
# *In Re Microsoft*: U.S. Law Enforcement Not Entitled to Email Stored in Ireland

By Denise E. Backhouse, M. James Daley, and Taylor M. Hoffman

Published on LinkedIn / August 28, 2016

On June 7-8, 2016, The Sedona Conference held its 8th Annual International Programme on Cross-Border Discovery & Data Protection Laws in Berlin, and one of the hot topics was the whether a warrant for the content of email messages, served on a U.S.-based email application provider, could reach emails stored on a server outside of the U.S. The panel in Berlin discussing the case, styled *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, featured the U.S. Magistrate Judge from the Southern District of New York who famously issued the warrant over Microsoft's objections. But at the time of the panel discussion, that judge's ruling, and the District Court's affirmance of that ruling, were being appealed to the Second Circuit, and the panelists could only speculate on what the outcome would be and what impact it might have on the free flow of data between the U.S. and Europe.

Five weeks after the panel, on July 14, the Second Circuit issued its much-anticipated ruling. The court found that the issuance of a warrant to obtain private

emails stored on a server in Dublin, Ireland, constituted an impermissible extraterritorial application of the Stored Communications Act, 18 U.S. Code §§ 2701 et seq. (SCA). The case attracted significant international attention, including amicus briefing from Ireland and from Jan Philipp Albrecht, a German member of the European Parliament. While the ruling effectively defuses an explosive issue at a tense time in EU/U.S. data protection relations, the many practical implications raised concerning cross-border government investigations and underlying problems with the outdated SCA remain to be resolved.

The case concerned a warrant requested by U.S. law enforcement authorities, ordering U.S.-based Microsoft to disclose all email from a certain individual's account, in connection with an ongoing drug investigation. Microsoft disclosed certain non-content account data stored in the U.S., but declined to produce the emails themselves, which were stored only in Ireland, the data center closest to the country indicated on the account holder's registration. Instead, Microsoft moved to quash the warrant as it applied to the email content, on the ground that it was an impermissible extraterritorial search and seizure.

Denying Microsoft's motion, the District Court held that it was empowered to order the disclosure in part because of the unique "hybrid: part search warrant and part subpoena" structure of a warrant issued under SCA section 2703(a). Viewing the SCA authorization as more like a subpoena commanding a person to act, rather than a traditional warrant authorizing the seizure of property, the principles of extraterritoriality did not apply and SCA warrants may require "the recipient to produce information in its possession, custody, or control regardless of the location of that information." (emphasis added). The District Court also considered the practical implications of an alternative holding, reasoning that, otherwise, anyone seeking to avoid U.S. jurisdiction over their email could simply give a false country code in their account registration. Moreover, the cumbersome Mutual Legal Assistance Treaty (MLAT) process that would apply if SCA warrants were treated as traditional warrants would slow investigations and be limited to MLAT signatory countries.

Reversing the District Court, the Circuit Court relied on the presumption against the extraterritorial application of statutes as stated by the U.S. Supreme Court in *Morrison v. National Australian Bank Ltd.*, 561 U.S. 247 (2010) and the recent *RJR Nabisco, Inc. v. European Community*, 579 U.S. ___, 2016 WL 3369423 (June 20, 2016). The SCA does not explicitly address extra-U.S. application;

implicitly, the term "warrant" and invocation of criminal procedure rules suggest that the SCA was intended to apply domestically. In their Majority Opinion, Circuit Judge Susan L. Carney and District Judge Victor A. Bolden (D. Conn.) went further. Applying Morrison's second-stage "focus" test, they found that "the SCA's focus lies primarily on the need to protect users' privacy interests[.]" Rejecting the Government's argument that the SCA primarily concerns not storage but disclosure (an act that would occur in the U.S.), the Majority held that here, the "focus" conduct is the invasion of privacy that would occur when the protected account content is accessed -- in Dublin, Ireland. Thus, the warrant was an unlawful extraterritorial extension of the SCA and the District Court's practical concerns could not prevail. The Majority noted that this outcome serves the interests of comity that govern cross-border criminal investigations, as reflected in the MLAT process.

In his separate, concurring opinion, Circuit Judge Gerard E. Lynch agreed that, based on the record, the Majority correctly applied default statutory construction rules to reach the right result, but found the case closer, and the Government's position stronger, than the Majority allowed. In Judge Lynch's view, Microsoft's privacy arguments were "a red herring" and the dispute was "not about privacy but the international reach of American law." Citing Professor Orin Kerr's critiques of the SCA, Judge Lynch urged Congress to move forward with revising the "badly outdated" Act to account for new technologies and global data management practices. "[M]ere location abroad" should not control and a more complex balancing of conflicting policy goals was required than the simplistic single "focus" test. It is Congress's job "to strike a balance between privacy and the needs of law enforcement."

The Second Circuit's ruling may incidentally help EU/U.S. data transfer mechanisms, including model contract clauses and the Privacy Shield program, to survive scrutiny against doubts that the U.S. can guarantee the privacy of European data subjects. In an ongoing action brought by Austrian data protection advocate Max Schrems against another U.S.-based service provider, Facebook, the U.S. government will submit an amicus brief to the Irish High Court (*DPC v. Facebook Ireland Ltd. and Schrems*, Record Number 2016 No 4809P). Whether European courts will now be persuaded that U.S authorities will provide European data subjects an equivalent level of data privacy protection that they enjoy under EU law, thus allowing data to flow freely under Privacy Shield, model contract clauses, or binding corporate rules, remains to be seen.

**Denise E. Backhouse, Esq.**, CIPP/E, is Shareholder and eDiscovery Counsel in the New York City office of Littler Mendelson, P.C. Denise is a member of the Steering Committee of The Sedona Conference Working Group 6 and Co-Editor-in-Chief of The Sedona Conference *International Investigations Principles* (forthcoming fall 2016).

**M. James Daley, Esq.**, CIPP/US & EU, is Senior Counsel for Global Data Privacy & Security, Information Governance and eDiscovery, based in the Chicago office of Seyfarth Shaw LLP. Jim is former Co-Chair of The Sedona Conference Working Group 6, Editor-in-Chief of The Sedona Conference *International Framework for Analysis of Cross-Border Discovery Conflicts* and Senior Editor of The Sedona Conference *International Litigation Principles*.

**Taylor M. Hoffman, Esq.**, is global head of eDiscovery at Swiss Re, based in Armonk, NY. Taylor is a member of Steering Committee of The Sedona Conference Working Group 6, and a Contributing Editor to The Sedona Conference *Practical In-House Approaches for Cross-Border Discovery and Data Protection*.