US CLOUD Act

Overview, Consequences and Risks

Markus Mössner
May 04, 2023

Disclaimers

- I am not a lawyer or legal expert
- This presentation expresses my private opinion

What is the US CLOUD Act?

Stored Communication Act (SCA)*

- Voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party Internet service providers (ISPs). Enacted as Title II of the Electronic Communications Privacy Act of 1986 (ECPA).

Clarifying Lawful Overseas Use of Data (CLOUD) Act*

- The CLOUD Act was the result of a lawsuit in 2013 between the US Federal Bureau of Investigations (FBI) and Microsoft on a SCA request to hand out data stored outside the US. Microsoft successfully claimed that the SCA does not cover data *outside* the US.
- It amends the SCA to allow federal law enforcement to compel U.S.-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the U.S. **or on foreign soil**.
- It asserts that US data and communication companies must provide stored data for a customer or subscriber on **any** server they own and operate when requested by warrant, but provides mechanisms for the companies or the courts to reject or challenge these if they believe the request violates the privacy rights of the foreign country the data is stored in. It also provides an alternative and expedited route through "executive agreements"; the first and so far only such agreement was with the United Kingdom.

*) Source: Wikipedia

CLOUD Act vs. EU GDPR / CH (V)DSG

- The European Data Protection Supervisor sees the CLOUD act in competition with the cooperation agreement between the US and the EU. If the US needs data they can use the existing Mutual Legal Assistance in Criminal Matters Treaty (MLAT).
  - Data transfers to foreign countries by a company subject to GDPR are only allowed (e.g. if it has been legally requested to do so) if this corresponds to an international agreement of the EU. A company therefore is only allowed to transfer data to the US if the requirement is according to the terms in the MLAT. If the data transfer is only according to the CLOUD act, this would be in breach of GDPR Art. 48. Exceptions according to Art. 49 are tricky to say the least.*
  - Transparency of data transfers based on the CLOUD act are also an area of concern. People subject to such data transfers may not necessarily be informed which is in breach with Art. 8 of the EU Charta. Natural persons have no possibility to object to such data transfers, they have no access, information or deletion rights
- The situation in relation to the Swiss DSG / VDSG is similar to the EU GDPR.*

Conclusion
Data transfers from the EU or Switzerland based on the CLOUD act are only lawfully possible according to GDPR / DSG in few, very specific cases.

*) Source: Bericht zum US Cloud Act, Bundesamt für Justiz

US Options beyond the CLOUD Act

- Section 702, Foreign Intelligence Surveillance Act (FISA)*
  - Permits the Attorney General and the Director of National Intelligence to jointly authorize targeting of non-US persons reasonably believed to be located outside the United States.
  - Authorizes foreign surveillance programs by the National Security Agency (NSA), like PRISM and some earlier data collection activities which were previously authorized under the President's Surveillance Program from 2001.
- Executive Order (EO) 12333*
  - Signed on December 4, 1981 by U.S. President Ronald Reagan, was an Executive Order intended to extend powers and responsibilities of U.S. intelligence agencies and direct the leaders of U.S. federal agencies to co-operate fully with CIA requests for information. This executive order was titled United States Intelligence Activities.
  - Part 2.3 permits collection, retention and dissemination of the following types of information along with several others.
    - (c) Information obtained in the course of lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation
    - …
    - (i) Incidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws

*) Source: Wikipedia

Possible Data Protection Measures

- Data Encryption
- Access Control
- Contracts

Data Encryption

At Rest

Data is encrypted when stored on devices like hard drives, SSDs, tapes, etc.
This protects against storage devices being stolen. When storing data at a CSP without giving out the encryption keys encryption at rest will protect against unauthorized access by anyone who has no access to the encryption keys.

In Transit

Data is encrypted when being transferred between systems, e.g. using HTTPS, TLS
This protects data against unauthorized disclosure or modification “over the line“, i.e. when being transferred. This also ensures data protection between systems in the cloud or on-premises. It will ensure data cannot be accessed or modified by unauthorized systems or people as long as the encryption keys are not compromised. Encryption keys however have to be available on the involved end points (systems).

