

INSIGHTS

Tech Rally – Industry Giants Back Google's Play to Protect Data

March 15, 2017

On March 10, 2017, Google Inc. filed its objection to a Pennsylvania magistrate judge's order to comply with search warrants and turn over personal user data partially stored on foreign servers abroad. A number of technology companies, including Yahoo!, Microsoft Corp., and Apple Inc., filed amicus briefs in support of Google's fight.

In a February decision, U.S. Magistrate Judge Thomas Rueter required that Google comply with warrants issued pursuant to the Stored Communications Act and produce the emails of two targets of criminal investigations – emails stored in "shards" across multiple locations both within the U.S. and abroad. In a departure from the Second Circuit's 2016 *Microsoft* decision, the court ruled that extraterritoriality issues were not implicated because the invasion of user privacy occurs not when Google accesses the data abroad or discloses it, but when law enforcement reviews the electronic data within the United States.

In its objection, Google argues that the focus of the SCA is "protecting the privacy of electronic communications entrusted to service providers by regulating the conditions under which access to those communications may or may not occur." According to Google, the court's view that the key privacy invasion authorized by a SCA warrant occurs only upon review of disclosed communications – excluding the preceding search, seizure, and disclosure – improperly narrowed what conduct is relevant to the focus of the SCA, with the erroneous effect of limiting what conduct is prohibited by the principles of extraterritoriality.

Further, Google stresses the distinction between a subpoena or order and a warrant under the SCA. The first two instruments apply to production of subscriber information and usage records, respectively; the warrant, to customer private communications. Analogizing the difference to a bank retrieving business records versus seizing and retrieving the contents of a customer's safe deposit box, Google argues that such an invasion of a private content is an extraterritorial action not contemplated by Congress in the original SCA or any of its subsequent amendments.

The amici extend and supplement Google's arguments with reasoning based in the text of the SCA, the Federal Rules of Criminal Procedure, and Fourth Amendment jurisprudence. For example, Microsoft, joined by Amazon.com, Cisco Systems, Inc., and Apple Inc., argues that a SCA warrant interferes with a user's ability to exclude and limit access, an important property right. Yahoo, in a separate brief, explains that the SCA incorporates Federal Rule of Criminal Procedure 41 governing warrants, and that the court should look to application of that rule to determine the scope of a SCA warrant.

The common refrain throughout the briefs, including Google's objection, is an exhortation that Congress clarify and update the SCA. The briefs uniformly argue that the court overstepped its bounds in essentially legislating policy preferences on extraterritorial reach. The briefs even offer Congress guidance on some of its options to modernize the statute, for example, by extending the SCA to emails stored abroad, but only those of U.S. citizens and permanent residents; extending the SCA overseas only in national security matters or for certain serious crimes; or requiring notification to foreign governments when a warrant with extraterritorial reach is issued.

It is possible that the new Congress might reform the Electronic Communications Privacy Act, which contains the SCA. Already, the House has passed the Email Privacy Act, which would require law enforcement to obtain a warrant to access emails that are more than 180 days old, a protection not currently in the ECPA. Similar legislation was passed unanimously by the House in the last congress but stalled in the Senate. Such reform efforts may provide an opportunity for stakeholders – such as technology companies, law enforcement, and privacy advocates – to discuss a new path forward on the foreign server issue as well as broader issues arising from the challenges of conducting criminal investigations that attempt to access continually changing technology. As innovation inevitably outpaces legal and legislative developments, companies that store personal data will continue to be in tension with law enforcement over its investigation techniques.

Google's brief objecting to the order is [here](#). Our previous discussion of the *Google* decision is [here](#).