Linklaters

July 2016

Overseas Data Protected From U.S. Search Warrant

Appellate court applies "presumption against extraterritorial application of United States statutes," but also distinguishes search warrants from subpoenas.

In a unanimous July 14 decision (available here)[1], an appellate court held that a U.S.-based service provider served with a search warrant did not have to produce data stored and maintained outside the United States.

The U.S. government had sought a warrant under Section 2703 of the Stored Communications Act ("SCA") to gather electronic evidence related to a customer's email account believed to be used in carrying out a narcotics trafficking scheme. The warrant required Microsoft Corporation to seize and produce the contents of one of its customer's email accounts, which Microsoft in part stored in Ireland. At issue was whether the SCA warrant applied to electronic data stored and maintained offshore.

The decision represents a landmark victory for Microsoft, which was supported by court submissions from many other technology and telecommunications companies. The decision – the latest in an ongoing battle between technology companies and the U.S. government over the government's authority to force these companies to assist in its investigations – allows the company to protect customer privacy for information stored abroad, requires the U.S. government to resort to other means to access such data and avoids potential serious conflicts with European data privacy laws.

Microsoft's Data Storage

Microsoft provides web-based email to its customers in over 100 countries and stores the contents of customers' email accounts and other related information on a network of servers housed in various regional data centers, including in Dublin, Ireland. The only way to access customer email data stored in a particular region is by accessing that region's data center and collecting the information. That information can then be transferred electronically to the United States.

Contents

[1] Opinion, *Microsoft Corp. v. United States (In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.)*, Docket No. 14-2985 (2d Cir. July 14, 2016).

The Lower Court's Issuance of the SCA Warrant

Upon being served with the SCA warrant in 2013, Microsoft complied in part by producing email content that was stored on servers located in the United States. Microsoft then moved to quash the warrant as it applied to email content stored in Ireland. The lower court, likening the warrant to a subpoena, denied Microsoft's motion, reasoning that, unlike a traditional warrant, an SCA warrant is executed by a third-party service provider rather than a government agent. This comparison was critical to the lower court's analysis because a subpoena requires the party to "produce information in its possession, custody, or control regardless of the location of that information," whereas warrants traditionally have been limited to require production of materials located only within U.S. territory. The lower court also focused on the location where the government would review the electronic content (in the United States), rather than where Microsoft would seize it (abroad, in Ireland). When Microsoft did not fully comply with the SCA warrant, the court held it in civil contempt. Microsoft appealed.

The Appeal

On appeal, the U.S. Court of Appeals for the Second Circuit, which covers New York, Connecticut, and Vermont, focused on the purpose of the SCA and noted how the technological landscape has changed over the 30 years since its enactment.

The SCA

Congress enacted the SCA to extend constitutional privacy protections to electronic communication and remote computing services. The SCA generally requires service providers not to disclose electronic records unless an exception applies. In answering the question whether the SCA authorized the warrant's enforcement as to customer content stored in Ireland, the appellate court focused on the issue of extraterritoriality – specifically, whether the SCA applied overseas.

i. Plain Meaning of the SCA

The court considered the plain meaning of the SCA and determined that Congress did not intend the SCA to apply extraterritorially. It relied on the seminal U.S. Supreme Court case *Morrison v. National Australian Bank Ltd.*, 561 U.S. 247 (2010), which held that there is a "presumption against extraterritorial application of United States statutes … unless a contrary intent clearly applies." The court observed that the SCA does not explicitly mention, or implicitly allude to, any extraterritorial application.

ii. The SCA's Use of the Term of Art "Warrant"

The court also believed that Congress had intentionally used the "term of art 'warrant'" to convey its traditional legal meaning, which included that warrants "[were] traditionally moored to privacy concepts applied within the territory of the United States."

iii. Relevance of Law on "Subpoenas"

Unlike the lower court, the appellate court was not persuaded by the government's attempt to analogize an SCA warrant to a subpoena. It explained that the SCA treated these as distinct legal concepts, as evidenced by its separate use of the terms "subpoena" and "warrant," and that there was no other reasonable basis in the statute to infer that Congress intended "warrant" to mean "subpoena." It also noted that, contrary to the government's contention, warrants have been executed by third parties, who then are considered government agents. Finally, the court rejected any attempt by the government to import law developed in the subpoena context into the SCA's warrant provisions.

Determining Whether the SCA Warrant Would Require a Prohibited Extraterritorial Application

Having determined that the SCA's warrant provisions did not contemplate extraterritorial application, the appellate court then considered whether the SCA warrant at issue in fact would involve extraterritorial application. In making this determination, the court found that the "focus" of the SCA was its privacy provisions (and not, as the government contended, its disclosure provisions). In light of this focus, the court held that the execution of the SCA warrant would constitute an unlawful extraterritorial application because the invasion of the customer's privacy, i.e., where Microsoft seizes the customer's protected content, would occur in the Ireland data center.

The EU Perspective

Although the Second Circuit's opinion did not address potential conflicts with foreign data privacy laws, the SCA warrant posed particular challenges under European privacy law. The information held by Microsoft in Ireland contained "personal data" regulated under the EU's Data Protection Directive 95/46/EU ("the Directive"). Both the collection and transfer of the data to the United States from Ireland posed potentially significant challenges under that Directive. Although the Directive recognizes processing and transfer of personal data in response to mandatory legal obligations, it is generally regarded that those legal obligations must be EU legal obligations, rather than those imposed by non-EU law.

A mandatory U.S. legal obligation – of purported extra-territorial effect – requiring disclosure of data located in Ireland would have put Microsoft at grave risk of breaching the Irish implementation of the Directive. While existing sanctions under the Directive may be non-threatening, the EU General Data Protection Regulation (the "Regulation"), which replaces the Directive in May 2018, exposes those subject to the Regulation to fines of up to 4% of global group-wide turnover. A pattern of extraterritorial requests from the United States, in breach of EU privacy law, could have left technology companies in potentially significant conflict with the new Regulation and its severe financial penalties.

Implications

This decision is an important victory for technology companies and will protect user privacy and shield technology and telecommunications companies from search warrants seeking the production of customer data held outside the United States. But it is important to note that the decision did not address the extraterritorial reach of subpoenas, which require companies to turn over materials in their "possession, custody, or control," and which some courts have interpreted to apply abroad.

From an EU perspective the decision not only averts a potential serious conflict with EU data protection regulations applying the Directive and the Regulation described above, but also helps trans-Atlantic negotiations in other privacy areas. In particular, the decision should help the recently adopted US-EU Privacy Shield (a replacement for the Federal Trade Commission's Safe Harbor scheme) fend off challenges from privacy advocates in the EU.

Given its wide-reaching implications, this Second Circuit decision is unlikely to be the final word in the ongoing dispute between technology companies and the U.S. government over the government's authority to force these companies to assist in its investigations.

Linklaters

Contacts

For further information please contact:

Richard Cumbley
Partner
+44 207 456 4681
richard.cumbley@linklaters.com

Paul Hessler
Partner
+1 212 903 9132
paul.hessler@linklaters.com

Georgina Kon
Partner
+44 207 456 5532
georgina.kon@linklaters.com

Adam Lurie
Partner
+1 202 654 9227
adam.lurie@linklaters.com

Douglas Tween
Partner
+1 212 903 9072
douglas.tween@linklaters.com

Efrat Fish
Associate
+1 212 903 9440
efrat.fish@linklaters.com

Caitlin Potratz
Associate
+1 202 654 9240
caitlin.potratz@linklaters.com

1345 Avenue of the Americas
New York, NY 10105

Telephone +1 212 903 9000
Facsimile +1 212 903 9100