HOGE · FENTON

DOES MICROSOFT'S LATEST COURT VICTORY PAVE THE WAY FOR SECURING PRIVACY FOR CONSUMERS?

On July 14, 2016, the U. S. Court of Appeals for the Second Circuit significantly limited the federal government's reach for personal data stored by U.S.-based companies abroad in Microsoft Corp v. United States. This latest ruling involved a search warrant for the contents of a customer e-mail account @MSN.com that Microsoft maintains in Dublin, Ireland, which was allegedly being used for drug trafficking. The court concluded that the federal Stored Communications Act, 18 U.S.C. § 2703, does not authorize search warrants for the seizure of email content stored exclusively on foreign servers—even when those servers abroad are "owned, maintained, controlled, or operated by" U.S.-based electronic service providers.

The battle against the government over privacy rights is not new to Microsoft and other online service providers throughout the country, who are undoubtedly celebrating Microsoft's victory because they, too, have customer account data stored abroad, particularly in countries that view the privacy in personal information as a fundamental human right.

Most of us have personal and company email accounts through Microsoft, Yahoo! and other electronic communication services. You should know that these companies receive search warrants seeking email content and other private user information for criminal investigations. These warrants are often accompanied by a confidentiality or "gag" order, prohibiting the electronic communications services companies from notifying their users of the government warrant. These companies must comply with valid search warrants or face charges of contempt. Now, thanks to Microsoft taking the heat of a civil contempt order, other electronic communications service providers have a legal basis to refuse to comply with such requests when the data is maintained outside of the U.S. At least for now. The government can still appeal the matter to the U.S. Supreme Court. Moreover, while the Court rejected the government's argument that the warrant issued to Microsoft was akin to a subpoena, it remains to be seen if the Court would agree that a subpoena for basic subscriber information (e.g., IP addresses) would require a recipient to produce such information to the government, no matter where it is located, so long as the information is subject to the recipient's custody or control.

Stephanie O. Sparks - Chair - Privacy & Data Security and IP

Stephanie O. Sparks is a shareholder of, and chairs the firm's Privacy & Data Security and Intellectual Property teams. She counsels companies on privacy laws and helps them create and implement administrative, technical, and physical safeguards for data security.

Stephanie also conducts onsite data security and compliance assessments; provides privacy and data security awareness training; prepares record management policies, record retention/destruction schedules, and data breach incident response plans; negotiates business associate agreements mandated by HIPAA, and other agreements involving privacy and data protection, hosting, migration and transfer.

Contact Stephanie at 408.947.2431 or **stephanie.sparks@hogefenton.com**

Citation: Microsoft Corp. v. United States, Docket No. 14-2985 (2nd Cir. filed July 14, 2016)

Related Attorneys

- Stephanie O. Sparks