Craig Stewart

Partner
303.295.8478
Denver
cstewart@hollandhart.com

Supreme Court to Consider Whether Companies That Store Data Outside the U.S. Can Be Required to Produce It in the U.S.

Publication — 11/13/2017

Last month, the United States Supreme Court granted certiorari to consider the issue of whether Microsoft must produce, based on a warrant under the Stored Communications Act, the contents of a customer's email account stored on a server located outside the United States. The Supreme Court's ruling on the issue will impact companies which store data outside the U.S., including but not limited to large tech companies like Alphabet/Google, Amazon, and Apple.

The Stored Communications Act, enacted in 1986 as part of the Electronic Communications Privacy Act, generally prohibits the unauthorized acquisition, alteration, or blocking of communications stored in electronic storage facilities. The SCA also addresses voluntary and required disclosures of customer records. A governmental entity may require disclosure of electronic records in certain situations, sometimes requiring a warrant, sometimes not. Companies have argued that the SCA, and the disclosure requirements under it, does not extend to data stored outside of the U.S.

In *Microsoft v. United States*, the United States District Court for the Southern District of New York issued a warrant, served on Microsoft at its Redmond, Washington headquarters, directing Microsoft to seize and produce the email account of a customer alleged to be trafficking drugs. Microsoft complied with the warrant as to data stored in the U.S. Part of the customer's account's content was stored on servers in Ireland, and Microsoft moved to quash the warrant as to that foreign-stored data. The district court denied the motion to quash, and Microsoft appealed.

On appeal, Microsoft contended that Congress's use of the term “warrant” in the SCA includes territorial limitations because law enforcement officers typically can execute a warrant to seize items only in the United States or in U.S.-controlled areas. The government contended that an SCA warrant is akin to a subpoena and requires a recipient to produce materials in its custody or control regardless of where they are located.

The Second Circuit sided with Microsoft. Noting that the focus of the SCA's relevant provisions is on protecting the privacy of a user's stored communications, the court held that the SCA does not authorize a U.S. court to issue and enforce an SCA warrant as to a customer's electronic communications stored on servers outside the U.S. The Second Circuit focused on the location of the data, not on the customer's location or citizenship. It held that enforcing the warrant to compel Microsoft to seize the contents of the customer's communications stored in Ireland constitutes an unlawful, extraterritorial application of the CSA's warrant

provision.

The Supreme Court likely will issue its opinion near the end of this term. Additionally, given the intersection of privacy and security in a world with cross-border crime and terrorism, Congress has considered changes to help the ECPA and SCA address the challenges and technology of the 21st century. Businesses which store data outside the U.S. should stay tuned.

For more information, please contact Craig Stewart (303.295.8478 / cstewart@hollandhart.com) and Romaine Marshall (801.799.5922 / rcmarshall@hollandhart.com).