BerkeleyLaw
UNIVERSITY OF CALIFORNIA
Berkeley Center for Law, Business and the Economy

University of California, Berkeley
School of Law
2850 Telegraph Ave, Suite 500
Berkeley, CA 94705-7220

Ph: 510.642.0532 – Fax: 510.643.7095
E-mail: BCLBE@law.berkeley.edu
http://www.law.berkeley.edu/bclbe.htm

Securing the Cloud: Microsoft's Battle with the Department of Justice

By Jenna Al-Huneidi, J.D. Candidate 2017 | October 26, 2015

Reliance on cloud storage has become an integral, and often overlooked, aspect of the daily activities of individuals and businesses throughout the world. Information stored in the "cloud" such as emails, photos, contact lists, and documents are actually stored in data centers located in many different countries. The information stored by a user is located in the data center closest to the location in which the individual or business registered their account. The purpose of these worldwide datacenters is to improve the efficiency and security of obtaining, accessing, and distributing such information. For example, Microsoft stores European users' cloud data in its Irish data center.

An ongoing battle between Microsoft and the Department of Justice has raised many concerns among a number of tech companies that reap significant revenue from cloud computing throughout the global community. Microsoft is in the midst of an appeal from a New York Magistrate decision, adopted in full by the District Court, to uphold a warrant, compelling Microsoft to seize the emails, photos, and contacts of account data stored in Ireland and turn them over to the DoJ for a criminal investigation. On appeal to the Second Circuit, the government argues that it has the right to demand the information stored abroad by any US corporation regardless of jurisdictional issues, conflicts of laws problems, and international treaties to the contrary.

The case carries important implications regarding the reach of the US government's access to data outside of its territories. The warrant stems from authority granted under the Electronic Communications Privacy Act (ECPA), which allows production of the requested documents stored within the US, but is silent as to its extraterritorial application. Under the ECPA to obtain the breadth of information sought, the government was required to issue a warrant rather than a subpoena. As a result, the government is subject to heightened procedural obstacles of obtaining a warrant, such as territorial limitations subjecting the warrant's application strictly to U.S. jurisdiction.

The Magistrate Judge declared that a warrant under the ECPA is actually a hybrid of both a subpoena and a warrant, thus relieving the government of the substantive limitations of a warrant (i.e. it extends to the physical reach of data within Microsoft's control). It is important to note that the government could compel disclosure from Ireland through the Mutual Legal Assistance Treaty (MLAT). However, the Magistrate judge reasoned that the more burdensome, slow, and complex process of retrieving the information through MLAT made this option less feasible.

Microsoft argues that such a ruling equally implicates our ability to protect data stored within the US from the reach of foreign nations, which have increasingly proposed and enacted legislation to combat intrusion into stored data after the Snowden NSA leaks, which have also spurred a wide distrust for cloud storage among businesses and individuals. Furthermore, it argues that if the US refuses to comply with MLAT, other nations will likewise refuse compliance, thereby

BerkeleyLaw
UNIVERSITY OF CALIFORNIA
Berkeley Center for Law, Business and the Economy

University of California, Berkeley
School of Law
2850 Telegraph Ave, Suite 500
Berkeley, CA 94705-7220

Ph: 510.642.0532 – Fax: 510.643.7095
E-mail: BCLBE@law.berkeley.edu
http://www.law.berkeley.edu/bclbe.htm

increasing the security threat to information stored within the US, and also diminishing our sovereign relations.

Even more, such a decision would pose significant economic, criminal, and security concerns for tech companies with data centers abroad. Due to increasing international legislation, many nations have imposed laws in which corporate officials are liable for the actions of a corporation that violates foreign law. As Apple argued in its amicus brief, conflicting foreign law regarding data privacy, such as that requested of Microsoft, may subject corporate officials to criminal and civil sanctions. Additionally, such a decision would discourage foreign customers from utilizing the services of these companies because the security of their private information would be at risk. Thus, tasking tech corporations with law enforcement responsibilities, that may extend beyond the terms of service agreed upon by users will severely affect their ability to compete on a global market.

These larger economic implications clearly pose concerns throughout the tech industry, which is forecast to generate approximately $98.6 billion in revenue in 2015. This is further evidenced by the large support of the amici from tech giants such as Apple, Verizon, and Amazon, as well as organizations such as the U.S. Chamber of Commerce, and a number of news media organizations. If the Second Circuit adopts the Magistrate position, we will surely see a much-heightened level of encryption from these tech giants requiring the government to subpoena the user, who holds the key to the information, directly rather than the company.