Title
Microsoft, Ireland and a Level Playing Field for U.S. Cloud Companies

Author
Schwartz, Paul M

Publication Date
2016-08-01

Peer reviewed

Bloomberg BNA

Privacy and Security Law Report®

Microsoft v. United States

After the recent Microsoft v. United States decision, the law faces the task of clarifying questions about the international reach of a variety of a legal authorities and processes. In so doing, it should maintain a level playing field for U.S. cloud companies who store their data extra-territorially. There is no policy reason to set a heavier compliance burden on U.S. companies in meeting these requests, the author writes.

Microsoft, Ireland and a Level Playing Field for U.S. Cloud Companies

BY PAUL M. SCHWARTZ

In the recent ''Microsoft Ireland'' decision, the Second Circuit clarified a critical issue regarding the reach of U.S. search warrants. *Microsoft Corp. v. United States (In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp.)*, No. 14-2985, 2016 BL 225943 (2d Cir. July 14, 2016) (15 PVLR 1465, 7/18/16). This decision is important to U.S. tech companies because of their growing reliance on and profits from the Cloud. At the same time, this opinion did not resolve important questions about how courts should determine where contested information retrieval takes place in an age of interconnected information technology (IT). The law now faces the task of clarifying questions about the international reach of a variety of a legal authorities and processes. In so doing, it should maintain a level playing field for U.S. cloud companies who store their data extra-territorially.

Paul M. Schwartz is professor of law at the University of California, Berkeley School of Law and director of the Berkeley Center for Law & Technology.

Microsoft Ireland

In this case, *Microsoft v. United States*, the U.S. Court of Appeals for the Second Circuit decided that a warrant issued pursuant to the Stored Communications Act (SCA) of 1986 did not require Microsoft to turn over material from a data center located outside of the U.S. Pursuant to a SCA warrant, the government had sought all information associated with an e-mail account at Microsoft's free online service, ''msn.com,'' regardless of where in the world it was stored. In response, Microsoft attorneys provided the government with data stored in the U.S., but drew the line at surrendering information located in its Dublin, Ireland data center.

The Second Circuit reached its verdict on a simple statutory basis. Its holding: ''Neither explicitly nor implicitly does the statute envision the application of its warrant provisions overseas.'' *Id.* at 3. Microsoft was not obligated by the SCA to give the government information from extra-territorial data centers because Congress in enacting this statute had not intended to give a global reach to such warrants.

Look to the Cloud

Cloud services are already a significant source of profits and an essential source of future growth for U.S. tech companies. Gartner Inc. estimates that the worldwide public cloud market will grow 16 percent this year and reach $204 billion by the end of 2016. *Gartner Says*

 ISSN 1538-3423

Worldwide Public Cloud Services Market Is Forecast to Reach $204 Billion in 2016, Gartner (Jan. 25, 2016). U.S. tech giants have invested heavily in the Cloud and already reaping significant rewards from it. Companies such as Alphabet's Inc.'s Google, IBM Corp., Microsoft Corp. and Salesforce.com Inc., offer different kinds of cloud-based services and products. For all these companies, however, earning and maintaining customer trust is key.

These tech companies now face a potentially existential threat to their global cloud businesses depending on how American law regulates the access of public authorities and private parties to their extra-territorial data. In particular, post-Snowden, European companies can be skittish about sharing data with U.S. companies. European customers worry that data storage with American companies will bring them under a legal regime that provides broader third-party access to personal information than European Union law. *See* Elizabeth Dwoskin, *EU Data-Privacy Law Raises Daunting Prospects for U.S. Companies*, Wall Street J. (Dec. 16, 2015).

Gartner Inc. estimates that the worldwide public cloud market will grow 16 percent this year and reach $204 billion by the end of 2016.

The Market Responds

U.S. tech companies are responding to these European concerns. These enterprises have spent millions of dollars building data centers throughout Europe and are offering a variety of EU-only data storage options. Jeremy Kahn, *Amazon's Pitch to Europe: Your Data is Safe From American Spies*, Bloomberg (Jan. 6, 2016). These companies are also taking other steps to avoid extra-territorial use of American law.

