June 26, 2018

Protecting Foreign Government Cloud Service Customers

AWS is fully committed to protecting its customers' data and complying with applicable laws in each country in which it operates. Critically, we are committed to working closely with foreign government customers to ensure that their cloud content remains safe and secure in AWS data centers located anywhere in the world. Despite some initial reports that sought to stoke fears about the application in the United States of the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), the law has created additional safeguards for cloud content—on top of existing protections. More importantly, we do not believe the CLOUD Act enables the U.S. government to access foreign government cloud content. We are confident in our ability to protect foreign government cloud content using legal means available under U.S. law, including application of sovereign immunity and comity defenses. And as an added layer of security, foreign government customers can also apply strong encryption to cloud content on AWS services, which acts as a complete safeguard against any access not authorized by the customer. We provide our insights and clarifications about the legal, structural, and practical protections available to foreign governments below.

Summarizing the CLOUD Act

Let's start with what has changed. The CLOUD Act created a specific judicial mechanism that U.S. law enforcement can use pursuant to the Stored Communications Act (SCA) to seek access to information held outside the United States if that information was used to commit a crime under U.S. law. Importantly, the CLOUD Act explicitly recognizes the right of cloud service providers to challenge disclosing information if doing so would conflict with another country's laws or national interests. Prior to the CLOUD Act, that right was a disputed under the SCA—although we have not seen any evidence of U.S. law enforcement using the SCA to seek information owned by a foreign government, it is now clear that AWS can challenge disclosure of foreign government cloud content if disclosure would violate foreign law or sovereignty. We will work with the foreign government customers to help ensure that both AWS and our customers are best positioned to realize these benefits.

Additionally, the CLOUD Act contemplates that the U.S. government will enter into new "executive agreements" with foreign governments. These executive agreements will serve to simplify and govern bilateral foreign law enforcement information requests under mutually agreeable terms and conditions that can provide additional grounds to resist disclosure and ensure that all disclosures are fully authorized by both governments. Through these executive agreements, foreign governments will be able to help shape the application of the CLOUD Act through diplomacy with the U.S. government. We are happy to work directly with foreign government customers and the U.S. Department of Justice (DOJ) to help expedite entry into executive agreements.

What hasn't changed? The CLOUD Act does not give U.S. law enforcement unlimited or unfettered access to customer information stored inside or outside the United States. To protect individual rights, U.S. law applies procedural safeguards to law enforcement information requests, and the CLOUD Act does not change these protections. In cases of crimes, such as terrorism, the CLOUD Act enables U.S. law enforcement to apply to an independent U.S. court to obtain a warrant or order. That application must specify the evidence sought and provide sufficient facts to demonstrate to the U.S. court that there is probable cause to believe a crime has occurred and the evidence is directly related to that crime. An independent judge decides whether U.S. law enforcement has met its burden, and that judge's decision

is subject to appeal and review by independent appellate courts. This is a far more rigorous and independent procedure than exists for law enforcement information requests in other countries.

AWS's top priority is the security of our customers' cloud content. The CLOUD Act doesn't change that. We stand by our commitment to not disclose customer cloud content unless legally compelled to do so. We also stand by our commitment that we will notify customers before disclosing cloud content. Finally, the CLOUD Act will not prevent us from acting to protect our customers—in fact, it provides us with additional means to challenge disclosure. We have challenged U.S. government requests for customer information that we believed were unlawful or overbroad, winning decisions that have helped to set legal standards for protecting customer privacy interests, and we remain committed to doing so.[1]

Governments are Moving to the Cloud

AWS offers the world's most comprehensive and broadly adopted cloud services, serving millions of active customers every month and tens of thousands of government agencies, education institutions, and nonprofit organizations around the world. Although AWS has become the chosen cloud service provider for all types of government customers, including ministries and agencies (e.g., UK Ministry of Justice, UK Driver and Vehicle Licensing Agency, Singapore Land Transport Authority, and U.S. Departments of State, Homeland Security, Energy, Health and Human Services, and Agriculture), instrumentalities (e.g., Italian Court of Auditors), and related organizations (e.g., World Bank, the United Nations, and Europol), all AWS customers benefit from the infrastructure we have built to meet the requirements of the most security-sensitive bodies. Even with the incredible pace of innovation and adoption of cloud services as a more secure, scalable, and cost-effective alternative than traditional IT infrastructure, we believe we are just at the beginning of what is possible with the cloud. Our government customers recognize this fact, and they are adopting advanced cloud solutions to address their largest, most pressing operational, social, and economic needs—from artificial intelligence to the Internet-of-things, computer vision, voice-enabled applications, natural language processing and comprehension, big data, virtual reality, and much more. We see a path for foreign governments to embrace the future of cloud technologies to meet these critical needs, while enjoying legal, structural, and practical protections for their cloud content.

