



Author:

Martin Whitworth

November 2018

Don't Get Spooked by the CLOUD Act

The CLOUD Act

In March 2018, as part of a larger "omnibus" spending bill, the U.S. passed legislation designed to address how governments, courts, and law enforcement should request data kept outside of their national borders: the Clarifying Lawful Overseas Use of Data Act (CLOUD Act).

The CLOUD Act looks to establish reciprocal bilateral executive agreements that allow the U.S. government agencies to access data, relevant to a specific legal case, stored overseas in exchange for allowing foreign governments to access data stored in the U.S.

It also provides for the case where if no such bilateral executive agreement exists with a country or region, and the demand for data breaches local privacy laws, then service providers may be able to seek to quash the request from law enforcement.

This paper looks to clarify just how the CLOUD Act is, and isn't, going to impact cloud usage and cloud service providers (CSPs).

The Facts (vs Myths) of the CLOUD Act

There is more than enough fear, uncertainty, and doubt (FUD), confusion, and misunderstanding when it comes to the CLOUD Act — and this has generated claims or myths that need to be cleared up.

The CLOUD Act Does Not Provide Unfettered Access to Personal Data by Law Enforcement

Law enforcement may request content from service providers only if the subject has consented or with a warrant issued by a U.S. court in accordance with the CLOUD Act, or in conformity with an agreed bilateral executive agreement.

CSPs Can Help Protect Customers' Content

The CLOUD Act makes no provision to disclosing encryption keys, and CSPs may offer a variety of services aimed at improving the security of customer data.

Extraterritorial Access to Data Needs Bilateral Agreement

The CLOUD Act provides a new process for accessing extraterritorial data. It also provides a new framework for the U.S. to enter into bilateral agreements with other countries or regions regarding law enforcement requests for data. Where there is no bilateral agreement, requests for extraterritorial data will have to go through the process of pursuing mutual legal assistance treaties or MLATs (<https://www.mlat.info/>), which means little has changed in these cases.

There is more than enough FUD, confusion, and misunderstanding when it comes to the CLOUD Act.

The CLOUD Act does not ignore, supersede, or change another country's local laws.

The CLOUD Act Provides Reciprocal Access

The CLOUD Act is designed to allow reciprocal access to data between U.S. and bilateral agreement partners, but only through an agreed and approved legal process.

The CLOUD Act Does Not Take Precedence Over Existing Laws

The CLOUD Act does not ignore, supersede, or change another country's local laws. In fact, the CLOUD Act recognizes the right for service providers to challenge requests that conflict with another country's laws or national interests.

The CLOUD Act and CSPs

Further to the above myths, there are several more claims that are directed specifically at the CSP marketplace.

The CLOUD Act is Not Targeting CSPs

While it is true that global CSPs are the custodians of much of the data that U.S. law enforcement would conceivably seek access to under the CLOUD Act, they are not the only likely recipients of a warrant. All organizations operating from the U.S. that hold data outside of the U.S. are equally subject to this legislation.

The CLOUD Act Does Not Only Apply to CSPs

The CLOUD Act applies to all organizations operating from the U.S. that provide electronic communication services or remote computing services to their users (including email and cloud service providers) irrespective of whether services are provided in the U.S. or another country.

There is No Provision for Decryption

There is no provision within the CLOUD Act for the decryption of data that CSPs hold on behalf of their users or customers. The act is not a magic decoder ring that law enforcement can use to unencrypt data that is under the control of the end user. This is important: even if data encrypted by the CSP could be forced to be disclosed, data encrypted by the customer could not be decrypted by the CSP.

Local CSPs Are Creating Much of the FUD

The CLOUD Act does provide a new framework, but it does not suggest that either a local or foreign CSP should be a preferable solution. Organizations must understand just what the stance and capabilities of any prospective CSP are — for example, can they provide customer-controlled encryption, do they offer configurable regional data stores, do they provide the services that best suits their business, etc.

What Does it Mean for CSPs?

CSPs can be a great resource to help organizations navigate the complexities of the CLOUD Act — particularly regarding the ways it affects their services. This will require CSPs to be very clear about services that they offer that can support the protection of customer data, such as data segmentation, encryption, and key

The potential for conflict between the CLOUD Act and GDPR consequently hinges on whether the U.S. and the EU, as a collective whole, can negotiate an executive agreement that satisfies both parties.

management. Finally, CSPs must work with their customers to clearly define responsibilities and potential reactions to approaches by law enforcement.

Do Regional CSPs Have to Comply With the CLOUD Act?

