

## The CLOUD Act and U.S. Law Safeguards for Enterprise Customers

A number of safeguards including those adopted as part of the process that led to the CLOUD Act limit the ability of U.S. law enforcement to seek information of enterprise customers. These safeguards are contained in a range of legislative and non-legislative binding instruments designed to help protect customer privacy rights.

- **The CLOUD Act Only Authorizes Limited Forms of Legal Process.** U.S. law enforcement uses the CLOUD Act to obtain digital content from technology providers in connection with *criminal* cases through a court-issued warrant on a showing of probable cause; the CLOUD Act does not provide the U.S. government with any new *national security* tools. Any request made under the CLOUD Act is subject to safeguards, including:
  - Warrant Requirement: U.S. law enforcement agencies use warrants to obtain content data. Warrants are subject to strict safeguards and may only be issued by a magistrate if a law enforcement officer makes a showing that there is probable cause to believe the information sought will contain evidence of a crime. Requiring a magistrate to issue the warrant ensures that a neutral and detached officer approves the requested search. In addition, the Fourth Amendment of the U.S. Constitution requires a warrant to describe with particularity the place to be searched, and the persons or things to be seized. This particularly requirement ensures the search will be carefully tailored to its justifications.
  - No Bulk Requests: The CLOUD Act does not authorize bulk requests by law enforcement. Instead, law enforcement officers use warrants to obtain content—and warrants are issued in particular cases to obtain specific types of data that are identified with particularity in the warrant itself, as described above.

---

### **About BSA**

BSA | The Software Alliance ([www.bsa.org](http://www.bsa.org)) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Akamai, Apple, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

- **Providers May Bring Comity Challenges to U.S. Legal Process:** When U.S. legal process seeks data overseas, technology providers can ask a court to set aside that process because it conflicts with a foreign country’s law. The CLOUD Act specifically preserves the ability of providers to bring such common law comity challenges. Indeed, the U.S. Department of Justice has recognized the availability of such challenges. In an argument before the Supreme Court, the Department of Justice said that when U.S. legal process conflicts with a foreign law “courts conduct a comity analysis.”<sup>1</sup> In a later brief to the Supreme Court, the Department of Justice said that the “CLOUD Act does not affect the availability or application of a common-law comity analysis.”<sup>2</sup>
- **The U.S. Department of Justice Has Committed to Serve Legal Process on Enterprise Customers Directly.** In December 2017, the U.S. Department of Justice issued guidance limiting the circumstances in which federal prosecutors should serve legal requests on technology companies for enterprise customer data.<sup>3</sup> **Specifically, the U.S. Department of Justice guidance provides that prosecutors “should seek data directly from the enterprise, rather than its cloud-storage provider, if doing so will not compromise the investigation”<sup>4</sup>.** This guidance recognizes that in many cases, the enterprise customer—and not the cloud provider—will be the appropriate entity to respond to legal process.
- **CLOUD Act Bilateral Agreements Will Provide Further Protections.** In addition to preserving the ability of providers to bring common law comity challenges, the CLOUD Act also creates a new statutory mechanism for providers to bring comity challenges when legal process conflicts with the law of a qualifying foreign country<sup>5</sup> that enters into a new CLOUD Act bilateral agreement. The CLOUD Act also ensures that providers can notify a qualifying foreign government of legal process seeking the content of its nationals or residents, when the foreign government has entered into a new CLOUD Act bilateral

---

<sup>1</sup> Transcript of Oral Argument at 27, *United States v. Microsoft Corp.*, No. 17-2 (2018), available at [https://www.supremecourt.gov/oral\\_arguments/argument\\_transcripts/2017/17-2\\_j4ek.pdf](https://www.supremecourt.gov/oral_arguments/argument_transcripts/2017/17-2_j4ek.pdf).

<sup>2</sup> Brief of Petitioner at 5, *United States v. Microsoft Corp.*, No. 17-2 (2018), available at [https://www.supremecourt.gov/DocketPDF/17/17-2/41851/20180330172237829\\_17-2motUnitedStates.pdf](https://www.supremecourt.gov/DocketPDF/17/17-2/41851/20180330172237829_17-2motUnitedStates.pdf).

<sup>3</sup> See Computer Crime and Intellectual Property Section, Criminal Division, U.S. Dep’t of Justice, Seeking Enterprise Customer Data Held by Cloud Service Providers, December 2017, available at <https://www.justice.gov/criminal-ccips/file/1017511/download>.

<sup>4</sup> A similar provision is contained in the proposed E-evidence regulation in Article 5(6) available at <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN>

<sup>5</sup> A qualifying foreign country under the CLOUD Act is a third country that has entered into bilateral agreements on Cross-Border Data Requests with the United States and that afford reciprocal rights to the United States.

agreement. This notification will enable the foreign government to engage in direct diplomatic discussion with the United States.

---

For further information, please contact:  
Thomas Boué, Director General, Policy – EMEA  
thomasb@bsa.org or +32.2.274.1315