Implications of Microsoft's win in overseas server email case

On 14 July 2016, the United States Court of Appeals for the Second Circuit released its decision in *Microsoft Corp. v. United States*, rejecting the US Government's efforts to require Microsoft to turn over emails held overseas in its data centre in Dublin, Ireland, pursuant to a judicially authorised search warrant. Jeewon Kim Serrato, Agnes Dunogue and Christopher LaVigne of Shearman & Sterling LLP explain how this decision, while narrow, runs counter to a trend in which courts have generally accepted the US Government's efforts to obtain evidence stored abroad, and discuss how the case may have meaningful implications for where corporations store their data in the future and on the US Government's ability to use certain investigative techniques to obtain data stored overseas.

The *Microsoft* decision

The *Microsoft* case[1] began three years ago when a Southern District of New York Magistrate Judge issued a search warrant compelling Microsoft to disclose the contents of an email account at Microsoft's free online service, 'msn.com.' The Judge issued the warrant, based on the US Department of Justice's underlying affidavit, which established probable cause to believe that the email account had been used in connection with a narcotics trafficking investigation. Microsoft complied with the warrant and provided some of the data that was stored on Microsoft's servers located in the United States but refused to provide the emails that were stored on a server in Ireland. Microsoft argued that the emails stored in servers outside of the US were beyond the reach of the warrant issued pursuant to the Stored Communications Act ('SCA') 1986. The US Government argued (and Microsoft conceded) that the company could pull information from any of its servers and that the warrant could compel a Microsoft employee in the US to pull the emails from the Irish server. The District Court agreed with the US Government, ordered Microsoft to provide this data, and Microsoft appealed.

In reversing the District Court's decision, the Second Circuit in July 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[2]."

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, commonly called the SCA, "protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers[3]." Under the SCA, some information can be obtained from service providers by *subpoena*, whereas other information requires a court order (often known as a '2703(d) Order') and still other information (including email content) can only be obtained with a search warrant.

The US Government argued that a search warrant under the SCA functioned similar to that of a *subpoena* for the purposes of this analysis, and applied extraterritorially: "[a] 'warrant' issued under the statute functions as a form of compelled disclosure - that is, a court order requiring the recipient to disclose certain records[4]." The Second Circuit rejected this argument.

According to the Second Circuit, 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[5]." Furthermore, the court emphasised a "longstanding principle" articulated in a 2010 Supreme Court decision, *Morrison v. National Australia Bank Ltd.*, that a statute must contain a "clear indication of an extraterritorial application" in order to apply extraterritorially[6]. The Court of Appeals found that the plain language of the SCA did not contain a clear indication of extraterritorial application, and that the information sought from Microsoft was stored exclusively in Ireland. Therefore, the Second 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 *Microsoft* decision, however, states only that the warrant provisions of the SCA may not be applied extraterritorially. The Second Circuit did not address whether the US Government could unilaterally obtain foreign-stored evidence through the use of a *subpoena* under the SCA.

Impact of the decision on privacy and cross-border data searches

In analysing the impact of the decision, it is important to note the specific set of facts that were before the Court.

First, the specific subset of emails in question were emails that were recent (less than 180 days old), and that resided on Microsoft's servers located outside the US and that, according to statements made in the case, do not exist in any form or part (back-up or otherwise) on the company's servers in the US. If the emails were older than 180 days, or if Microsoft had a copy of all or part of the customer's email account on a server in the US, the outcome of the case may have been different.

Second, neither the customer's citizenship nor the physical location were known. Although Microsoft stated in its argument that the email accounts were stored on servers that are closest to the customer, this case was not about an Irish citizen's data being stored in Ireland. The Court of Appeals, therefore, did not address whether the outcome of the case would have been different if the email account belonged to an Irish citizen or to a US citizen. Arguably, if the US Government sought overseas email content belonging to a US citizen who is located in the US, the case may have had a different outcome.

The *Microsoft* decision leaves open the question of how the law will be interpreted when the citizenship of the data owner is known - and which country's laws should apply

While the *Microsoft* case has been described in the media as a significant success for privacy advocates[7], the impact of this decision may be more complex than what it seems at first blush. The Court of Appeals based its decision on the location of the server, not the citizenship of the email account's owner or the 'citizenship' of the data controller (in this case, Microsoft). This may be contrary to the European Union's perspective on data privacy. According to the EU General Data Protection Regulation, which goes into effect in May 2018, the EU data privacy principles apply to data controllers who process the personal data of Europeans regardless of whether the processing takes place within the EU or not. In other words, the *Microsoft* decision focused on where the data is stored, whereas the EU data protection regulation will apply based on whose information is being processed. The *Microsoft* decision leaves open the question of how the law will be interpreted when the citizenship of the data owner is known - and which country's laws should apply.