While regional (not U.S.-based) CSPs are not specifically within the scope of the CLOUD Act, they are likely to come into scope for law enforcement requests for data if executive agreements are negotiated. Additionally, they will still be expected to respond to requests made via MLATs and letters rogatory (<https://legal-dictionary.thefreedictionary.com/letters+rogatory>). When considering CSPs, do the appropriate due diligence and get a clear understanding of the art of the possible — then make your choices. Most importantly, don't panic and don't become a victim of FUD.

The CLOUD Act and GDPR

Minimal Conflict

There are a whole range of unfounded claims being made about possible conflicts between the CLOUD Act and the EU GDPR. In fact, there is only one area of potential issue and this lies around the subject of data transfers outside of the EU — and, specifically, a potential conflict between section 2713 of the CLOUD Act (<https://www.congress.gov/bill/115th-congress/senate-bill/2383/text>) and article 48 of GDPR (<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>).

A Resolution?

To resolve this, we need to look at two different scenarios:

- **If there is an executive agreement in place**, then any details of what is or isn't allowed will need to be hammered out by the two parties (the U.S. and a third-party country or region), and primacy of the executive agreement or the GDPR will be decided by the courts.
- **If there is no executive agreement in place**, then the handing over of any data to U.S. authorities will depend on the reaction to the CLOUD Act warrant by service providers operating from the U.S. and whether they seek to quash the warrant based on a conflict with local laws (i.e., GDPR).

The potential for conflict between the CLOUD Act and GDPR consequently hinges on whether the U.S. and the EU, as a collective whole, can negotiate an executive agreement that satisfies both parties. However, to be clear, only businesses that are hosting data or information that is related to a serious crime would be impacted. In fact, current European Commission activities are set to create an EU equivalent of the CLOUD Act — the so-called e-Evidence Regulation. With both the CLOUD Act and the e-Evidence Regulation in place, we could have the basis for a bilateral executive agreement between the U.S. and the EU that removes any conflict with GDPR or other local legislation.

The Ability to Quash is Very Limited

It should also be noted that the ability of a CSP to seek to quash a CLOUD Act warrant for access to a customer's or subscriber's information only applies if:

- The person/entity is not a U.S. citizen and does not reside in the U.S.
- The required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government

So, we will still have a possible conflict if a U.S. citizen, resident in the EU, is the subject of a CLOUD Act warrant.

What About Brexit?

The U.S. and the U.K. are already negotiating an executive agreement that will provide for the exchange of data for the protection of society, national security, and law enforcement. Details are not available at this time but are likely to reflect previous data exchange agreements that have existed between the two countries for intelligence and law enforcement. As the U.K. is to leave the EU in 2019, the GDPR will not directly apply, but the U.K. has already passed into law the U.K. Data Protection Act 2018 (which implements the EU's GDPR, while providing for certain permitted derogations, additions, and U.K.-specific provisions). These will all be addressed within the executive agreement.

Conclusion

The CLOUD Act is in place and is yet to be tested in the courts — but organizations still must carry on with their businesses. The key is to keep calm and to remember a few basic items:

- Only data that is relevant to protecting public safety and combating serious crime, including terrorism, is subject to the CLOUD Act.
- Your CSPs are your partners, so talk to them and understand what they can do and what their stance is with respect to approach by law enforcement.
- Encryption is your friend. Not only does encryption help mitigate concerns over rogue service provider admins or hacking attacks by malicious outsiders, but in the event that a service provider has to turn over data as part of a lawful request by U.S. or other government agency, that data is useless to them without the cooperation of the enterprise.
- Be informed about the CLOUD Act and other local legislation that could impact your business.
- Under the CLOUD Act, request to access to data is made either by a warrant issued by a U.S. court (which can be challenged if it conflicts with local laws) or via a bilateral executive agreement between the U.S. and a third-party country or region.
- In selecting a service provider, as always it is important to undertake appropriate due diligence to ascertain that your needs can be met, that you will be fully compliant, and your risks can be managed in line with current and evolving legislation.

The CLOUD Act is in place and is yet to be tested in the courts, but organizations still must carry on with their businesses.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Copyright and Restrictions:

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the Custom Solutions information line at 508-988-7610 or permissions@idc.com. Translation and/or localization of this document require an additional license from IDC. For more information on IDC visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Global Headquarters: 5 Speen Street Framingham, MA 01701
USA P.508.872.8200
F.508.935.4015 www.idc.com.

Copyright 2018 IDC.
Reproduction is forbidden unless authorized. All rights reserved.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.