In Use

Data is encrypted while being processed by a system
This protects data from being accessed while operations are being performed on the data, i.e. on the processing system itself. As data being processed in the cloud needs to be available in unencrypted form, this typically is not given. Homomorphic encryption is the only way to fully protect the data in use, however it comes with an increase in necessary compute power by a factor of >10‘000

Access Control - Keys and Data

Encryption keys need to be protected in order to keep encrypted data save. This is typically done by Hardware Security Modules (HSMs) or similar services in the cloud (e.g. Azure Key Vault) which allow to store a key and perform operations with it without allowing the key to be accessed outside of the secure hardware / service. This guarantees that a key cannot be stolen and abused outside of the trusted environment.
Key operations however are possible, if the correct credentials are provided to the HSM or service. This allows anyone with access to the HSM or service and possession or control of the necessary credentials to perform operations with the key stored in the HSM / service, e.g. decryption of subsequent keys, signing of documents or code, issuing of certificates or tokens

When processing or transferring data the involved systems need to be able to access keys to perform operations on the data. Therefore the decryption key as well as the unencrypted data need to be available on the corresponding systems at least while the operation is being performed. This allows anyone with access to the system on a deep technical level (admin, root) to access keys and / or data.

Protection and ownership of keys are not relevant in this context. In the end keys need to be available and accessible to the CSP if he is to perform services for a customer. In addition all services are fully virtualized, workloads can be shifted between systems, so all keys have to be cached and transferred together with the workload in order to be available where ever data is to be processed or transferred. This increases availability and flexibility but on the other hand makes it nearly impossible to know where any data and the corresponding keys are and to adequately protect them.

Access Control – Users and Services

- Cloud environments typically use so-called security tokens to identify users, systems and processes and authorize them to access systems, services or data and perform operations on these. Therefore, the protection of these tokens but also – and more importantly – the instances issuing such tokens need to be protected from unauthorized access and use.

  - Tokens are protected using digital signatures, which ensure their content cannot be modified without detection. Verification of these signatures is therefore a basic functionality of any access control layer of any service. In addition, the lifetime of tokens is limited typically to a short time period, i.e. to a single request or a couple of minutes or even seconds.

  - Services issuing tokens are protected by several layers. The keys are kept secure (e.g. in a HSM) and access to the service is limited to a small group of trusted individuals. Systems issuing tokens are hardened and carefully monitored and in general offer a small attack surface.

- Anyone with the possibility to issue security tokens can create access options to all levels of a CSP environment, bypassing all available protection mechanisms

Contracts - CSP Processes

Microsoft*

- Microsoft does not provide any government with direct and unfettered access to our customers' data, and we do not provide any government with our encryption keys or the ability to break our encryption.
- If a government wants customer data, it must follow applicable legal process. It must serve us with a warrant or court order for content, or a subpoena for subscriber information or other non-content data.
- All requests must target specific accounts and identifiers.
- Microsoft's legal compliance team reviews all requests to ensure they are valid, rejects those that are not valid, and only provides the data specified.

Google*

1. Redirection
   If Google receives a request from a government agency for Cloud customer data, Google informs the government that it should issue the request directly to the organization in question. This approach is aligned with U.S. government policy and our contractual commitments.
2. 2. Evaluation of Legal Validity
   If the government nonetheless compels Google to respond to a request for customer data, a dedicated team of Google lawyers and specially trained personnel will carefully review the request to verify that it is lawful, proportionate, and satisfies Google's policies. Google maintains a dedicated, specialist, and cross-functional team to evaluate and process requests for user data while upholding the law and protecting users' privacy and security. All requests for user data must be processed and approved by team members before any data is made available. Training and support from legal counsel equips the relevant employees with the necessary skills to evaluate the validity of the legal process and ensure that all requests are handled in accordance with both the law and Google's policies and procedures. Furthermore, we object to, or limit or modify, any legal process that we reasonably determine to be overbroad, disproportionate, incompatible with applicable law, or otherwise unlawful.
3. 3. Customer Notice and Transparency
   We will notify the customer before their customer data is disclosed unless such notification is prohibited by law, could obstruct a government investigation, or lead to death or serious physical harm to an individual. Where prior notification by Google is prohibited under applicable law, it is Google's policy to notify the customer when any prohibition is eventually lifted, such as when a statutory or court ordered disclosure prohibition period has expired. This notification typically goes to the Google Cloud customer's point of contact.
4. 4. Customer Challenges
   Google will, to the extent allowed by law and by the terms of the government request, comply with a customer's reasonable requests regarding its efforts to oppose a request, such as the customer filing an objection to the disclosure with the relevant court and providing a copy of the objection to Google. If Google notifies the customer of a legal 8 request for customer data and the customer subsequently files an objection to disclosure with an appropriate tribunal and provides a copy of the objection to Google, Google will not provide the data in response to the request and hold it in escrow if legally permissible through the pendency of a customer challenge.

