

California Requires Warrant To Search Electronic Communications

Article By:

Katharine Goodloe

On Thursday, October 8, California Governor **Jerry Brown** signed into law the **California Electronic Communications Privacy Act (“CalECPA”)**, which requires law enforcement officials in California to obtain a warrant to access digital records, including emails and text messages.

The new law was supported by privacy rights advocates and technology companies, many of which are pushing for similar reforms to the federal **Electronic Communications Privacy Act (“ECPA”)**. The federal law, enacted in 1986, has been widely criticized as outdated, in part because it purports to permit law enforcement officials to obtain emails older than 180 days with a subpoena, rather than with a warrant. That provision of ECPA was held unconstitutional by the Sixth Circuit Court of Appeals in 2010, but the statute has not yet been updated to require a warrant for all emails, regardless of their age.

The new California law applies to all state and local law enforcement officials in California, who now must obtain a warrant before accessing any “electronic communication information.” That term is defined broadly to include not just the contents of communications, but also the sender, recipient, format, time, and date of the communications; any information about the location of the sender or recipient at the time of the communications; and any information pertaining to any individual or device participating in the communications, including an IP address.

CalECPA also sharply limits the ability of law enforcement officials to obtain information directly from a smartphone or similar device. Before accessing information stored on a device (or information generated through the operation of the device), officials must either obtain a warrant, obtain the consent of the person possessing the phone, or fit into one of the statute’s narrow exceptions (such as those allowing access to phones that are stolen or abandoned).

Certain information still may be accessed with a subpoena, however. Government entities that could obtain electronic communications information with a subpoena under prior law may still do so, but only if that information is not sought for the purpose of investigating or prosecuting a criminal offense. And law enforcement may also issue subpoenas for basic subscriber information — the name, street address, phone number, email address, or similar contact information provided by a subscriber to obtain the account.

CalECPA imposes strict new limits on law enforcement's ability to access and review the information obtained by warrant. For example, all warrants must require that information "unrelated to the objective of the warrant" be sealed and not subject to further review, use, or disclosure without a court order. A court can also order that information be destroyed as soon as feasible after the government's investigation. And courts may appoint special masters to ensure that only information "necessary to achieve the objective of the warrant or order" is produced or accessed when a warrant is executed.

CalECPA also requires the government to notify a person whose information is obtained by warrant at the time the warrant is executed. A court can authorize delayed notice, though, if it has reason to believe a specific adverse event would result from notification. Even persons whose information is obtained through the statute's emergency exception must be notified within three days that their information has been obtained, although this notice likewise may be delayed by court order.

CalECPA expressly authorizes service providers or "any other recipient" of legal process issued under the statute to challenge a warrant, or to petition the court to order the destruction of information obtained in violation of the law. In addition, the law provides there is no cause of action against any California or foreign corporation for providing information or assistance in accordance with the terms of legal process issued under the statute.

© 2024 Covington & Burling LLP

National Law Review, Volumess V, Number 286

Source URL: <https://natlawreview.com/article/california-requires-warrant-to-search-electronic-communications>