BARNES & THORNBURG LLP

Second Circuit Confirms Privacy Rights And Territorial Limits Of Search Warrants Under The Stored Communications Act

July 29, 2016 | | The GEE Blog

Meena T. Sinfelt
Partner
White Collar, Compliance and Investigations
Co-Chair

Recently, the U.S. Court of Appeals for the Second Circuit handed Microsoft and privacy advocates a landmark win limiting the "long arm of justice" to within the United States' own borders. In a highly anticipated ruling, the Second Circuit, *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation,* unequivocally stated that the federal government cannot use a search warrant to compel a U.S. corporation to provide the email contents of its customers which are stored *outside* the U.S. Historically, the Department of Justice (DOJ) interpreted its jurisdictional reach to have little or no boundaries. For decades, companies have been required to produce documents and witnesses from overseas for ongoing criminal investigations simply by service of a subpoena. However, a subpoena goes to the custodian of the information the government is seeking and, in many cases, the government does not want the custodian to be aware that the government is investigating. In criminal cases involving foreign located evidence, DOJ would traditionally make a legal request to their government counterparts in a particular foreign country (a Mutual Legal Assistance Treaty, or MLAT, request) in order to receive the evidence. However, the MLAT process is lengthy and poses many other hurdles for the government. With that background, the government has been increasingly using a provision under the Stored Communications Act (SCA) to obtain search warrants directing internet service providers (ISPs), like Microsoft, to obtain the contents of customers' email accounts.[1] *See* 18 U.S.C. § 2701 *et seq*. This was the basic background when the U.S. government served Microsoft with a search warrant for the contents of a customer's email account. The search warrant was constitutionally and procedurally valid on its face. The issue arose when Microsoft attempted to comply with the search warrant. Pursuant to the search warrant, Microsoft produced information which was stored in the U.S. However, certain data requested by the U.S. government was physically stored and maintained in Dublin, Ireland. Therefore, to comply with the search warrant, Microsoft would have had to copy and transfer data from outside the United States. Herein lies the crux of the dispute. With some exception, Rule 41 of the Federal Rules of Criminal Procedure only allows a federal magistrate judge to issue a warrant for property located within its district and restricts the execution of the warrant to the same federal district, but certainly limited to the United States and its territories. *See* Fed. R. Crim. Pro. 41(b)(5). Microsoft, accordingly, moved to

quash the search warrant.[2] Blurring the distinctions between a subpoena and a search warrant, the government opposed the motion to quash, contending that, just like a subpoena, a recipient of a SCA-warrant warrant had to produce records, no matter where they were located, so long as they were in their custody or control. Both the magistrate judge and the chief judge in the Southern District of New York agreed with the government. Microsoft appealed the ruling and one need only look at the list of *amici* in support of Microsoft's position to understand the significance of the Second Circuit's eventual ruling. The list of *amici* reads like a "who's who" in big technology. As technological advances are made, the average citizen increasingly relies on his or her e-mail system or cellular phone to keep more than just correspondence – people keep information related to business, taxes, health, kids, schooling, and the list goes on. The collective position of Microsoft and its *amici* reflects a general trend of increased efforts by private companies to protect individual privacy rights as related to electronic communications, particularly when the information is or the conduct occurs outside the U.S. Further, where a company is merely a custodian or host for the ultimate user's electronic data, it was argued that the court should take additional measures to ensure privacy rights are not violated. Ultimately, the Second Circuit's decision resoundingly confirmed privacy concepts embodied in the Fourth Amendment, stating that a warrant directing a company to seize the contents of its customer's communications which are stored outside the U.S., represents an unconstitutional application of the SCA. Could it be that we are witnessing a judicial trend to uphold traditional constraints on the U.S. government's ability to conduct unlawful searches and seizures? Perhaps the Second Circuit took note of the Supreme Court's recent decision in *McDonnell v. United States*, wherein it stated that a criminal statute will not be construed "on the assumption that the Government will 'use it responsibly.'" If this ruling stands or spreads to other courts, will U.S. companies take proactive measures to safeguard privacy rights and re-evaluate or migrate customer stored data from the U.S. to locations overseas? Will law enforcement's efforts to pursue foreign-based information truly be stifled by the Second Circuit's ruling? Or will the traditional MLAT process continue to provide U.S. law enforcement valuable information while still respecting interests of comity? [1] Under § 2703, the government may prevent a provider of remote computing service from disclosing the existence of the government's request by obtaining a search warrant. [2] Normally, there is limited to no ability to quash a warrant pre-execution. Rather, the aggrieved party must obtain post-execution relief through a motion to suppress. However, the SCA does provide computing service providers with the ability to challenge an SCA-warrant.