By David White

Whose Laws Govern That Slippery Data?

Storage in the cloud has complicated the question for companies and courts

The issue of jurisdiction over data stored in cloud-hosted environments has been a hot topic lately. In early June, Apple, Microsoft, Amazon, Cisco and several other technology giants filed amicus briefs in support of Google's move to overturn a federal court order requiring it to produce information stored on servers outside the United States in response to a search warrant. In their amicus briefs, each company argues that reaching into foreign territory for data isn't allowed under federal law, while the government retorts that data in the control of U.S. companies is subject to its search and seizure powers under the Stored Communications Act (SCA).

The SCA itself is silent as to whether it applies outside of the U.S. In the absence of clear statutory guidance, courts tend to assume that the intent of the lawmakers was not to extend jurisdiction outside the U.S. Yet, given the nature of cloud storage, the courts are having significant trouble shoehorning new technologies into longstanding legal frameworks.

Thus far, only the U.S. Court of Appeals for the Second Circuit has addressed the extraterritorial application of the SCA head on. Last year in *Microsoft Corp. v. United States*, the appeals court held that the statute's focus was on privacy, rejected the government argument that it was a permissible disclosure and ruled that Microsoft did not have to produce data stored on servers located in Ireland. The court reasoned that doing so would be an invasion of the Irish customers' privacy and an improper extraterritorial application of the law.

The Google court has distinguished the present case from *Microsoft* in that the data requested by the subpoena is not "tethered" to any particular user location. Therefore, the court decided, the disclosure of information that is stored abroad but processed and retrieved from the company's U.S. headquarters is a domestic application of the SCA, and is not overreaching.

On its face, this ruling seems to be a split from *Microsoft*, even though the two are actually consistent. Hosting emails in a foreign data center is not akin to sheltering funds in an offshore bank account. Most users have little to no control over where their information is physically stored. This precept is often the main selling point of cloud storage. Powerful algorithms determine the most efficient and optimal storage location, and often fragment the data to achieve this.

Much of the legal discourse on this topic seems to focus on the physical storage locations of the data and on the producing party's ability to access and control the data from within the U.S. Yet, these two concepts are actually irrelevant constructs that carry over from our notions of a physical or analog world. What was truly central to the *Microsoft* case was that the data sought was sent and received by a user most likely located in Ireland and who had certain expectations of privacy that were protected by the sovereign power of his state, and that they were not U.S. emails subject to the boundaries of the SCA. A domestic email sender or recipient would not typically have a reasonable expectation that their electronic communications will be free from legitimate U.S. government search simply because a technology service provider moved this data to an offshore server, any more than a foreign actor would expect to lose their rights to privacy simply because data was (often without the actor's knowledge) moved to a U.S. server.

The law, which was written at a time when the storage of digital information was more akin to a single physical object, is having trouble wrapping itself around this digital transformation when dealing with ones and zeros that can manifest themselves in multiple locations all at the same time. It also is in tension with most foreign data protection and privacy laws, which often seek to extend the protection of citizens' privacy interests in data stored abroad.

> ***The law, which was written at a time when the storage of digital information was more akin to a single physical object, is having trouble keeping up with the fluidity with which information now flows.***

Rather than focusing on the location of the data, or the ability to access it, the primary focus should be on the bubbles of privacy rights that surround and attach themselves to the data regardless of its physical location. In the Google case, the disputed warrant relates to the further investigation of persons who have already been indicted in the district, and there is no indication that the relevant email accounts were used by persons outside the United States. These are key facts that should not be overlooked.

The court, while not directly acknowledging the attachment of privacy rights, seems at times to allude to them. For example, it stated that "[e]lectronically transferring data from a server in a foreign country to Google's data center in California does not amount to a 'seizure' because there is no meaningful interference with the account holder's possessory interest in the user data." Contrary to the position taken in the amicus briefs filed in support of Google, the court was not holding that the data should be disclosed just because remote access was possible, but rather because remote access did not violate the privacy rights and expectations of the data owners, as it would have in the *Microsoft* matter.

Given the fluid nature of electronic data, and the simple fact that companies now move information around the globe faster than the blink of an eye, it is no wonder that the courts are struggling to resolve these issues. This is particularly true given the need to apply precedent that originates from a world with very different physical boundaries.

How courts will apply established legal precedent to cloud considerations in future cases is anyone's guess. But what is certain is that these issues will be an unavoidable challenge for judges, given the growing prominence of cloud services. Until new legal constructs are fleshed out, we are bound to continue to see these cases coming up over and over again.

David White is a director at AlixPartners LLP, where he advises clients on information governance, information security and electronic discovery. He can be reached at dwhite@alixpartners.com.