



THE CLOUD ACT: MYTH VS. FACT

The CLOUD Act represents a breakthrough approach to protect individual privacy while enabling law enforcement to access data for the purposes of investigating serious crimes. As this approach – which is supported by major stakeholders in the technology industry and law enforcement communities – gains momentum, there have been some inaccurate descriptions of the legislation. This document seeks to separate those myths from the facts about the CLOUD Act.

X MYTH: The CLOUD Act would allow foreign governments to conduct real-time wiretaps on Americans. Some argue that the CLOUD Act would enable foreign governments to obtain real-time interception of users' communications without requiring the standards or due process required under US laws, including the *Wiretap Act*.

✓ FACT: The CLOUD Act includes strong safeguards around real-time access that parallel existing standards.

- The CLOUD Act explicitly forbids a foreign government certified under the Act to target a US person directly or indirectly.
- The CLOUD Act establishes several requirements for any real-time access to digital communications by a certified government. A real-time surveillance order must be for a fixed, limited duration, last no longer than is reasonably necessary to accomplish its purpose, and only be available when the same information cannot reasonably be obtained by less intrusive methods.
- These requirements parallel those delineated in the *Wiretap Act* and, in fact, were replicated nearly verbatim in the CLOUD Act.
- Though the CLOUD Act does not adopt the *Wiretap Act's* approach of limiting its application to a list of predicate offenses, it limits foreign government access to investigations related to serious crimes – a designation arguably more restrictive than the *Wiretap Act's* enumerated offenses.

X MYTH: The CLOUD Act would circumvent Congress. Some argue that the CLOUD Act undermines Congress's authority by allowing the Attorney General to directly enter into agreements with foreign governments without Congress's advice and consent, as opposed to Mutual Legal Assistance Treaties, which require Senate ratification.

✓ FACT: The CLOUD Act ensures a robust role for Congress.

- Far from diminishing Congress's oversight, the CLOUD Act creates a three-pronged mechanism to ensure robust Congressional oversight and opportunities for Congress to intervene should it have concerns with a particular agreement.
 - First, it establishes rigorous statutory criteria that every country must meet before it can be certified under the Act.
 - Second, it requires the Executive Branch to report any certification decision to Congress, imposes a mandatory waiting period before the certification goes into effect, and creates an expedited procedure for Congress to override any such certification.
 - Finally, it ensures that these certifications are transparent, providing the public with information about which countries are certified and empowering advocates to hold the Executive Branch accountable for its decisions.
- This approach adopts a tried-and-true oversight mechanism. In fact, Congress oversees numerous other agreements – including on highly sensitive matters, such as civilian nuclear cooperation (“123” agreements) – using precisely the approach adopted by the CLOUD Act.

X MYTH: The CLOUD Act would support foreign governments in committing human rights abuses. Some argue that, under the CLOUD Act, the government could enter into agreements with countries that do not protect human rights, potentially allowing them to obtain information on their citizens through such agreements and use it in support of torture and other abuses.

✓ FACT: The CLOUD Act contains clear, robust human rights protections.

- The CLOUD Act explicitly requires that the Attorney General and Secretary of State certify to Congress that a country “affords robust substantive and procedural protections for privacy and civil liberties,” based upon an examination of its human rights record among other factors, before certifying that country for an agreement under the Act.
- Specifically, the CLOUD Act requires an examination of a country's adherence to international human rights obligations and commitments –

- including “protection from arbitrary and unlawful interference with privacy;” “fair trial rights;” “freedom of expression, association, and peaceful assembly;” “prohibitions on arbitrary arrest and detention;” and prohibitions against torture and cruel, inhuman, or degrading treatment or punishment – as part of the certification.
- Moreover, the CLOUD Act requires that any individual agreement negotiated under the Act include specific safeguards prohibiting any surveillance order issued by a foreign government from being used to impinge upon freedom of speech.

X MYTH: The CLOUD Act would allow foreign governments to access US persons’ data in violation of the Constitution. Some argue that the CLOUD Act would allow searches and seizures within the US that violate Fourth Amendment protections, potentially endangering U.S. persons’ data that is “incidentally” collected by wiretaps.

✓ FACT: The CLOUD Act imposes strict requirements on access to data belonging to US persons.

- The CLOUD Act prohibits the targeting of US persons’ data by foreign governments.
- Furthermore, it prohibits any effort to circumvent a country’s own legal requirements, either by asking a certified country to request the data on their behalf or targeting a non-US person for the purpose of accessing communications data belonging to a U.S. person.
- The CLOUD Act also requires foreign governments to adopt robust minimization procedures for all data collected and precludes the dissemination of information related to U.S. persons except in very limited circumstances (evidence of a serious crime).

X MYTH: The CLOUD Act does not require independent judicial oversight of surveillance orders prior to their issuance. Some argue that the CLOUD Act would allow foreign governments to issue surveillance orders without any review by a judicial or other independent body before they are issued.

✓ FACT: The CLOUD Act explicitly requires judicial oversight of such orders.

- The CLOUD Act requires that every agreement negotiated under the Act include a requirement that any surveillance order issued by a foreign government must be (1) individualized, and (2) “subject to review or oversight by a court, judge, magistrate, or other independent authority.”

X MYTH: The CLOUD Act weakens standards for foreign governments to obtain data. Some argue that the CLOUD Act would create easier pathways for foreign government to access data by circumventing the Mutual Legal Assistant Treaty (MLAT) process and by retreating from the “probable cause” standard adopted by MLATs.

✓ FACT: The CLOUD Act maintains high standards for data access while adapting to an evolving international legal landscape.

- Foreign governments – from the United Kingdom to Brazil – are rewriting or reinterpreting their law enforcement access laws to apply to US technology companies in ways that compromise the MLAT process.
- These laws can require access to content on US or foreign persons without privacy protections.
- Far from creating an “easier pathway” for foreign governments to obtain data, the CLOUD Act recognizes that doing nothing and letting foreign governments write their own rules will lead to a race to the bottom for individual privacy. Instead, the CLOUD Act seeks to ensure that the US Government can use its diplomatic leverage to control foreign governments’ access to digital evidence and the privacy of US persons even as the international legal landscape evolves.
- In addition, the CLOUD Act acknowledges that foreign governments’ legal systems operate in a way this differs from our own. Rather than impose foreign concepts on them, it adopts a minimum legal standard – one that is analogous to probable cause – foreign countries must meet before they can be certified.
- By conditioning certification on meeting rigorous privacy standards – including independent oversight and authorization, individualized surveillance orders, and a reasonable justification based on specific and articulable facts that the request seeks evidence of a serious crime – the CLOUD Act provides an incentive for foreign countries to raise their privacy standards for data access, leading to a net gain in privacy rights around the globe.