Brussels, February 2019

The CLOUD Act and the European Union: Myths vs. Facts

The U.S. CLOUD Act both protects individual privacy and enables U.S. law enforcement to access data, regardless of where it is stored, pursuant to a court-issued warrant based on probable cause of a specific criminal act. Importantly, however, the CLOUD Act also empowers the United States government to enter into new bilateral agreements with other governments that would enable law enforcement agencies to access data across each other's borders to investigate and prosecute crimes, subject to an agreed-upon set of processes and controls negotiated between the two governments.

Inaccurate descriptions of the legislation have led to fears about its impact on the privacy of citizens of the European Union (EU). This white paper seeks to separate those myths from the facts about the CLOUD Act.

X MYTH: The CLOUD Act enables widespread access to EU citizens' data, effecting the return of US bulk surveillance.

✓FACT: The CLOUD Act does not authorize bulk surveillance, and only applies to court-authorized criminal investigations.

The CLOUD Act does not authorize bulk requests by law enforcement. Instead, law enforcement may only access digital content from service providers:

1. in connection with a criminal case;
2. after obtaining a warrant from a court based on **probable cause**; and
3. only the specific types of data that are identified with particularity in the warrant itself.

The CLOUD Act does not provide the US government with any new authority to obtain content – of either US, EU or other foreign citizens – on *national security* grounds. It also does not expand the scope of *who* or *what types of data* can be subject to court-issued warrants.

About BSA

BSA | The Software Alliance (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.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

X MYTH: The CLOUD Act fundamentally undermines EU citizens' privacy, violating the US-EU *Privacy Shield* agreement.

✓FACT: The CLOUD Act rests on strong privacy protections and would not encroach on EU citizens' privacy.

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. Warrants can be issued only where courts find that there is probable cause of a specific criminal act.

As a further protection, service providers can ask a court to set aside a warrant issued by a U.S. court in two circumstances.

- First, providers may seek to set aside a warrant based on conflicts with a foreign country's law, when that country has not entered into an international agreement authorized by the Act. The CLOUD Act specifically preserves the ability of service 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."[1] Similarly, in a 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."[2]

- Second, providers may seek to set aside a warrant issued by a U.S. court if: (1) the subscriber is not a U.S. person and (2) the disclosure sought would create a material risk of violating the laws of a qualifying government that has entered into a bilateral agreement of the type contemplated by the Act. This mechanism creates a specific way for providers to bring such challenges, and sets out a list of factors a court should take into account in assessing them, including the interest of the foreign government in prohibiting disclosure, the U.S. government's interest in the information, the location and nationality of the subscriber, and the likelihood of timely and effective access to the information through other means.

Further, with respect to the new international agreements, the CLOUD Act only authorizes the United States to enter agreements providing for access to citizens' data stored within another country with a national government that "affords robust

[1] 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.
[2] 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.

substantive and procedural protections for privacy and civil liberties." US law enforcement activities under such agreements are subject to judicial oversight, and the CLOUD Act authorizes service providers to notify the foreign government of the fact that U.S. law enforcement seeks the data of a national or resident of that country. Finally, the Act prohibits an Executive Agreement that includes a mandate that companies subject to a warrant be capable of decrypting data stored on their systems. Such privacy protections ensure that EU citizens' data is protected against unlawful or inappropriate disclosure to US law enforcement.

The European Commission concluded its second annual review on implementation of the Privacy Shield agreement in December 2018, nine months after the passage of the CLOUD Act. It found no evidence that the CLOUD Act undermined protections or commitments set forth in the Privacy Shield agreement. In fact, the Commission Staff Working Group supporting the review found that "the CLOUD Act subjects the conclusion of such executive agreements to a number of safeguards and requirements: the foreign domestic law and its implementation must provide sufficient substantive and procedural protections for privacy and civil liberties…orders must be limited to address serious crimes, comply with the foreign domestic law, be specifically targeted and be subject to independent review or oversight."[3]

X MYTH: The CLOUD Act is a one-way street, enabling the US to access EU citizens' data without reciprocal EU access of US data.

✓FACT: The CLOUD Act explicitly provides for bilateral agreements and makes provision for the sharing of US citizens' information with foreign authorities.

