

Expert comment

Rob Corbet is a Partner at Arthur Cox — the views expressed are his own

On 25th April 2014, a New York court ordered Microsoft to comply with a search warrant to disclose a large amount of content, contact, payment and other data relating to an email account hosted in Ireland. The decision sheds light on the views of certain members of the US judiciary towards sovereign jurisdiction and, in particular, the extent to which a US court should be able to compel the production of data stored in servers overseas — in this case, in Dublin.

Background

The facts of the case in question ('In Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation', 13 Mag. 2814, heard by Judge James Francis IV) were quite straightforward.

On 4th December 2013, Judge Francis issued a search warrant in favour of the US government authorising the search and seizure of information associated with a specified web-based email account that was 'stored at premises owned, maintained, controlled, or operated by Microsoft Corporation'. Microsoft sought to quash the warrant on the basis that it directed the production of information stored in Dublin, and that courts in the United States are not authorised to issue warrants for extraterritorial search and seizure.

US government position

The US government sought to rely on prior case law to argue that an entity lawfully obligated to produce information must do so regardless of the location of that information. The government produced academic literature demonstrating that this approach was consistent with the view that, in the context of digital information, 'a search occurs when information from or about the data are exposed to possible human observation, such as when it appears on a screen, rather than when it is copied by the hard drive or processed by the computer.'

Microsoft's position

Microsoft's position was that Federal Courts lack the authority to issue warrants for the search and seizure of property outside the territorial limits of the United States. This presumption against territorial

application is well enshrined in US law and provides that 'when a statute gives no clear indication of an extraterritorial application, it has none', to reflect the 'presumption that United States law governs domestically but does not rule the world' (Microsoft Corp. v. AT & T Corp., 550 U.S. 437, 454 (2007)). The principle is also a fundamental tenet of international law.

Judgment

Despite these principles, Judge Francis appears to have determined that the presumption that United States law does not rule the world is a rebuttable one. In order to rebut it, the Judge explored the structure of the US Stored Communications Act ('SCA'), its legislative history and, most tellingly of all, 'the practical consequences that would flow from adopting it.'

On Congressional intention, the judge extrapolated from various provisions on the US PATRIOT Act that it was the intention of Congress to facilitate access to data across State boundaries, although the examples the Judge cited relate only to data investigations within United States, not internationally.

The judgment then moved to 'practical considerations' of accepting Microsoft's territorial arguments, stating that 'if the territorial restrictions on conventional warrants applied to warrants issued under [the SCA], the burden on the government would be substantial, and law enforcement efforts would be seriously impeded.' Therefore the Judge concluded that, notwithstanding that the Microsoft position was 'not inconsistent with the statutory language...it is difficult to believe that, in light of the practical consequences that would follow, Congress intended to limit the reach of SCA Warrants to data stored in the United States'.

The fact that a process already exists for the service of search warrants internationally under a Mutual Legal Assistance Treaty ('MLAT') did not negate the need for the Judge to apply the SCA to Irish data. The Judge noted that the MLAT process tended to be slow, and it requires the cooperation of two governments. The Judge noted that (heaven forbid) a nation receiving a MLAT request from the US was likely to have discretion to decline the request for assistance. The Judge quoted examples of the MLATs between US and Canada, and between US and the UK.

[\(Continued from page 2\)](#)

Notably, Judge Francis IV did not feel that it was necessary to consider the terms of the MLAT between Ireland and the US.

Although clearly irrelevant to the facts at hand, the Judge went on to raise further domestic alarm by referring to Google having reportedly explored the possibility of establishing true 'offshore' server farms located at sea beyond the territorial jurisdiction of any nation.

Not prepared to accept such a panacea, the Judge refused to quash the search warrant, resulting in Microsoft being compelled to produce the relevant customer data from its Irish data centre.

Conclusion

The judgment is a perfect illustration of the tensions that exist between EU and US data protection law.

Post-Snowden, European distrust of US surveillance laws is at an all-time high. Further, the US court order ignores the reality that Microsoft Ireland is now indirectly faced with a warrant to transfer copious personal data relating to one of its customers to the US, notwithstanding the provisions of section 11 of the Data Protection Acts 1988 and 2003, which arguably restrict such transfers in the absence of a MLAT or similar Irish law process.

Microsoft appears to face the unpalatable choice of either breaching European data transfer laws or failing to comply with a US court order. The fact that the EU Data Retention Directive (which forms a basis for the retention of communications data for lawful access purposes) has itself been declared invalid by the Court of Justice of the EU (see page 17) further complicates matters.

In short, ISPs are currently caught in a complex legal web whereby EU law appears to require them to retain communications data under an invalid EU Directive, EU law prevents them from sending the data to the US but US court orders can compel them to transfer the data to the US notwith-

standing the provisions of Irish or other EU laws.

In short: a challenging world wide legal web.

Rob Corbet
Partner at Arthur Cox
rob.corbet@arthurcox.com