Consider the cloud market in Germany, the fourth-largest economic power in the world and the country with the largest gross domestic product in the EU. Microsoft has developed an innovative ''data trustee'' approach for the German market. *Microsoft Announces Plan to Offer Cloud Services from German Datacenters*, Microsoft News Centre Europe (Nov. 11, 2015). First, it opened data centers in Frankfurt and Magdeburg and offered business clients the option of storing data exclusively in these German centers. Second, it partnered with Deutsche Telekom's independent subsidiary T-Systems, which will act as data trustee for information in these centers. While Microsoft operates the data centers, T-System controls access to all stored information. Through a web of contracts and trusts, Microsoft limits its access to data on the German servers and assigns T-Systems exclusive legal authority to release information stored on them. *Id.*

Other companies are exploring the use of encryption in their EU data centers. In this model, customers are given keys to their information and have sole ability to de-crypt stored data. See Larry Greenemeier, *Why the FBI Wants ''Special Access'' to Your Smartphone*, Scientific American (Jul. 9, 2015), (noting that Apple ''allows its customers to have sole possession of the decryption key for gadgets running iOS 8''). This approach is analogous to the San Bernardino iPhone case where Apple Inc. argued that it lacked the ability, at least not without considerable additional effort, to unlock information stored on the phone seized by U.S. authorities. *Matter of Search of an Apple iPhone Seized During Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, No. ED 15-0451M, 2016 BL 48534 (C.D. Cal. Feb. 16, 2016).

Microsoft Ireland: Revisited

We can now understand the meaning of the Microsoft Ireland decision. It ends the ability of the U.S. government to leverage SCA's warrant authority to make global data requests. Such demands must now be made pursuant to the process for Mutual Legal Assistance Treaties (MLAT's). *Mutual Legal Assistance Treaties*, Access (last visited July 19, 2016). As a result, U.S. tech companies now exist on a level-playing field with non-U.S. companies. Requests from EU authorities for data in cloud centers in the U.S. are made pursuant to the MLAT process; requests from U.S. authorities for similar data in the EU are made in the same fashion.

The Second Circuit reached this result through a close reading of the SCA. First, the court found that Congress, in enacting this law in 1986, did not address the issue at stake in this case. Not surprisingly, Congress failed to anticipate the age of interconnected global servers and the rise of Cloud services. As the concurrence in this case by Judge Gerald Lynch stated: ''The now-familiar idea of 'cloud storage' of personal electronic data by multinational companies was hardly foreseeable to Congress in 1986, and the related prospects for diplomatic strife were surely not on the congressional radar when the Act was adopted.'' *Microsoft Corp.*, 2016 BL 225943 at *30. Second, the Second Circuit gave weight to the general rule presuming domestic effect for statutes. *Id.* at *26. Given the lack of evidence of a Congressional intent to create an extraterritorial application for SCA warrants, the court decided that Microsoft would win its legal battle against global use of these authorities.

The Microsoft Ireland decision ends the ability of the U.S. government to leverage the Stored Communications Act's warrant authority to make global data requests.

By limiting the reach of SCA warrants, the Microsoft Ireland opinion creates pressure for needed action to update America's law regarding electronic privacy. A broad coalition of civil liberty organizations and U.S. tech companies support reform of the Electronic Communications Privacy Act, of which the SCA forms a part. *See, e.g.*, Digital Due Process, ECPA Reform Why Now? (last visited Jul. 20, 2016); ACLU, *Modernizing the Electronic Communications Privacy Act*, ACLU (last visited Jul. 19, 2016). A reform proposal, the International Communications Privacy Act, has been introduced in the Senate; among its provisions, this bill

  PVLR ISSN 1538-3423

would reform the MLAT process by bringing greater transparency and accountability to it. The International Communications Privacy Act, S.2986, 114th Congress (2016). For media coverage, *see, e.g.*, Grant Gross, *Senators want warrant protections for US email stored overseas*, PCWorld (May 26, 2016).

Where Does the Activity Take Place?

Microsoft Ireland answered one aspect of the location question by limiting extra-territorial use of SCA warrants. The open question is how U.S. courts should assess the location of cloud computing activity in other legal contexts. Beyond the SCA, a variety of other U.S. laws permit a public or private party to use legal process to demand that another entity provide it with data located outside of the country. A range of warrants, subpoenas, administrative orders, judicial orders, and discovery mechanism allow U.S. courts to order a party to retrieve such information located outside the U.S. *Matter of Search of an Apple iPhone Seized During Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, No. ED 15-0451M, 2016 BL 48534 (C.D. Cal. Feb. 16, 2016).

The issue of how the law should evaluate the locus of data retrieval in the Cloud will only become more important.

But how does one determine the location of information that is stored in the Cloud? In reaching its verdict in Microsoft Ireland, the Second Circuit had to decide where the contested information retrieval would take place. For the magistrate judge and the District Court alike, the search warrant merely placed an obligation on Microsoft in the United States. *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466, 467-68 (S.D.N.Y. 2014). For these judicial officials, it was salient that Microsoft could use a database management program from the U.S. to collect account data stored on its servers globally. *Id.* at 468. Like Microsoft's Headquarters in Redmond, the database management program was located in the U.S. Hence, the magistrate judge and district court thought a SCA warrant would suffice to order the company to deliver records to the government, no matter where the documents were located, as long as they were subject to Microsoft's custody or control. *Id.* at 476.