Legal Protections: Sovereignty and National Interests

Foreign governments, including their ministries, agencies, and instrumentalities, are unique–both in their interests as customers and as sovereign entities under U.S. laws. That fact allows AWS to challenge U.S. law enforcement information requests that may target the cloud content of foreign governments.

Although the CLOUD Act states that cloud service providers must comply with obligations in the SCA to disclose information pertaining to a "customer" or "subscriber" in response to a valid U.S. law enforcement information request (subject to the procedural protections for warrants and other orders described above), we believe that the terms "customer" and "subscriber" as used in the CLOUD Act do not and cannot include foreign governments. And we are in good company: U.S. courts have long recognized that the general words of a statute do not include governments and do not affect the rights of governments unless such an interpretation is clear and indisputable from the text of the statute. This is especially so where application of the statute would deprive a sovereign foreign government of established interests or where the results of such an application would be absurd. We believe our

[1] See, for example, https://www.aclu.org/sites/default/files/field_document/2010-10-25-AmazonvLay-Order.pdf and http://www.wiwd.uscourts.gov/opinions/pdfs/2006-2009/07-GJ-04-11-23-07.PDF

perspective on the CLOUD Act fulfills both these conditions in light of the unique sovereign interests a foreign government has in its own cloud content.

Further, because the CLOUD Act does not specifically mention foreign governments as among those whose cloud content is subject to U.S. law enforcement information requests, we believe the CLOUD Act should not apply to the cloud content of a foreign government. Interpreting the CLOUD Act to allow U.S. law enforcement to access the cloud content of foreign governments would lead to an absurd result, as it would allow an end-run around the protections of sovereign immunity under Foreign Sovereign Immunities Act (FSIA) by enabling the U.S. government to obtain a foreign government's information without having to subject the foreign government to federal jurisdiction (we discuss sovereign immunity in more detail below). We do not believe the CLOUD Act expands the ability of U.S. law enforcement officials to reach the cloud content of foreign governments. Further, we believe the plain language of the CLOUD Act, and in particular its respect for comity, would preclude any disclosure of foreign government cloud content.

The FSIA explicitly protects the sovereign immunity of foreign governments, and the CLOUD Act does nothing to change that fact because the CLOUD Act contains no waivers of sovereign immunity. The FSIA stands as the exclusive framework for obtaining (or defeating) jurisdiction over a foreign government in U.S. courts, a position unequivocally and repeatedly confirmed by the U.S. Supreme Court.[2] Indeed, the U.S. Supreme Court has frequently stated that it will "construe statutes to avoid unreasonable interference with other nations' sovereign authority where possible."[3] Sovereign immunity strictly limits a court's jurisdiction, and once sovereign immunity is established, the court lacks both personal and subject matter jurisdiction. Jurisdiction is essential because courts cannot enforce a request for information under the CLOUD Act (or compel any act) without jurisdiction, and the power of a court to issue warrants or other orders for information cannot be more extensive than its jurisdiction. As a baseline matter, there is no question that foreign governments enjoy sovereign immunity to any court action in the United States.

Although AWS is not itself entitled to sovereign immunity, we believe that AWS may effectively assert derivative sovereign immunity in response to U.S. law enforcement information requests under the CLOUD Act. Indeed, U.S. courts have recognized the protections of derivative sovereign immunity for private U.S. companies acting at the direction of foreign governments (in *Butters v. Vance Int'l, Inc.* and *Alicog v. Kingdom of Saudi Arabia*). Derivative sovereign immunity would apply as long as AWS is acting at the direction of a foreign government and that foreign government's use of cloud services align with activities that are peculiar to sovereigns (e.g., executing government functions or maintaining state secrets). A key pillar for application of the principle of derivative sovereign immunity is our belief that AWS's customers, and not AWS itself, have complete control over their cloud content. We are very clear that AWS acts on cloud content stored on AWS services only at the direction of our customers, as embodied in our commitments under our contracts for cloud services and our compliance with global privacy and data protection regimes, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the EU. Foreign governments make their own judgments about what information they will make available, and under

[2] See e.g., *Permanent Mission of India to the United Nations v. City of New York*. and *Argentine Republic v. Amerada Hess Shipping Corp.*

[3] *RJR Nabisco, Inc. v. European Cmty*.

what terms, to other governments—often through high-level diplomacy and international agreements. A foreign government's use of cloud services should not alter this foundational principle.