Third, the *Microsoft* decision is binding precedent in the Second Circuit and other Circuits may have different views. The case could also be appealed to the US Supreme Court, which could overturn the Second Circuit's decision, uphold it or find that its holding is no longer relevant in assessing the warrant provisions of the SCA. Specifically, the SCA notes that a warrant obtained to compel the production of communications should generally be issued "using the procedures described in the Federal Rules of Criminal Procedure." The Second Circuit applied Rule 41 pertaining to federal warrants, and determined that the geographical scope of warrants under Rule 41 was limited to US territory. Reflecting potential disagreement, the US Supreme Court adopted a proposed amendment to Rule 41 of the Federal Rules of Criminal Procedure on 28 April 2016 while the decision in the *Microsoft* case was pending[8]. The amendment altered the text of Rule 41 to permit a magistrate judge to issue a warrant for information located outside of the US if the location of the information has been concealed through technological means[9]. While it does not appear that this amendment would have been applicable to the *Microsoft* case if it had been in effect, other Circuit courts of appeal may find an extraterritorial element in the amended Rule 41 that the Second Circuit found lacking in the *Microsoft* decision.

Judge Gerard Lynch in his concurring opinion in *Microsoft* wrote that Congress should adopt a "more complex balancing exercise" and stated: "I am skeptical of the conclusion that the mere location abroad of the server on which the service provider has chosen to store communications should be controlling, putting those communications beyond the reach of a purely 'domestic' statute. That may be the default position to which a court must revert in the absence of guidance from Congress, but it is not likely to constitute the ideal balance of conflicting policy goals[10]."

Perhaps taking a cue from this call for legislative action, the day after the *Microsoft* decision, the US Department of Justice published draft legislation to update the laws for cross-border data requests. The Obama administration is also working to negotiate and implement new bilateral agreements with foreign governments that would permit

foreign governments to serve US technology companies with warrants for email searches and wiretaps and grant the US reciprocal authority[11]. A group of legislators is also sponsoring a law known as the International Communications Privacy Act, which seeks to amend the ECPA.

The debate in the US is far from over and undoubtedly the view in the EU that its laws may apply extraterritorially based on the citizenship of the data owner may also need to be considered in context.

What businesses need to know

The *Microsoft* decision restricts somewhat the US Government's capabilities in collecting data. However, it does not dramatically alter the US Government's present ability to collect information from foreign countries. While the decision itself protects corporations storing information abroad from search warrants issued under the SCA, it does not protect them from other unilateral mechanisms of compulsion. It also does not diminish the US or other countries' ability to request data from the 'host country,' when the citizenship of the data owner is known.

That said, for companies based inside and outside the United States that are assessing their data privacy policies, this means that a careful consideration of the location of the data will be helpful when they receive a data request from the US Government. Companies should also have set procedures for handling such data requests, which include a review of the relevant data protection laws that apply in a particular case.

In the long term, the Second Circuit's decision may spur action by the US Government to update its laws surrounding electronic communications stored abroad. The *Microsoft* case may also encourage other countries to push for data localisation and demand that their citizens' data be stored only in their own countries. For tech companies that build or rent data centres around the world, monitoring these developments will be key to determining how their users' data may be stored in various locations to meet customer demand. For smaller businesses and startups, this may mean they can no longer respond to customers by stating their data is "somewhere in the cloud."

Jeewon Kim Serrato Counsel
Agnes Dunogue Partner
Christopher LaVigne Partner
Shearman & Sterling LLP, Washington, DC, and New York
jeewon.serrato@shearman.com
agnes.dunogue@shearman.com
christopher.lavigne@shearman.com

The authors would like to thank Benjamin Cohen and Benjamin Klebanoff, Associates at Shearman & Sterling LLP, for contributing to this article.

1. —F.3d—, 2016 WL 3770056 (2nd Cir. 2016).
2. Ibid at *1.
3. Electronic Communications Privacy Act of 1986, US Department of Justice, https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (last revised 30 July 2013).
4. Brief for the United States at 9, Microsoft Corp., —F.3d—, 2016 WL 3770056 (No. 14-2985), 2015 WL 1139654.
5. 2016 WL 3770056, at *12.
6. 561 U.S. 247, 255 (2010).
7. See, e.g., Delvin Barrett & Jay Green, 'Microsoft Wins Appeals Ruling on Data Searches,' Wall Street Journal, 14 July 2016, http://www.wsj.com/articles/microsoft-wins-appeals-ruling-on-data-searches-1468511551; Henry Farrell, 'Microsoft Just Won a Big Privacy Fight with the Government. Here's What that Means.,' Washington Post: Monkey Cage Blog, 15 July 2016, https://www.washingtonpost.com/news/monkey-cage/wp/2016/07/15/microsoft-just-won-a-big-privacy-fight-with-the-government-heres-what-that-means/
8. Order re Amendments to the Federal Rules of Criminal Procedure at 6, US, 28 April 2016, https://www.supremecourt.gov/orders/courtorders/frcr16_mj80.pdf
9. Ibid at 6 - 7.
10. Microsoft Corp., —F.3d—, 2016 WL 3770056, at *25-26 (Lynch, J., concurring).
11. Delvin Barrett & Jay Green, 'U.S. to Allow Foreigners to Serve Warrants on U.S. Internet Firms,' Wall Street Journal, 15 July 2016, http://www.wsj.com/articles/obama-administration-negotiating-international-data-sharing-agreements-1468619305