

Southern District of New York Significantly Broadens Reach of Warrants under the Stored Communications Act: Forces Microsoft to Produce Customer Email on an Extraterritorial Server

Article By:

Bennett B. Borden

Last Friday, in the Southern District of New York, U.S. Magistrate Judge James C. Francis IV compelled extensive production of the contents of an unnamed user's email account stored on a Microsoft server located in Dublin, Ireland.^[1] This startling ruling could have a significant impact on not only the use of free email services like Hotmail and Gmail, but also all cloud-based services like Office 365, Google Apps, and even cloud providers like Amazon. If this ruling stands and is widely adopted, U.S. service providers may be compelled to produce customer's data regardless of the jurisdiction in which it physically resides.

The **Stored Communications Act (SCA)** was enacted in 1986 as part of the larger Electronic Communications Privacy Act (ECPA), and sought to provide 4th Amendment-like protections to the contents of electronic communications in the hands of service providers like Microsoft. Under the SCA, the government can obtain certain kinds of electronic information held by a service provider only upon a showing of probable cause of wrongdoing. Obtaining the actual content of an electronic communication requires a higher showing than for, say, account information. If the showing requirement is met, a court can issue an SCA Warrant.^[2] The SCA Warrant is served on a service provider, who then conducts a search and produces relevant communications. Prior to this ruling, SCA Warrants typically did not apply to communications stored outside of the jurisdiction of the United States.

In its motion to quash the SCA Warrant in this case, Microsoft's argument was simple: warrants are not subpoenas. If the government served a subpoena on Microsoft, then Microsoft would be required to produce relevant information within its possession, custody or control regardless of where it physically resided. But, by attempting to obtain information located on servers in Ireland via a warrant, the U.S. government sought information outside of the territorial limits of the United States. Because Federal courts have no authority to issue warrants for the search and seizure of property outside the territorial limits of the United States, Microsoft argued it should not be required to produce the information. In support of its argument, Microsoft noted the SCA Warrant is referred to as just that, a "warrant," and also requires to the use of warrant procedures in obtaining it.

This argument, however, failed to convince Judge Francis. After conceding Microsoft's analysis was "not inconsistent with the statutory language" of the SCA, Judge Francis held that the SCA Warrant was not a typical warrant, but was a "hybrid: part search warrant and part subpoena." It is like a search warrant in that an application is made to a magistrate upon a showing of probable cause. But it is executed like a subpoena in that it is served upon a service provider who then conducts the search (as opposed to government agents) and provides the results. The prohibition on extraterritorial searches is based, Judge Francis held, on the concern that government agents were searching and seizing property in a foreign jurisdiction. When the service provider is the one doing to searching and seizing, those concerns are not present.

Judge Francis also focused on the practical consequences that would result from following Microsoft's argument (and previous case law), that it would "seriously impede" legitimate law enforcement efforts, and that individuals could evade an SCA Warrant simply by assuring their data was stored on servers outside the United States. In the short term, an appeal is virtually certain. In a TechNet.com blog post, David Howard, Microsoft's Corporate Vice President & Deputy General Counsel suggested Microsoft would "bring the issue before a U.S. district court judge and probably to a federal court of appeals." David Howard, *One step on the path to challenging search warrant jurisdiction*, TechNet (Apr. 25, 2014, 6:04 PM), available [here](#).

If that appeal fails, this opinion has troubling far-reaching implications. Barring a successful appeal, U.S. service providers may be forced to produce digital content to U.S. government agents— including but not limited to customer emails – no matter whether that content is hosted in Silicon Valley or Siberia.

[1] Microsoft must disclose:

- a. The contents of all e-mails stored in the account, including copies of e-mails sent from the account;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and sources of payment (including any credit or bank account number);
- c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;
- d. All records pertaining to communications between MSN . . . and any person regarding the account, including contacts with support services and records of actions taken.

[2] The evidentiary burdens the government must meet, as well as the specifics about varying kinds of electronic communications are a bit arcane because the SCA is so dated. A full discussion of these intricacies is beyond the scope of this alert. But Judge Francis describes them well [in the opinion](#).

© 2025 Faegre Drinker Biddle & Reath LLP. All Rights Reserved.

National Law Review, Volume IV, Number 121

Source URL: <https://natlawreview.com/article/southern-district-new-york-significantly-broadens-reach->

[warrants-under-stored-commun](#)