The CLOUD Act authorizes bilateral agreements between the US and other national governments to provide for mutual law enforcement access to data stored by service providers in the other country. Prior to bilateral agreements, the CLOUD Act provisions would apply similar to the current E-Evidence proposal from the European Commission, which authorizes EU-based law enforcement agencies to access content wherever it is stored, subject to a comity analysis similar to the analysis in the CLOUD Act and under US common law. In this process, service providers could bring common law comity challenges asserting a warrant conflicts with foreign law; courts would assess such claims by weighing a series of comity factors, including the importance of the information to the investigation, whether there are alternative means to obtain the information, and the extent to which compliance with the request would undermine important interests of the state where information is located.

X MYTH: The CLOUD Act allows law enforcement access through limited or secretive judicial process.

[3] "Commission Staff Working Document Accompanying the Report from the Commission to the European Parliament and the Council on the second annual review of the functioning of the EU-U.S. Privacy Shield," SWD (2018) 497, December 19, 2018. https://ec.europa.eu/info/sites/info/files/staff_working_document_-_second_annual_review.pdf.

✓**FACT: The CLOUD Act authorizes law enforcement access only through transparent, robust, publicly accountable judicial proceedings with strong oversight.** The CLOUD Act establishes a robust judicial process with several features ensuring transparency, accountability, and oversight:

- It allows for US access to digital content stored overseas only through court-issued warrants that articulate probable cause and specify particular information regarding the individuals and information targeted by the warrant.
- It provides service providers the opportunity to challenge warrants if they do not target US persons or if they would require service providers to take actions in violation of another nation's laws.
- It authorizes service providers to notify the government of a citizen whose data is being sought by US law enforcement.
- It ensures the application of authorities for judicial review to legal processes established under agreements covered by the Act.
- It creates mechanisms for sustained oversight of agreements by the US Congress.

X **MYTH: The CLOUD Act forces companies to turn EU citizens' data over to US law enforcement without recourse.**

✓**FACT: The CLOUD Act provides businesses a substantial basis to challenge court orders for the production of EU citizens' data.** When U.S. legal process seeks data overseas, service providers can ask a court to set aside that process because it conflicts with a foreign country's law, in two ways.

- First, the CLOUD Act specifically preserves the ability of service providers to bring common law comity challenges when the request conflicts with the law of a country that has not entered into a bilateral agreement of the type created by the CLOUD Act. The U.S. Department of Justice has recognized the availability of such challenges in previous court filings. The ability to bring these challenges provide businesses with strong recourse to protect the data of EU citizens.
- Second, a new statutory mechanism allows providers to seek to set aside a warrant issued by a U.S. court if: (1) the subscriber is not a US person and (2) the disclosure sought would create a material risk of violating the laws of a qualifying government that has entered into a new bilateral agreement of the type contemplated in the Act. This statutory mechanism creates a specific way for providers to bring such challenges, and sets out a list of comity factors the court is to take into account in assessing such challenges.

X **MYTH: In the area of Justice and Home Affairs, the Commission has entered into contracts with companies to design, develop, manage or maintain large-scale IT**

systems. The CLOUD Act will enable broad access to sensitive data stored in those systems about EU citizens.[4]

✓**FACT:** Under U.S. law, service providers cannot be issued a warrant for digital evidence absent specific, articulable grounds for probable cause of a criminal act within the jurisdiction of the United States. Suppliers of eu-LISA, the European Agency providing operational management of large-scale IT systems, are bound by the General Data Protection Regulation (GDPR), by confidentiality agreements, and by other relevant domestic laws, which may impose obligations for protecting sensitive information. If a US warrant issues for content that conflicts with these obligations, a court would apply a comity analysis to address that conflict Moreover, no direct eu-LISA suppliers are currently registered in the US, and only providers established in the EU may participate in EU tenders.

For further information, please contact:

Thomas Boué, Director General, Policy – EMEA

thomasb@bsa.org or +32.2.274.1315

[4] http://www.europarl.europa.eu/doceo/document/E-8-2018-003651_EN.html Question from Sophia in 't Veld, Member of the European Parliament, 2 July 2018, replied by Commissioner Vera Jourová on behalf of the European Commission on 25 October 2018.