answer that, let's look at four services from which government agencies in the U.S. commonly request information: Gmail, YouTube, Google Voice and Blogger. Here are examples of the types of data we may be compelled to disclose, depending on the ECPA legal process, the scope of the request, and what is requested and available. If we believe a request is overly broad, we will seek to narrow it.

**Gmail**

Subpoena:
- Subscriber registration information (e.g., name, account creation information, associated email addresses, phone number)
- Sign-in IP addresses and associated time stamps

Court Order:
- Non-content information (such as non-content email header information)
- Information obtainable with a subpoena

Search Warrant:
- Email content
- Information obtainable with a subpoena or court order

**YouTube**

Subpoena:
- Subscriber registration information
• Sign-in IP addresses and associated time stamps
Court Order:
• Video upload IP address and associated time stamp
• Information obtainable with a subpoena
Search Warrant:
• Copy of a private video and associated video information
• Private message content
• Information obtainable with a subpoena or court order

Google Voice
Subpoena:
• Subscriber registration information
• Sign-up IP address and associated time stamp
• Telephone connection records
• Billing information
Court Order:
• Forwarding number
• Information obtainable with a subpoena
Search Warrant:
• Stored text message content
• Stored voicemail content
• Information obtainable with a subpoena or court order

***