The Second Court disagreed with this approach. In its view, the execution of the government warrant would take place outside of the U.S. Essential to the analysis of that court was the location in Dublin, Ireland of the sought-after data. Its judgment was that the ''invasion of the customer's privacy takes place . . . where the customer's protected content is accessed—here, where it is seized by Microsoft, acting as an agent of the government.'' *Microsoft Corp.*, 2016 BL 225943 at *20. The Second Circuit explained that the magistrate judge below had failed to give adequate weight to the storage of the data in Dublin, the necessity of Microsoft interacting with the Dublin datacenter ''in order to retrieve the information for the government's benefit,'' and the location of the data ''within the jurisdiction of a foreign sovereign.''

Recommendations

The issue of how the law should evaluate the locus of data retrieval in the Cloud will only become more important. The necessary analysis must be sensitive to the underlying legal context, including the nature of the underlying statutory authorization. Two recommendations can be made, however, that are appropriate for a broad range of such information request.

First, in deciding extra-territorial requests for personal information involving cloud providers, U.S. courts should be aware of distinctions among cloud computing types. Current classifications include infrastructure as a service, platform as a service, software as a service, information as a service, and business process as a service. For a concise introduction, see Nayan B. Ruparelia, Cloud Computer 25-41 (2016). For a discussion of some of the legal implications of these different cloud models, see Paul M. Schwartz, Information Privacy in the Cloud, 161 U. Pa. L. Rev. 1623 (2013). As shown by the Microsoft's data trustee model, moreover, these models are still evolving. The differences among cloud services matter because they bear on the issue of whether retrieval of the information will be made outside of the U.S. Variations in cloud models also matter because of their impact on how retrieval of information might violate a foreign sovereign's law, including data protection law.

Distinctions among approaches to cloud computing bear as well on how courts should decide whether the cloud company has control over the information. The applicable tests can use different language, but the basic idea is the same and relates to concepts of supervision and command. The underlying question for the Microsoft Ireland court was whether the documents subject to the issued warrant were ''subject to the recipient's custody or control.'' *Microsoft Corp.*, 2016 BL 225943 at *3. In civil litigation, Rule 34 of the Federal Rules of Civil Procedure asks whether sought-after information is under the ''custody, possession, or control'' of a party. Fed. R. Civ. P. 34. The Microsoft Germany example is also illustrative here. Depending on the specific kind of service, the information may not be subject to a cloud company's control.

It would be a significant error to establish different rules for international data requests based on the home country of the cloud service provider.

Second, the law should clarify questions about the international reach of a variety of legal authorities and processes. Here, there is a need to balance a variety of policy goals, including, depending on the context, furthering the battle against international terrorism, assisting in domestic litigation, protecting individual privacy, and respecting the law of foreign nations. But there is

another policy goal, one little acknowledged, that squarely belongs in this mix: U.S. policymakers should keep a level playing field level for U.S. tech companies. Microsoft Ireland reaches this result: U.S. and EU law enforcement requests for stored data in different countries will now go through the same MLAT-process. Note, however, a press report that the Obama administration is engaged in international negotiations that might change this current equilibrium around the MLAT process. Devlin Barrett & Jay Greene, U.S. to Allow Foreigners to Serve Warrants on U.S. Internet Firms, Wall St. J. (July 15, 2016).

It would be a significant error to establish different rules for international data requests based on the home country of the cloud service provider. Such a possibility is mentioned as a hypothetical by Judge Lynch near the end of his concurrence in *U.S. v. Microsoft*. For Judge Lynch, Congress, in finding the ''ideal balance'' in an amended SCA, must do more than defer to ''the mere location abroad of the server on which the service provider has chosen to store communications.''*Microsoft Corp.*, 2016 BL 225943 at *31. In listing a range of potential approaches and noting that the absence of any ''all-or-nothing choice,'' Judge Lynch observes, ''[Congress] is free to decide, for example, to set different rules for access to communications stored abroad depending on the nationality of the subscriber or of *the corporate service provider*'' (emphasis supplied). *Id.*

Here is a road that should not be taken. The law should not demand more of domestic companies than non-U.S. companies in regulating requests for information in extra-territorial clouds. There is no policy reason to set a heavier compliance burden on U.S. companies in meeting these requests. Moreover, today's market for IT is an international one and different legal standards for domestic and non-domestic companies would simply encourage the use of foreign services. Customers would ''route around'' U.S. regulation by storing their information abroad with the competitors of U.S. tech companies. The playing field in cloud computing services should be kept level.

  PVLR ISSN 1538-3423