SHEARMAN & STERLING LLP

LITIGATION, PRIVACY & DATA PROTECTION | July 19, 2016

In the Matter of Microsoft: Why It Matters

On July 14, 2016, the Second Circuit released its decision in *Microsoft Corp. v. United States*, No. 14-2985, slip op. (2d Cir. July 14, 2016). The Second Circuit rejected the Government's efforts to require Microsoft to turn over emails held overseas in its data center in Dublin, Ireland pursuant to a judicially-authorized search warrant. This decision may have significant implications for where corporations store their data in the future and on the US Government's ability to use certain investigative techniques to obtain overseas data, such as email search warrants.

Background on ECPA/Morrison Case

The Electronic Communications Privacy Act (ECPA) was enacted in 1986 to address, in part, the interception of computer, digital and electronic communications. Title II of the ECPA, which is commonly called the Stored Communications Act (SCA), "protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers." Under the SCA, some information can be obtained from service providers by subpoena, other information requires a court order (often known as a "2703(d) Order), and still other information (including email content) can be obtained with a search warrant.

In a 2010 decision, *Morrison v. National Australia Bank Ltd.*, the Supreme Court emphasized the presumption, when interpreting United States laws, that Congress intended legislation to apply "only within the territorial jurisdiction of the United States" unless it is clear that the legislation is intended to apply extraterritorially. In *Morrison*, non-American purchasers of National Australia Bank (NAB) stock—all of whom bought their shares outside of the United States—sued NAB and its American subsidiary in a US district court. The Supreme Court held that the Securities Exchange Act of 1934 does not provide a cause of action to foreign plaintiffs, suing foreign and American defendants, for alleged misconduct in connection with non-domestic transactions in securities listed on a foreign stock exchange. The "longstanding principle" invoked by the Court, that US laws only apply within the territorial jurisdiction of the United States unless expressly stated otherwise, was reaffirmed by the Supreme Court this year in *RJR Nabisco, Inc. v. European Cmty*.

The Microsoft Case

In *Microsoft*, the Second Circuit held that the Government could not obtain a search warrant under the SCA to obtain electronic communications from Microsoft that were held on servers in Ireland. The Second Circuit reasoned that Congress did not intend the SCA's warrant provisions to apply extraterritorially. "When, in 1968, Congress passed the Stored Communications Act as part of the broader Electronic Communications Privacy Act, its aim was to protect user privacy in the context of new technology that required a user's interaction with a service provider. Neither explicitly nor implicitly does the statute envision the application of its warrant provisions overseas." The

primary focus of the SCA was to protect "users' privacy interests in stored communications," and a search warrant protects privacy "in a distinctly territorial way."

Because the information sought from Microsoft was stored exclusively in Ireland, the Circuit held that the court's issuance of a warrant in these circumstances would be extraterritorial and in violation of the "longstanding principle" raised in *Morrison*. The Circuit recognized the importance of foreign privacy interests, noting, "But we find it difficult to dismiss those interests of hand on the theory that the foreign sovereign's interests are unaffected when a United States judge issues an order requiring a service provider to 'collect' from servers located overseas and 'import' into the United States data, possibly belonging to a foreign citizen, simply because the service provider has a base of operations within the United States."

Impact on Data Privacy Laws

The Microsoft decision matters because the US Government was seeking to obtain data stored from Ireland via a judicially-authorized search warrant, which would violate Irish data protection law. If the US Government were allowed to obtain overseas data pursuant to such a search warrant, then Microsoft and many other companies storing data abroad would be placed in a difficult position—turn over data in violation of the laws of the countries where they store data, or risk contempt sanctions for failing to comply with a US court order.

This could have created a competitive disadvantage to the US tech industry. Customers would have a choice between using a US cloud service provider, subject to the ECPA, and an Irish cloud service provider, which is not subject to the ECPA and which could provide some legal protections against the US Government's ability to collect data pursuant to search warrants under the SCA. The outcome of the case here shows that customers overseas should be able to use products and services from a US company without losing certain legal protections and rights in their country. It should be noted, however, that the *Microsoft* Court did not address all potential avenues through which the US Government could collect overseas data via the ECPA. In certain instances, for example, US authorities may seek to rely on a grand jury subpoena to collect old email content—typically over 180 days—and the Circuit stated that the enforceability of such subpoenas was not before it.

The EU has been very focused on the reach of US Government data activities. By way of example, the European Court of Justice struck down the US-EU Safe Harbor arrangement last year citing those concerns, which was one of the main vehicles by which companies were able to transfer data from the EU to the US. A new agreement—called the EU-US Privacy Shield program—was just finalized last week. For those that were watching the Microsoft case, the decision by the Second Circuit should assuage some of the EU's concerns about the reach of US Government activities and lower the risk that the new data sharing agreement would be challenged by EU authorities.

The Second Circuit's decision may also have a significant impact on the US Government's ability to obtain data from countries like China and Russia pursuant to the ECPA, since those countries, like the EU, have passed data protection laws that require certain data to be maintained within their borders. China, for example, promulgated guidelines in 2013 limiting the types of data that can be transmitted abroad and the circumstances under which such data can be sent, and for decades has prohibited the dissemination of "national secrets" beyond its borders. Similarly, Russia in 2014 adopted Federal Law No. 242, which prohibits storing the personal data of Russians

outside of the Russian Federation. Under the framework adopted by the Second Circuit, US federal authorities would be unable to collect data from servers stored within these countries using a SCA warrant.

Key Takeaways

- The Second Circuit's holding makes clear that materials stored on servers outside of the United States cannot be collected using an SCA warrant. The Court of Appeals did not, however, decide whether information from these sources was immune to collection under the SCA in its entirety.
- As a matter of public policy, the Court of Appeals was most concerned about the location of the data subject to search, rather than the location of the person or entity impacted by the search, when the identity of such person or entity is unknown.
- The holdings in the case will have implications on how the US Government may approach data collection from US companies pursuant to the ECPA, and US-based companies may benefit from evaluating where their data is stored and how they respond to requests for data.
- In order to address the complexities of modern technology, this case may provide impetus for Congress to update the SCA, a law enacted before the widespread use of the Internet, to clarify how data maintained overseas may be collected.

CONTACTS

Jeewon Kim Serrato
Washington, DC
+1.202.508.8032
jeewon.serrato@shearman.com

Adam S. Hakki
New York
+1.212.848.4924
ahakki@shearman.com

Agnès Dunogué
New York
+1.212.848.5257
agnes.dunogue@shearman.com

Christopher L. LaVigne
New York
+1.212.848.4432
christopher.lavigne@shearman.com

Richard C. Hsu
Menlo Park
+1.650.838.3774
richard.hsu@shearman.com

Benjamin Klebanoff
New York
+1.212.848.7316
benjamin.klebanoff@shearman.com

599 LEXINGTON AVENUE | NEW YORK | NY | 10022-6069