In addition to the sovereign immunity defenses described above, the CLOUD Act confirms that the principles of comity enable cloud service providers to challenge disclosing information to U.S. law enforcement if doing so would conflict with a foreign country's laws or national interests. Although comity analysis involves multiple considerations, the most important factor is the relative national interests at play. Sovereign immunity, and the United States' express recognition of it, weighs heavily in the comity analysis too, and we believe U.S. courts will give significant weight to comity (bolstered by a sovereign immunity foundation) for the simple reason that if a U.S. court were to do otherwise, it would risk undermining the United States' own sovereign immunity in the proceedings of foreign courts. The U.S. government's interests in enforcing a U.S. law enforcement information request would be significantly diminished if compliance would expose the U.S. government itself to similar information demands from foreign governments without the explicit agreement of the U.S. government. Indeed, U.S. courts have a demonstrated history of rejecting information requests leveled against foreign governments.

Structural Protections: Executive Agreements, Foreign Laws, and Contract Terms

The CLOUD Act creates positive incentives for foreign governments to negotiate reciprocal executive agreements with the U.S. government and to enact protections under their own laws for information vital to their national interests. In doing so, foreign governments can take the initiative to further shape the application of the CLOUD Act to cloud content. Under executive agreements, cloud service providers will not only have the independent right to challenge U.S. law enforcement information requests where the request conflicts with a foreign nation's laws, but they may also inform foreign governments of the targets of information requests. Executive agreements under the CLOUD Act will further allow the U.S. government and foreign governments to establish the conditions under which their sovereign national interests must be recognized. AWS stands ready to help support efforts to establish an executive agreement between the United States and foreign governments using or seeking to adopt cloud services.

To help realize the benefits of sovereign immunity and comity described above, AWS will work with foreign government customers to add contractual protections to the agreements governing their use of AWS services. For example, our contracts can be adapted to: (1) expressly recognize, and not waive, the sovereign immunity of a foreign government and the derivative immunity of AWS (including recognizing that the terms "customer" and "subscriber" as used in the CLOUD Act do not apply to a foreign government); (2) affirm the right of a foreign government to direct the management of their cloud content; (3) define the scope of AWS's activities in service of the foreign government's directives and particular sovereign rights and interests; (4) affirm the foreign government's objection to any disclosure of its cloud content; (5) prohibit AWS from disclosing foreign government cloud content; and (6) recognize specific foreign laws that would be violated by the disclosure of foreign government cloud content.

Practical Protections: Respecting Foreign Governments and Encryption

It bears noting that the U.S. government generally does not seek information owned by foreign governments through the SCA. In fact, we are not aware of any U.S. law enforcement information requests under the SCA seeking information owned by a foreign government. This is not surprising, as the internal guidelines of both the DOJ and the Federal Bureau of Investigation (FBI) direct against making such requests. In December 2017, the DOJ issued publicly available guidance that discourages prosecutors from seeking information from cloud service providers and instead advises prosecutors, where possible,

to seek information directly from the customer that owns the information.[4] For its part, the FBI's Domestic Investigations and Operations Guide provides for specific restrictions against using the SCA to request information relating to the capabilities, intentions, and activities of foreign governments unless doing so would fall within the FBI's core national security mission.[5]

Finally, we know that the best way to protect content—whether it's stored in the cloud or elsewhere—is to render it inaccessible to unauthorized parties. That is why we provide tools and advanced encryption services that customers can use to protect their cloud content and why customers can choose from a number of supported third-party encryption solutions when they use AWS services. Cloud content that has been encrypted is rendered useless without the applicable decryption keys. Further, the CLOUD Act expressly prohibits executive agreements from creating any obligation that cloud service providers be capable of decrypting content.

Protections for Foreign Governments

Taken together, we believe that the circumscribed scope of the CLOUD Act, combined with the legal, structural, and practical protections available under the law can safeguard the cloud content of sovereign foreign governments, while establishing a framework for international cooperation in fighting crime.

[4] DOJ guidance available at https://www.justice.gov/criminal-ccips/file/1017511/download.

[5] Excerpt from 2013 FBI Domestic Investigations and Operations Guide:

> 9.9 (U) INVESTIGATIVE METHODS NOT AUTHORIZED DURING A FULL POSITIVE FOREIGN INTELLIGENCE INVESTIGATION [*Emphasis in original*]
>
> The following investigative methods are not permitted to be used for the purpose of collecting positive foreign intelligence pursuant to PFI Collection Requirements:
>
> . . .
>
> H) (U//FOUO) *Stored wire and electronic communications and transactional records.* (Section 18.6.8) [*Referring to the SCA*]