Amazon*

- The CLOUD Act does not impact AWS services or how we operate our business. Historically, we have received very few United States law enforcement requests, and we are transparent about the number of requests that we receive. We are always vigilant about customer privacy and security, and we are committed to providing our customers with industry-leading privacy and security protections when using our products and services. When we receive a request for content from law enforcement, we carefully examine it to authenticate accuracy and to verify that it complies with applicable law. Where we need to act to protect customers, we'll continue to do so. We have a history of challenging government requests for customer information that we believe are overbroad or otherwise inappropriate. If we are required to disclose customer content, we will continue to notify customers before disclosure to provide them the opportunity to seek protection from disclosure, unless prohibited by law

*) Source: CSP's information pages

CLOUD Act in action

To allow comparison of these numbers the selected reporting period is Jan – Jun 2022 where not otherwise noted (e.g. FISA data)

Microsoft Azure*

	Total Requests	
	Total Number of Law Enforcement Requests	Accounts / Users Specified in Requests
	#	#
TOTAL	26.365	58.665

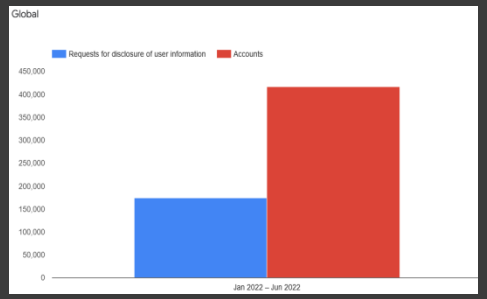
Some Customer Data Disclosed			
Law Enforcement Requests Resulting in Disclosure of Content		Law Enforcement Requests Resulting in Disclosure of Only Subscriber/Transactional (Non-Content) Data	
%	#	%	#
3,76%	992	53,26%	14.043

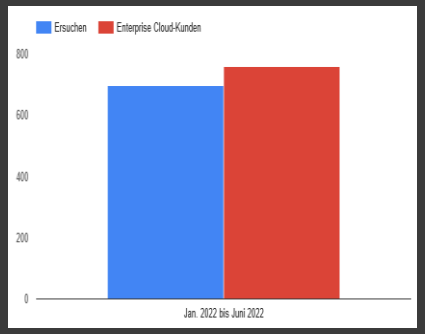
No Customer Data Disclosed			
Law Enforcement Requests Resulting in Disclosure of No Customer Data (No Data Found)		Law Enforcement Requests Resulting in Disclosure of No Customer Data (Request Rejected for Not Meeting Legal Requirements)	
%	#	%	#
17,94%	4.730	25,03%	6.600

National Security Requests 2021:

- 0 – 499 orders based on FISA
- ~ 12’000 accounts impacted

Google Cloud*

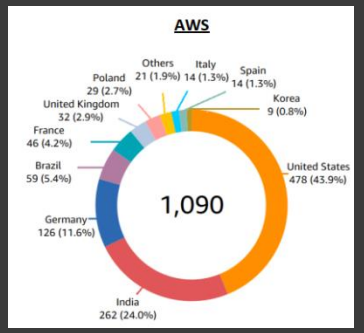


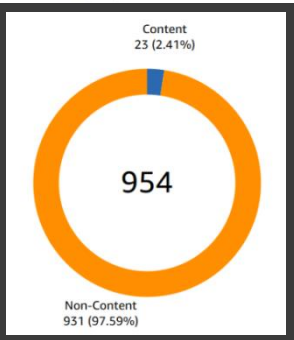


National Security Requests 2021:

- 0 – 499 orders based on FISA
- ~ 28’000 accounts impacted

Amazon AWS*





- No requests from US government that resulted in foreign data being exposed
- 0 – 249 orders based on FISA

Note: Your CSP’s transparency reports might (not) be fun to read…

*) Source: CSP's information pages

Considerations

- Using cloud-based solutions operated by US CSPs may result in conflicting situations with EU GDPR or Swiss DSG / VDSG.
  Make sure you fully understand the risks as well as the do‘s and don‘ts!

- Countermeasures on technology level have their limits. The more you want your CSP to do for you, the more he needs access to unencrypted data opening up options for (lawful) access by others

- Think about unwanted / inacceptable risks. If you don‘t want anyone having access to certain data, assess whether going to the cloud / using cloud-based services esp. from US-based companies is a good idea