Part I: Background

During the era when the Sony Walkman birthed the personal audio revolution, Nintendo Entertainment Systems appeared on American shores, and Gordon Gekko made wireless phone calls on his chunky mobile phone, the 99th United States Congress passed the Stored Communications Act (SCA). Enacted in 1986, the SCA governs U.S. authority to compel disclosure of electronic communications or data stored with a service provider.

Fast forward two decades, the gap between advancements in technology and legislation became readily apparent when a federal appeals court, the United States Second Circuit, decided on July 14, 2016, that U.S. law enforcement could not compel a U.S. Cloud Service Provider (CSP) to disclose Content Information (e.g., emails) stored abroad with a U.S. search warrant.\[1\]

The SCA was passed decades before the modern internet came into existence. Today, CSPs often store email content all over the world, moving the location of the data frequently and breaking emails into “shards” so that different portions of a single email may be stored in multiple countries.\[2\]
In *Microsoft Corp. v. United States*, Microsoft contested its obligation to disclose Content Information stored exclusively in its Dublin, Ireland datacenter, in response to a government issued search warrant under the SCA.\[3\] The Second Circuit held that U.S. courts do not have the authority to issue and enforce a search warrant against a U.S.-based CSP for Content Information stored exclusively in data storage facilities outside the U.S.\[4\] In practice, this decision blocks U.S. government access to Content Information stored outside the U.S. even when the Content Information’s owner is a U.S. citizen, living in the U.S. and alleged to have committed a crime in the U.S. against a U.S. victim.\[5\]

However, U.S. law enforcement may obtain information from certain foreign entities through a treaty or bilateral agreement with another country. In the U.S., although law enforcement cannot use a search warrant to obtain Content Information stored outside the U.S., law enforcement can use the Mutual Legal Assistance Treaties (MLAT) process to request evidence from another country under such a treaty. To the extent that the U.S. government has a treaty or agreement, the process can be slow and uncertain, often taking months or even years to generate results.\[6\]

On February 27, 2018, the U.S. Supreme Court heard oral arguments in *United States v. Microsoft Corp.* Justices Ruth Bader Ginsburg, Sonia Sotomayor, and Stephen Breyer hinted that Congress, and not the Court, might best be situated to reconcile this gap between technology and law. Justice Ginsburg questioned the government’s lawyer, Deputy Solicitor General Michael Dreeben, as to why the court should even decide this case, asserting that it might be better left to Congress now that Congress is considering a bill on this very issue. Justice Ginsburg noted that the SCA is an old law that is not ready for new technology, since no one even knew of the cloud in 1986. Justice Sotomayor was not far behind noting that Congress was better suited to address foreign conflicts and that Congress has now taken up a bill that has bipartisan support. Justice Breyer opined that it might be better for Congress to adapt the statute to new technology as opposed to asking the court to do so.

On February 6, 2018, as were referenced by the Justices, Senator Orrin Hatch and Representative Doug Collins introduced the Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018 (H.R. 4943 and S. 2383) in response to the legislative gap readily apparent in *Microsoft Corp. v. United States*.

The CLOUD Act (H.R. 4943 and S. 2383) consists of two parts: Specifying that the SCA applies to data in the “possession, custody, or control” of providers, regardless of where the data is geographically located and authorizing executive agreements to allow foreign governments to request content directly from U.S.-based CSP.

The CLOUD Act has already received tough criticism, implicating a violation of the 4th Amendment. Stay tuned for the next post, analyzing both sides of the case for this new legislation’s attempt to bridge the gap between technology and the law.

\[1\] See Microsoft Corp. v. United States (In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197.
[2] DOJ Pet. for Cert. at p. 28

[3] Id. at 204

[4] Id. at 200

[5] DOJ Pet. for Cert. at p. 27


© Copyright 2020 Squire Patton Boggs (US) LLP

Source URL: https://www.natlawreview.com/article/cloud-act-bridging-gap-between-technology-and-law